



As Pessoas nos Sistemas de Gestão da Segurança da Informação

José Manuel Gaivéo

UNIVERSIDADE ABERTA

2008

UNIVERSIDADE ABERTA

Doutoramento em Informática

**As Pessoas nos Sistemas de Gestão da
Segurança da Informação**

José Manuel Gaivéo

Orientação:

Professor Doutor Alexandre Gomes Cerveira (DCET/UAb)

Professora Doutora Maria Leonilde dos Reis (DSI/ESCE/IPS)

2008

Dedicatória

à Adelaide

e

à Manuela

Agradecimentos

O presente trabalho só foi possível de concretizar com o apoio de diversas pessoas. Para todas elas e de um modo genérico quero aqui deixar claramente expressa a minha gratidão.

Pela contribuição fundamental que tiveram para a realização deste trabalho não quero no entanto deixar de agradecer particularmente a algumas Pessoas, cuja influência se revelou essencial na sua concretização.

Ao Professor Doutor Alexandre Cerveira e à Professora Doutora Leonilde Reis, pela motivação que conseguiram transmitir, pelo acompanhamento, apoio e orientação que se revelaram indispensáveis para a concretização deste trabalho.

Aos responsáveis do IPS, das suas Unidades Orgânicas e Serviços em que se baseou o Estudo de Caso, sem os quais estaria comprometida a realização deste trabalho, pela disponibilidade demonstrada e pelas informações prestadas.

A todas(os) as(os) Colegas que preencheram e devolveram os questionários que suportam a componente prática.

Ao IPS e à ESCE pela dispensa de serviço docente que se revelou fundamental para a finalização do trabalho.

Aos meus colegas da ESCE pelo apoio e incentivo.

À minha família e amigos pelo interesse e apoio que desde sempre manifestaram.

À minha esposa e à minha filha, pela paciência demonstrada durante a realização deste trabalho, assim como pelo carinho, apoio, incentivo e encorajamento constantes ao longo de todo o tempo que lhes retirei.

E de uma forma geral, a todos os que, de forma directa ou indirecta, contribuíram para a concretização deste trabalho.

Resumo

Este trabalho apresenta um enquadramento conceptual das necessidades organizacionais em termos da utilização da informação, de segurança da informação e do envolvimento das Pessoas nas actividades associadas quer à informação, quer à segurança dessa mesma informação.

Consideram-se igualmente os impactos, em termos de segurança, da utilização dos sistemas de informação que permitem a partilha da informação organizacional e das tecnologias de informação e comunicação que suportam esses mesmos sistemas.

Com estes objectivos foram estudadas diversas normas, directa ou indirectamente relacionadas com a segurança da informação, objectivando a sua utilização no suporte das necessidades de segurança identificadas.

Neste âmbito, foram também estudadas normas relacionadas com a gestão dos sistemas de informação e das tecnologias de informação e comunicação, particularmente nos aspectos que envolvem as Pessoas.

A construção do Modelo destinado a suportar a integração da segurança da informação nos sistemas desenvolvidos ou em desenvolvimento, baseou-se nas metodologias tradicionais que suportam a concepção e desenvolvimento quer dos sistemas de informação, quer dos sistemas de gestão de segurança da informação.

O Modelo foi concebido com base em referenciais obtidos através quer da revisão da literatura, quer das métricas e do normativo considerado adequado ao estudo desta problemática.

Este desenvolvimento tem como principal objectivo responder aos anseios e necessidades das Pessoas, quando confrontadas com a necessidade de assegurar a protecção da informação e dos sistemas e das tecnologias que a suportam.

A pertinência do Modelo é tanto maior quanto maior for a importância das Pessoas como activos organizacionais e as suas capacidades em utilizar adequadamente a informação na prossecução dos objectivos organizacionais na actual Sociedade da Informação.

A necessidade de obter a percepção das Pessoas acerca da segurança da informação foi colmatada através da realização de um questionário, sendo este construído com base na

especificidade da organização que é objecto de estudo, tendo como suporte fundamental para as questões a revisão da literatura, as métricas e as normas relacionadas com esta problemática.

A validação do Modelo, além das componentes relativas à legislação e normativos aplicáveis, foi efectuada tendo em consideração os tópicos pertinentes que foram obtidos através da análise das respostas aos questionários, considerando-se o seu enquadramento com os referenciais do referido Modelo.

Como vantagens decorrentes do Modelo devem referenciar-se a possibilidade de, através da percepção das Pessoas, proporcionar o seu maior envolvimento nas actividades organizacionais que incluam a utilização dos sistemas de informação e das tecnologias de informação e comunicação, considerando igualmente os impactos decorrentes de mudanças efectuadas quer em termos de sistemas de informação quer de tecnologias de informação e comunicação.

A aplicação do Modelo nas práticas de concepção, implementação e operação dos sistemas de gestão da segurança da informação na organização que suporta o estudo de caso, encontra vantagens na utilização dos referenciais do Modelo em conjunto com os itens e tópicos resultantes da análise dos resultados dos questionários, permitindo que as Pessoas utilizem esses aspectos como recomendações a incluir nessas actividades.

Outra das vantagens, com um potencial de impacto superior, relaciona-se com a segurança da informação, pessoal ou organizacional, com que as Pessoas têm de lidar, e que envolve inevitavelmente a segurança dos sistemas de informação e das tecnologias de informação e comunicação que suportam os fluxos de informação, e a respectiva segurança.

Abstract

This work presents a conceptual frame of organizational needs, concerning the use of information, information security, and People's involvement on information and information security related activities.

There are also taken into account the security impacts derived from the use of information systems, which allow information to be shared between organizations and the information and communications technologies that support the above mentioned systems.

In order to fulfil these objectives, several information security standards and others closely related where studied, in order to use it in responding to identified security needs.

Within this scope, information systems and information and communications technologies management related standards where also analysed, particularly the ones regarding People related subjects.

The development of the presented Model, whose objective is to support information security integration on mature or under development systems, was based on information systems and information security management systems conception and development methodologies.

These development striving to find answers to People's needs and fears concerning this matter, when facing the needs to assure information protection, as also protect systems and technologies that support it.

The Model relevance is bigger than to bigger was People as organizational assets in today's Information Society, and on adequate normative to information security study, in order to support organizational objectives.

The need to gain knowledge about People's perception concerning information security issues lead to the use of a questionnaire, built based on the specificity of the type of organization being studied and presenting questions supported by security standards.

This Model was validated with regard to relevant topics derived from answers provided by respondents to the questionnaire, apart from applicable standards and law, and taking into account Model references.

Model advantages refers to the possibility of, through People perception, allow the increasing of their involvement in organizational activities, including information and communication technologies and information systems use, taken into account information and communication technologies and information systems changes impact.

The Model application to develop, implement and operate the information security management systems on the organization that supports the case study, find advantages with an integrated usage of the Model references with the questionnaire results, allowing that People use it as main recommendations for practical application in these processes.

Another advantage, with a higher impact potential, relates to information security, either personal or organizational, that People use, evolving security of information and communication technologies and information systems that support information flows and security.

Índice

<i>Índice de Figuras</i>	<i>xii</i>
<i>Índice de Quadros</i>	<i>xiii</i>
<i>Índice de Tabelas</i>	<i>xiv</i>
<i>Índice de Tabelas</i>	<i>xiv</i>
<i>Siglas</i>	<i>xvii</i>
1 Introdução	1
1.1. Objectivos	1
1.2. Motivações	3
1.3. Enquadramento	6
1.4. Abordagem à Investigação	15
1.5. Resultados e Contributos	17
1.6. Estrutura do Trabalho	19
Referências bibliográficas	22
2 Enquadramento Normativo e Legal	25
2.1. Enquadramento Normativo	25
2.1.1. BS ISO/IEC 17799:2005 – Code of Practice for Information Security Management.....	28
2.1.2. BS ISO/IEC 27001:2005 – Information Security Management Systems - Requirements	30
2.1.3. BS 7799-3:2006 – Guidelines for Information Security Risk Management	31
2.1.4. ISO/IEC FDIS 13335-1:2004 – Concepts and models for information and communications technology security	32
2.1.5. ISO/IEC 21827:2002 – Systems Security Engineering - Capability Maturity Model (SSE-CMM).....	32
2.1.6. BS ISO/IEC 20000-1:2005 – Service Management - Specification.....	34
2.1.7. BS ISO/IEC 20000-2:2005 – Service Management - Code of practice	35
2.1.8. NIST SP800-12 – An Introduction to Computer Security: The NIST Handbook.....	36
2.1.9. NIST SP800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems	38
2.1.10. NIST SP800-16 – Information Technology Security Training Requirements: A Role -and Performance- Based Model.....	40
2.1.11. NIST SP800-18 – Guide for Developing Security Plans for Information Technology Systems	41
2.1.12. NIST SP800-26 – Security Self-Assessment Guide for Information Technology Systems	42
2.1.13. NIST SP800-27 – Engineering Principles for Information Technology Security (A Baseline for Achieving Security)	43
2.1.14. NIST SP800-30 – Risk Management Guide for Information Technology Systems	45
2.1.15. NIST SP800-33 – Underlying Technical Models for Information Technology Security	46
2.1.16. NIST SP800-34 – Contingency Planning Guide for Information Technology Systems	47
2.1.17. NIST SP800-55 – Security Metrics Guide for Information Technology Systems	49
2.1.18. NIST SP800-61 – Computer Security Incident Handling Guide	50
2.1.19. NIST SP800-64 – Security Considerations in the Information System Development Life Cycle	51

2.1.20. NIST SP800-80 – Guide for Developing Performance Metrics for Information Security	51
2.1.21. NIST SP800-100 – Information Security Handbook: A Guide for Managers	53
2.1.22. The Standard of Good Practice for Information Security (the Standard)	54
2.1.23. Cardholder Information Security Program (CISP).....	55
2.1.24. Information Technology Infrastructure Library (ITIL).....	56
2.1.25. OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security	57
2.1.26. Control Objectives for Information and related Technology (COBIT).....	58
2.1.27. Generally Accepted Information Security Principles (GAISP).....	60
2.1.28. Information Systems Security Assessment Framework (ISSAF)	64
2.1.29. IT Baseline Protection Manual.....	65
2.1.30. RFC 2196 – The Site Security Handbook.....	65
2.2. Enquadramento Legal.....	66
2.2.1. Legislação Nacional.....	66
2.2.1.1. <i>Lei da Criminalidade Informática</i>	67
2.2.1.2. <i>Protecção Jurídica de Programas de Computador</i>	67
2.2.1.3. <i>Lei da Protecção de Dados Pessoais</i>	68
2.2.1.4. <i>Lei das Comunicações Electrónicas</i>	68
2.2.1.5. <i>Lei da Protecção da Privacidade no Sector das Comunicações Electrónicas</i>	68
2.2.1.6. <i>A Segurança da Informação na Legislação e Regulamentação Nacional</i>	69
2.2.2. Regulamentos e Recomendações	76
2.2.3. Directivas da Comunidade Europeia.....	77
2.2.3.1. <i>Directiva 91/250/CEE do Conselho</i>	77
2.2.3.2. <i>Directiva 95/46/CE do Parlamento Europeu e do Conselho</i>	78
2.2.3.3. <i>Directiva 2002/58/CE do Parlamento Europeu e do Conselho</i>	78
2.2.4. Legislação Internacional	79
2.2.4.1. <i>Sarbanes-Oxley Act of 2002 (SOX)</i>	79
2.2.4.2. <i>Health Insurance Portability and Accountability Act (HIPAA)</i>	80
2.2.4.3. <i>Personal Information Protection and Electronic Documents Act (PIPEDA)</i>	81
2.3. Conclusões	82
Referências bibliográficas	82
3 Informação, Sistemas e Tecnologias de Informação e Comunicação.....	87
3.1. As Organizações e a Globalização	87
3.2. Informação	92
3.3. Sistemas de Informação.....	98
3.4. Tecnologias de Informação e Comunicação	105
3.5. Conclusões	108
Referências bibliográficas	108
4 Segurança da Informação.....	113
4.1. Evolução Histórica.....	114
4.2. Globalização e Segurança.....	117
4.3. Segurança da Informação e dos Sistemas de Informação	119
4.4. Políticas de Segurança	125
4.5. Sistemas de Gestão da Segurança da Informação.....	130
4.6. Conclusões	133

Referências bibliográficas	134
5 As Pessoas	137
5.1. O Capital Humano das Organizações	137
5.2. As Pessoas e as Tecnologias de Informação e Comunicação.....	142
5.3. Caracterização e Tipificação dos Utilizadores	146
5.4. As Pessoas e a Segurança da Informação	151
5.5. Usabilidade dos Sistemas de Informação.....	154
5.6. Impactos da Segurança na Usabilidade	158
5.7. Conclusões	161
Referências bibliográficas	161
6 Métricas de Segurança	167
6.1. Conceito de Métrica.....	167
6.2. Tipificação de Medições e Métricas de Segurança.....	169
6.3. Métricas	173
6.3.1. Princípios Orientadores.....	173
6.3.2. Normas de Referência.....	175
6.3.3. Especificação de Métricas.....	178
6.4. Conclusões	182
Referências bibliográficas	183
7 Criação do Modelo.....	187
7.1. Enquadramento Conceptual	188
7.1.1. Contributos da Literatura	188
7.1.2. Contributos das Métricas	193
7.1.3. Modelo SDLC.....	196
7.2. Normativo Aplicável	199
7.2.1. Normas	199
7.2.2. Contributos das Normas	209
7.2.3. Modelo PDCA	216
7.3. Modelo.....	217
7.3.1. Base de Desenvolvimento	217
7.3.2. Características do Modelo	219
7.3.3. Modelo Conceptual	221
7.4. Exemplos de Métricas.....	226
7.5. Conclusões	228
Referências bibliográficas	229
8 Estudo de Caso.....	235
8.1. Métodos e Técnicas de Análise.....	235
8.2. Selecção de Casos	236
8.3. Definição do Âmbito do Estudo	237
8.3.1. Caracterização da Instituição	238
8.3.2. Caracterização da População-Alvo	239

8.4. Elaboração dos Questionários	240
8.5. Análise dos Resultados dos Questionários	254
8.5.1. Resultados do Grupo A – Identificação/Caracterização do(a) Inquirido(a)	256
8.5.2. Resultados do Grupo B – Computador Pessoal	258
8.5.2.1. Existência e Partilha de Computador Pessoal	259
8.5.2.2. Acesso à Internet com o Computador Pessoal	260
8.5.2.3. Utilização de Password no Computador Pessoal	261
8.5.2.4. Utilização de Mecanismos de Protecção	262
8.5.2.5. Realização de Cópias de Segurança	263
8.5.2.6. Utilização do Computador Pessoal	264
8.5.2.7. Percepção da Segurança do Computador Pessoal	265
8.5.3. Resultados do Grupo C – Sistema Informático	268
8.5.3.1. Funcionamento e Mudanças no Sistema Informático	268
8.5.3.2. Conhecimentos e Formação em Informática	271
8.5.3.3. Password e Mecanismos de Acesso ao Sistema Informático	272
8.5.3.4. Utilização do Correio Electrónico	275
8.5.3.5. Acesso e Utilização do Sistema Informático	276
8.5.4. Resultados do Grupo D – Segurança da Informação	279
8.5.4.1. Políticas de Segurança da Informação e do Sistema Informático	279
8.5.4.2. Mecanismos de Protecção do Sistema Informático	281
8.5.4.3. Realização de Cópias de Segurança	282
8.5.4.4. Percepção da Facilidade de Acesso ao Sistema Informático	283
8.5.4.5. Controlo dos Activos do Sistema e da sua Utilização	285
8.5.4.6. Percepção da Segurança do Sistema Informático	286
8.5.5. Resultados do Grupo E – Usabilidade do Sistema Informático	295
8.5.5.1. Formação na Utilização do Sistema	295
8.5.5.2. Facilidade de Utilização e Aprendizagem do Sistema	298
8.5.6. Comparação com os Resultados do Grupo de Teste	301
8.6. Conclusões	302
Referências bibliográficas	304
9 Validação do Modelo	305
9.1. Princípios	305
9.2. Metodologia de Aplicação	306
9.3. Contributos dos Questionários	307
9.3.1. Contributos do Grupo A – Identificação/Caracterização do(a) Inquirido(a)	307
9.3.2. Contributos do Grupo B – Computador pessoal	307
9.3.3. Contributos do Grupo C – Sistema Informático	311
9.3.4. Contributos do Grupo D – Segurança da Informação	314
9.3.5. Contributos do Grupo E – Usabilidade do Sistema Informático	317
9.4. Análise das Questões de Partida na Perspectiva da Segurança	320
9.4.1. Percepção das Pessoas acerca da Segurança da Informação	321
9.4.2. Classificação da Segurança da Informação numa Perspectiva Pessoal	324
9.4.3. Percepção das Pessoas acerca da Utilização dos SI e das TIC	325
9.4.4. Impactos dos SGSI nas Actividades das Pessoas	328
9.5. Validação do MIDImOS	332
9.5.1. Análise dos Resultados	332
9.5.2. Definição e Aplicação de Métricas	335
9.6 Vantagens do Modelo	335
9.7. Conclusões	337
Referências bibliográficas	338

10 Conclusões.....	341
10.1. Resultados.....	341
10.2. Contributos Organizacionais do Modelo	343
10.3. Tendências de Evolução e Trabalhos Futuros.....	344
10.3.1. Tendências de Evolução da Segurança da Informação	344
10.3.2. Trabalhos Futuros	346
10.4. Conclusões Finais.....	348
Referências bibliográficas	351
Bibliografia	353
Índice Remissivo	373

Índice de Figuras

Figura 1.1 – Definição do projecto.....	18
Figura 1.2 – Estrutura do trabalho.....	20
Figura 3.1 – Componentes fundamentais de uma organização	90
Figura 3.2 – Contexto informacional	94
Figura 3.3 – Esquema básico de um sistema.....	99
Figura 3.4 – Adequação estratégica	104
Figura 4.1 – Desafio da segurança da informação	121
Figura 4.2 – Envoltórios da segurança da informação	122
Figura 4.3 – Integração da estratégia dos SGSI na estratégia da organização	132
Figura 5.1 – O indivíduo como um sistema processador de informação	140
Figura 5.2 – Modelo de Aceitação das Tecnologias	143
Figura 7.1 – Ciclo de Vida de Desenvolvimento de Sistemas	197
Figura 7.2 – Ciclo de Vida de Desenvolvimento de Sistemas (modelo reduzido).....	198
Figura 7.3 – Modelo de interacção das normas.....	201
Figura 7.4 – Modelo PDCA	217
Figura 7.5 – Base do MIDImOS	220
Figura 7.6 – Esquema conceptual do MIDImOS	222
Figura 7.7 – MIDImOS - Iniciação e Planeamento.....	223
Figura 7.8 – MIDImOS - Concepção e Desenvolvimento	224
Figura 7.9 – MIDImOS - Implementação e Teste.....	225
Figura 7.10 – MIDImOS - Operação, Manutenção e Optimização.....	226
Figura 8.1 – Fluxograma do modelo A de questionário.....	244
Figura 8.2 – Fluxograma do modelo B de questionário	245
Figura 8.3 – Fluxograma do modelo C de questionário	246

Índice de Quadros

Quadro 8.1 – Segurança do computador pessoal na perspectiva dos Docentes	266
Quadro 8.2 – Segurança do computador pessoal na perspectiva dos Não Docentes.....	267
Quadro 8.3 – Segurança do computador pessoal na perspectiva dos Técnicos.....	267
Quadro 8.4 – Avaliação das mudanças na perspectiva dos Docentes	269
Quadro 8.5 – Avaliação das mudanças na perspectiva dos Não Docentes	270
Quadro 8.6 – Avaliação das mudanças na perspectiva dos Técnicos.....	270
Quadro 8.7 – Avaliação dos conhecimentos em informática	272
Quadro 8.8 – Grau de segurança da <i>password</i>	275
Quadro 8.9 – Grau de participação na elaboração/alteração das políticas de segurança.....	281
Quadro 8.10 – Percepção dos Docentes acerca da facilidade de acesso ao sistema.....	284
Quadro 8.11 – Percepção dos Não Docentes acerca da facilidade de acesso ao sistema	284
Quadro 8.12 – Percepção dos Técnicos acerca da facilidade de acesso ao sistema	285
Quadro 8.13 – Percepção dos Docentes acerca da segurança do sistema	288
Quadro 8.14 – Percepção dos Não Docentes acerca da segurança do sistema.....	288
Quadro 8.15 – Percepção dos Técnicos acerca da segurança do sistema.....	289
Quadro 8.16 – Percepção dos Docentes acerca de aspectos relevantes para a segurança da informação	290
Quadro 8.17 – Percepção dos Não Docentes acerca de aspectos relevantes para a segurança da informação	290
Quadro 8.18 – Percepção dos Técnicos acerca de aspectos relevantes para a segurança da informação	291
Quadro 8.19 – Percepção dos Docentes acerca dos impactos das ameaças na segurança da informação	292
Quadro 8.20 – Percepção dos Não Docentes acerca dos impactos das ameaças na segurança da informação	293
Quadro 8.21 – Percepção dos Técnicos acerca dos impactos das ameaças na segurança da informação	294
Quadro 8.22 – Formação na utilização do Sistema Informático	296
Quadro 8.23 – Documentos acerca da utilização do Sistema Informático.....	297
Quadro 8.24 – Percepção dos Docentes acerca da utilização e aprendizagem do Sistema Informático.....	298
Quadro 8.25 – Percepção dos Não Docentes acerca da utilização e aprendizagem do Sistema Informático	299
Quadro 8.26 – Percepção dos Técnicos acerca da utilização e aprendizagem do Sistema Informático.....	299
Quadro 8.27 – Percepção dos Docentes acerca de aspectos relevantes para a usabilidade.....	300
Quadro 8.28 – Percepção dos Não Docentes acerca de aspectos relevantes para a usabilidade	300
Quadro 8.29 – Percepção dos Técnicos acerca de aspectos relevantes para a usabilidade	301

Índice de Tabelas

Tabela 6.1 – Exemplos de medições de confidencialidade, integridade e disponibilidade	179
Tabela 6.2 – Exemplos de possíveis métricas	181
Tabela 7.1 – Controlos para o referencial β ‘Aceitação e Desempenho’	190
Tabela 7.2 – Controlos para o referencial β ‘Activos Organizacionais’	190
Tabela 7.3 – Controlos para o referencial β ‘Ameaças e Violações de Segurança’	190
Tabela 7.4 – Controlos para o referencial β ‘Envolvimento das Pessoas’	191
Tabela 7.5 – Controlos para o referencial β ‘Estratégia Organizacional e Especificação de Requisitos’	191
Tabela 7.6 – Controlos para o referencial β ‘Formação’	191
Tabela 7.7 – Controlos para o referencial β ‘Mudanças nos SI e/ou nas TIC’	192
Tabela 7.8 – Controlos para o referencial β ‘Política de Segurança da Informação’	192
Tabela 7.9 – Controlos para o referencial β ‘Usabilidade dos SI e das TIC’	192
Tabela 7.10 – Referenciais β para resposta à principal questão do trabalho	193
Tabela 7.11 – Controlos para o referencial γ ‘Ameaças e Violações da Segurança’	194
Tabela 7.12 – Controlos para o referencial γ ‘Avaliação e Auditorias’	194
Tabela 7.13 – Controlos para o referencial γ ‘Gestão de Acessos’	194
Tabela 7.14 – Controlos para o referencial γ ‘Gestão dos Activos’	195
Tabela 7.15 – Controlos para o referencial γ ‘Política de Segurança da Informação’	195
Tabela 7.16 – Controlos para o referencial γ ‘Sensibilização, Treino e Educação’	195
Tabela 7.17 – Controlos para o referencial γ ‘Utilização dos Activos’	195
Tabela 7.18 – Referenciais γ para resposta à principal questão do trabalho	196
Tabela 7.19 – Controlos da norma BS ISO/IEC 17799 <i>versus</i> Questões de partida	203
Tabela 7.20 – Controlos da norma BS ISO/IEC 27001 <i>versus</i> Questões de partida	204
Tabela 7.21 – Controlos da norma NIST SP800-12 <i>versus</i> Questões de partida	204
Tabela 7.22 – Controlos da norma ISO/IEC 21827 <i>versus</i> Questões de partida	205
Tabela 7.23 – Controlos da norma NIST SP800-14 <i>versus</i> Questões de partida	205
Tabela 7.24 – Controlos da norma NIST SP800-18 <i>versus</i> Questões de partida	206
Tabela 7.25 – Controlos da norma COBIT <i>versus</i> Questões de partida	206
Tabela 7.26 – Controlos da norma GAISP <i>versus</i> Questões de partida	207
Tabela 7.27 – Controlos da norma OECD <i>versus</i> Questões de partida	207
Tabela 7.28 – Controlos da norma ISSAF <i>versus</i> Questões de partida	207
Tabela 7.29 – Controlos da norma the Standard <i>versus</i> Questões de partida	208
Tabela 7.30 – Controlos para o referencial α ‘Aceitação do SI e/ou do SGSI’	209
Tabela 7.31 – Controlos para o referencial α ‘Documentos das Políticas de Segurança’	209
Tabela 7.32 – Controlos para o referencial α ‘Avaliação e Auditorias’	210
Tabela 7.33 – Controlos para o referencial α ‘Gestão de Acessos’	210

Tabela 7.34 – Controlos para o referencial α ‘Gestão dos Activos’	211
Tabela 7.35 – Controlos para o referencial α ‘Leis, Regulamentos e Políticas’	211
Tabela 7.36 – Controlos para o referencial α ‘Métricas e Testes’	212
Tabela 7.37 – Controlos para o referencial α ‘Monitorização e Revisão da Segurança da Informação e/ou do SGSI’	212
Tabela 7.38 – Controlos para o referencial α ‘Mudanças no SI e/ou no SGSI’	213
Tabela 7.39 – Controlos para o referencial α ‘Política de Segurança da Informação’	213
Tabela 7.40 – Controlos para o referencial α ‘Responsabilidades, Papéis e Obrigações do Pessoal’	214
Tabela 7.41 – Controlos para o referencial α ‘Sensibilização, Treino e Educação’	215
Tabela 7.42 – Referenciais α para resposta à principal questão do trabalho	216
Tabela 7.43 – PDCA-Plan <i>versus</i> SDLC-Iniciação	218
Tabela 7.44 – PDCA-Do <i>versus</i> SDLC-Desenvolvimento	218
Tabela 7.45 – PDCA-Check <i>versus</i> SDLC-Implementação	218
Tabela 7.46 – PDCA-Act <i>versus</i> SDLC-Operação e Manutenção	218
Tabela 8.1 – Alterações às questões dos questionários	241
Tabela 8.2 – Questões do grupo C dos questionários acerca do ‘Funcionamento e Mudanças no Sistema Informático’ <i>versus</i> Referenciais MIDImOS	248
Tabela 8.3 – Questões do grupo C dos questionários acerca dos ‘Conhecimentos e Formação em Informática’ <i>versus</i> Referenciais MIDImOS	248
Tabela 8.4 – Questões do grupo C dos questionários acerca da ‘Password e Mecanismos de Acesso ao Sistema Informático’ <i>versus</i> Referenciais MIDImOS	249
Tabela 8.5 – Questões do grupo C dos questionários acerca da ‘Utilização do Correio Electrónico’ <i>versus</i> Referenciais MIDImOS	249
Tabela 8.6 – Questões do grupo C dos questionários acerca do ‘Acesso e Utilização do Sistema Informático’ <i>versus</i> Referenciais MIDImOS	250
Tabela 8.7 – Questões do grupo D dos questionários acerca das ‘Políticas de Segurança da Informação e do Sistema Informático’ <i>versus</i> Referenciais MIDImOS	250
Tabela 8.8 – Questões do grupo D dos questionários acerca dos ‘Mecanismos de Protecção do Sistema Informático’ <i>versus</i> Referenciais MIDImOS	251
Tabela 8.9 – Questões do grupo D dos questionários acerca da ‘Realização de Cópias de Segurança’ <i>versus</i> Referenciais MIDImOS	251
Tabela 8.10 – Questões do grupo D dos questionários acerca da ‘Percepção da Facilidade de Acesso ao Sistema Informático’ <i>versus</i> Referenciais MIDImOS	251
Tabela 8.11 – Questões do grupo D dos questionários acerca da ‘Controlo dos Activos do Sistema e da sua Utilização’ <i>versus</i> Referenciais MIDImOS	252
Tabela 8.12 – Questões do grupo D dos questionários acerca da ‘Percepção da Segurança do Sistema Informático’ <i>versus</i> Referenciais MIDImOS	252
Tabela 8.13 – Questões do grupo E dos questionários acerca da ‘Formação na Utilização do Sistema’ <i>versus</i> Referenciais MIDImOS	253
Tabela 8.14 – Questões do grupo E dos questionários acerca da ‘Facilidade de Utilização e Aprendizagem do Sistema’ <i>versus</i> Referenciais MIDImOS	253

Tabela 8.15 – Controlo dos questionários	255
Tabela 8.16 – Questões acerca da identificação/caracterização do(a) inquirido(a)	256
Tabela 8.17 – Questões acerca da existência e partilha de computador pessoal	259
Tabela 8.18 – Questões acerca do acesso à Internet com o computador pessoal	260
Tabela 8.19 – Questões acerca da utilização de password no computador pessoal	261
Tabela 8.20 – Questões acerca da utilização de mecanismos de protecção	262
Tabela 8.21 – Questões acerca da realização de cópias de segurança.....	263
Tabela 8.22 – Questões acerca da utilização do computador pessoal	264
Tabela 8.23 – Questões acerca da classificação de aspectos de segurança do computador pessoal.....	266
Tabela 8.24 – Questões acerca do funcionamento e mudanças no sistema informático	268
Tabela 8.25 – Questões acerca dos conhecimentos e formação em informática.....	271
Tabela 8.26 – Questões acerca da <i>password</i> e mecanismos de acesso ao sistema informático.....	273
Tabela 8.27 – Questões acerca da utilização do correio electrónico.....	275
Tabela 8.28 – Questões acerca do acesso e utilização do sistema informático	277
Tabela 8.29 – Questões acerca das políticas de segurança da informação e do sistema informático.....	280
Tabela 8.30 – Questões acerca dos mecanismos de protecção do sistema informático	281
Tabela 8.31 – Questões acerca da realização de cópias de segurança.....	282
Tabela 8.32 – Questões acerca do controlo dos activos do sistema e da sua utilização	285
Tabela 8.33 – Questões acerca da percepção da segurança do sistema informático	287
Tabela 8.34 – Questões acerca da formação na utilização do sistema	295
Tabela 9.1 – Tópicos do grupo B do questionário	308
Tabela 9.2 – Tópicos do grupo C do questionário	311
Tabela 9.3 – Tópicos do grupo D do questionário	314
Tabela 9.4 – Tópicos do grupo E do questionário.....	318
Tabela 9.5 – Itens relevantes na Questão 1 <i>versus</i> Impactos na actividade das Pessoas.....	329
Tabela 9.6 – Itens relevantes na Questão 2 <i>versus</i> Impactos na actividade das Pessoas.....	329
Tabela 9.7 – Itens relevantes na Questão 3 <i>versus</i> Impactos na actividade das Pessoas.....	330
Tabela 9.8 – Aplicação dos referenciais MIDImOS na Questão 1.....	333
Tabela 9.9 – Aplicação dos referenciais MIDImOS na Questão 2.....	334
Tabela 9.10 – Aplicação dos referenciais MIDImOS na Questão 3.....	334

Siglas

Neste trabalho são utilizadas abreviaturas de designações comuns, e também de organizações e de normativos assim referenciados a nível internacional, apresentando-se cada uma delas a quando da sua primeira utilização. As siglas utilizadas são:

BS – <i>British Standard</i>	PIPEDA – <i>Personal Information Protection and Electronic Documents Act</i>
BSI – <i>British Standard Institution</i>	PNSI – Política Nacional de Segurança da Informação
BSI – <i>Bundesamt für Sicherheit in der Informationstechnik</i>	SDLC – <i>System Development Life Cycle</i>
CISP – <i>Cardholder Information Security Program</i>	SGSI – Sistemas de Gestão da Segurança da Informação
CNPD – Comissão Nacional de Protecção de Dados	SI – Sistemas de Informação
COBIT – <i>Control Objectives for Information and related Technology</i>	SIBC – Sistemas de Informação Baseados em Computadores
ENSI – Estrutura Nacional de Segurança da Informação	SOX – <i>Sarbanes-Oxley Act</i>
FRISCO – <i>Framework of Information Systems Concepts</i>	SSE-CMM – <i>Systems Security Engineering - Capability Maturity Model</i>
FISMA – <i>Federal Information Security Management Act</i>	TAM – <i>Technology Acceptance Model</i>
GAISP – <i>Generally Accepted Information Security Principles</i>	TI – Tecnologias de Informação
HIPAA – <i>Health Insurance Portability and Accountability Act</i>	TIC – Tecnologias de Informação e Comunicação
IEC – <i>International Electrotechnical Commission</i>	UMIC – Unidade de Missão Inovação e Conhecimento
IPS – Instituto Politécnico de Setúbal	UMIC, I.P. – UMIC-Agência para a Inovação e o Conhecimento, I.P.
ISO – <i>International Standard Organization</i>	
ISSAF – <i>Information Systems Security Assessment Framework</i>	
ITIL – <i>Information Technology Infrastructure Library</i>	
MIDImOS – Modelo de Iniciação, Desenvolvimento, Implementação e Optimização da Segurança	
NIST – <i>National Institute of Standards and Technology</i>	
OECD – <i>Organisation for Economic Co-operation and Development</i>	
PDCA – <i>Plan-Do-Check-Act</i>	

1

Introdução

As preocupações com a segurança dos Sistemas de Informação (SI) cresceram exponencialmente com os efeitos da globalização nas sociedades, comportando riscos acrescidos para as organizações que, ao apostarem nos mercados surgidos com a utilização ampla das vias de comunicação digitais, se confrontam com a necessidade de assegurar a confidencialidade, integridade e disponibilidade da informação resultante dos contactos com os seus diversos parceiros.

Os aspectos relacionados com a segurança da informação suportada pelos referidos SI necessitam de ser identificados e avaliados de modo a ser possível garantir essa mesma segurança.

Uma das principais referências neste contexto são as Pessoas, devido essencialmente ao facto de serem identificados habitualmente como o elo mais fraco da segurança nos SI, onde deve ser tido em consideração que as Pessoas desempenham papéis fundamentais no contexto organizacional e são o motivo base para a sua existência, questionando-se assim se constituem ou não o seu elo mais forte.

Neste âmbito, considera-se que o papel das Pessoas no contexto da segurança da informação sobressai com especial relevância quando se assume que a informação constitui um dos activos fundamentais para as organizações e pode condicionar o desempenho nas suas diversas actividades.

1.1. Objectivos

A definição dos objectivos de um trabalho deste âmbito será desde início condicionada por um conjunto de pressupostos, muitos deles insuficientemente validados, que permitam definir uma estrutura base para suportar o arranque do processo de investigação, de modo a que este, no seu desenvolvimento, possibilite a validação dos referidos pressupostos.

No conjunto de pressupostos a ter em atenção constarão certamente a importância da informação, dos SI e das Tecnologias de Informação e Comunicação (TIC) que suportam a sua utilização, a percepção¹ das Pessoas (utilizadores actuais ou potenciais dos sistemas² organizacionais) acerca da informação que utilizam e respectiva segurança, assim como a forma de utilização dos SI e das TIC nas suas actividades pessoais, organizacionais e sociais.

Um dos objectivos deste trabalho é encontrar referenciais³ que permitam assegurar a privacidade da informação, sem que para tal se descure a sua partilha entre os parceiros de negócio, particularmente quando se adoptam políticas de segurança, políticas estas entendidas como a declaração do que é ou não permitido [Bishop 2002], e que descrevem a segurança em termos gerais [Barman 2002], facto pelo qual constituem a base de qualquer esforço de segurança [Peltier 2002].

Outro dos objectivos do trabalho reside na necessidade de garantir que os referenciais (como base do Modelo a desenvolver) a utilizar, ao facilitar a adopção de políticas de segurança da informação suportada nos SI organizacionais, potenciem o conjunto de actividades fundamentais para assegurar que os SI sejam fáceis de aprender e de utilizar, ou seja, que tenham uma usabilidade⁴ elevada.

Pretende-se ainda, perante a relevância das Pessoas nas organizações, não só garantir que os Sistemas de Gestão da Segurança da Informação (SGSI), implementados ou a implementar nas organizações, respondam às suas necessidades e anseios, como também que atendam à manutenção ou melhoria da confidencialidade, disponibilidade e integridade da informação pessoal e organizacional.

Neste contexto, caracterizado essencialmente pela diversidade de informação com que as Pessoas e as organizações têm de lidar, garantir a privacidade da informação pertinente para as actividades organizacionais, conduz à necessidade de assegurar a

¹ Uma ideia, uma crença ou uma imagem que se tem com resultado de como se vê ou entende algo [OxfDic 2005].

² A referência a sistemas ou a sistemas organizacionais, que podem corresponder a artefactos distintos, será entendida no contexto deste trabalho como relativa aos SI, a não ser nos casos especificados onde outra definição possa decorrer das citações efectuadas.

³ Parâmetros ou tópicos utilizados como referências orientadoras para aplicação prática do Modelo a desenvolver.

⁴ Definida essencialmente como facilidade de aprendizagem e de utilização (este termo será objecto de uma definição mais apropriada no capítulo 4).

segurança dessa mesma informação, dos seus suportes e das actividades e recursos associados à sua utilização.

A concepção de um Modelo para suporte das actividades associadas à segurança da informação emerge neste âmbito como um aspecto essencial para validação das componentes afectadas pela implementação de políticas de segurança (englobadas no SGSI), nomeadamente as Pessoas, a informação, os SI e as TIC.

Pretende-se assim definir um conjunto de parâmetros (caracterizados como padrões e/ou métricas) que, integrados num Modelo que atenda à segurança dos SI, permitam uma aferição posterior da segurança desses sistemas após implementação de SGSI, que tenham em atenção os utilizadores da informação organizacional, particularmente nos aspectos directamente relacionados com a sua percepção acerca das alterações nos SI e da segurança proporcionada.

No enquadramento com as definições estabelecidas, procura-se a instituição de uma base de expansão do caso de estudo que permita a aplicação prática do Modelo nas organizações, utilizando para isso os dados empíricos obtidos no estudo de forma a suportar o desenvolvimento dos SGSI de forma integrada e sustentada, onde o papel das Pessoas nessas actividades permita o sucesso das organizações nos processos associados à segurança da informação.

Perante este mesmo contexto, considerar-se-à ainda a emergência das novas TIC, em particular a sua utilização, não apenas nas actividades organizacionais mas também o impacto nas Pessoas e no seu desempenho quando são implementados e utilizados os já referidos SGSI.

1.2. Motivações

A informação, nos seus diversos formatos e suportes, sempre desempenhou e continuará a desempenhar um papel crucial nas actividades humanas, suportando frequentemente a satisfação de parte substancial das suas necessidades, condicionada pelo quando e como é utilizada para suprir essas necessidades.

Desde os primórdios da civilização humana, quando a utilização da informação era feita de forma rudimentar, a partilha de informação registava-se apenas entre os familiares mais próximos (membros das famílias, clãs ou tribos) e tinha essencialmente a ver com

os aspectos de segurança física dos membros da respectiva comunidade e com a sua alimentação, ou seja, visava quase exclusivamente a satisfação das necessidades mais básicas, no sentido se assegurar a respectiva sobrevivência.

A evolução das sociedades (sedentarização, relações com Pessoas externas às suas comunidades, evolução tecnológica, crescimento populacional, melhores condições de vida, de entre uma diversidade de aspectos) trouxe a necessidade de especialização, levando a que a partilha de informação também se passasse a fazer entre mestres e aprendizes, onde apenas alguns eleitos dispunham da informação necessária ao desempenho do conjunto de actividades que se foram tornando essenciais às sociedades.

Constata-se assim que a relevância da informação para as necessidades humanas tem sido um factor fundamental ao longo do processo evolutivo, marcado pelo que Toffler [1984] identificou como sendo a primeira (revolução agrícola) e a segunda (revolução industrial) vagas cujos tempos de desenvolvimento e de duração são cada vez menores, mas a assumpção plena desse facto apenas foi feita nas últimas décadas, mercê do contributo proporcionado pela evolução das TIC, que possibilitaram saltos qualitativos e quantitativos na aquisição, tratamento e partilha da informação.

Todavia, se a informação sempre foi fundamental para as Pessoas e para as organizações, assim como para as sociedades onde se inserem, o que mudou na actualidade foi a forma como essa informação passou a ser encarada, notando-se diferenças substanciais na sua partilha e na relevância que assume nas actividades humanas, e na forma como vai afectando e forçando mudanças nessas mesmas actividades.

Actualmente, perante a evolução tecnológica verificada, em particular em termos de TIC, os desafios que se colocam às Pessoas, às sociedades e às organizações leva a que as necessidades de informação assumam aspectos críticos que urge resolver, nomeadamente, mais informação, melhores acessos e mais Pessoas/organizações envolvidas.

Este crescimento da importância da informação conduziu a um tipo de problema que até aqui tinha sido descurado – a segurança (protecção) da informação – essencialmente porque a partilha de informação se registava apenas por interacções pessoais, ou seja,

através das actividades dos SI informais⁵, geralmente fora do controlo organizacional directo devido à sua dependência quase exclusiva das atitudes e comportamento pessoais.

Neste contexto de relevância das Pessoas nas actividades organizacionais, as suas capacidades e competências na aplicação dos SI e das TIC, a facilidade de aprendizagem e utilização dos sistemas organizacionais vai influenciar o seu sucesso e o desempenho das organizações onde se inserem, exigindo novas formações e competências e, conseqüentemente o apoio adequado dos responsáveis organizacionais.

A problemática da segurança da informação, e simultaneamente dos SI que a suportam, relaciona-se em primeiro lugar com as questões de poder institucional pois quem a detêm a informação está mais perto do poder, e depois relaciona-se também com o facto de um elevado número de organizações entender a informação como um factor crítico de sucesso, levando a que a sua posse e o seu conhecimento seja mantido a todo o custo.

Neste contexto, considerando a afirmação corrente de que “informação é poder”, Herrmann [2002] assume a verdade da afirmação devido ao facto de a informação conduzir a tomadas de decisão informadas e suportadas em conhecimento desde que correctamente integrada, analisada e sintetizada. Todavia, a autora menciona ainda que para a informação ser ‘poder’ é necessário que esta seja precisa, correcta e actual, exigindo que a sua aquisição, manipulação, armazenamento e partilha seja efectuada de forma segura.

Contudo, se a evolução verificada nas TIC comportou por um lado maiores facilidades de aquisição, tratamento e disponibilização de informação também comportou por outro lado que um maior número de Pessoas e organizações tivessem um acesso fácil e rápido à informação, independentemente da sua quantidade, qualidade, utilidade e adequabilidade.

Esta maior disponibilidade de informação, e simultaneamente de meios para a utilizar, comportou então problemas acrescidos às organizações e às Pessoas, transformando a necessidade de segurança da informação numa obrigatoriedade, em particular nas organizações que assumem a informação como essencial à sua actividade de negócio.

⁵ Baseados essencialmente nas pessoas e nas relações que estas estabelecem entre elas, sem recurso a qualquer formalismo expresso.

Controlar os acessos à informação, garantindo que se mantêm a sua confidencialidade, integridade e disponibilidade, traduz-se num factor fundamental cuja pertinência está directamente relacionada com o grau de relevância que a informação possui em concreto para cada organização.

A introdução dos SI e das TIC nas organizações e a sua utilização para suportar as actividades de negócio traduziu-se então num conjunto de desafios e exigências com que as organizações se viram confrontadas, e cujas respostas dependem da cultura organizacional e das Pessoas que as constituem.

Perante a constatação da relevância da informação e das Pessoas, encontra-se motivação para o desenvolvimento de um Modelo que permita a definição de referenciais adequados a propiciar uma identificação das melhores políticas de segurança da informação para uma organização, e a respectiva validação e medição considerando os factores relacionados com as Pessoas, com os SI e as TIC e as respectivas interacções nas envolventes organizacionais.

1.3. Enquadramento

A importância da informação, para as actividades das Pessoas, das organizações e das sociedades, reveste-se de formas distintas em função do estado de desenvolvimento das instituições⁶ e de como são envolvidos os activos das organizações na utilização da informação.

De forma similar, também os países, em função dos seus próprios interesses, definem as políticas, em termos de utilização dos SI e das TIC, e respectivas facilidades de acesso, que consideram essenciais para o seu desenvolvimento, com a sua frequente adequação às necessidades da população e à garantia da sua segurança e privacidade.

O actual desenvolvimento em termos das TIC tem potenciado uma ampla difusão e utilização da informação, permitindo o aparecimento de novos mercados e impondo novas necessidades e competências no âmbito do que surge definido como uma

⁶ A não ser em casos devidamente explicitados ou decorrentes de citações de autores, o termo ‘organização’ será utilizado considerando toda a sua abrangência, substituindo os termos ‘instituição’, ‘empresa’ e outros com o mesmo significado.

Sociedade da Informação, referenciada por muitos autores como também do Conhecimento.

Com a inevitabilidade da Sociedade da Informação, entende-se que devem ser considerados os seus potenciais impactos nas Pessoas, nas organizações e nas sociedades, e como tal abordadas todas as envolventes.

Relativamente às opções assumidas em Portugal no âmbito da Sociedade da Informação, constata-se o desenvolvimento de diversas actividades tendentes a colocar esta problemática nas principais opções de desenvolvimento do país, assumindo-a como um eixo estratégico para a construção do futuro.

Neste contexto, refira-se a criação da Unidade de Missão Inovação e Conhecimento (UMIC), na dependência da Presidência do Conselho de Ministros, com o objectivo fundamental de definir “uma visão estratégica global que associe o desenvolvimento da sociedade da informação aos principais desafios da sociedade portuguesa” [UMIC 2002], constitui o reconhecimento da importância da informação para o desenvolvimento do país.

Esta estrutura, criada para substituir a Missão para a Sociedade da Informação (primeira estrutura nacional criada especificamente para responder aos desafios colocados pela emergência da Sociedade da Informação), dando continuidade ao trabalho até então realizado, tem contribuído para a concretização de diversas iniciativas tendentes a suportar as políticas portuguesas no âmbito da Sociedade da Informação.

De entre as iniciativas da UMIC, referenciam-se o ‘Plano de Acção para a Sociedade da Informação: Uma nova Dimensão de Oportunidades’, que “pretende ser o principal instrumento de coordenação estratégica e operacional das políticas para o desenvolvimento da Sociedade da Informação em Portugal” [UMIC 2003a], e o ‘e-U Campus Virtual’ que envolve a disponibilização de serviços, conteúdos, aplicações e comunicações móveis para estudantes e professores do Ensino Superior, incentivando a produção, acesso e partilha de Conhecimento [UMIC 2003b].

A UMIC passou posteriormente a ser designada como UMIC – Agência para a Sociedade do Conhecimento, I.P., (UMIC-I.P.), tendo esta sido criada pelo Decreto-Lei n.º 16/2005, de 18 de Janeiro, assumindo como missão “o planeamento, a gestão, a coordenação e o desenvolvimento de projectos nas áreas da sociedade da informação e

governo electrónico”, com os seus estatutos a serem aprovados pela Portaria n.º 205/2005, de 21 de Fevereiro.

Posteriormente, o Decreto-Lei n.º 153/2007, de 27 de Abril, na sequência da aprovação da Lei Orgânica do Ministério da Ciência, Tecnologia e Ensino Superior, aprova uma nova orgânica, definindo a sua missão como mobilizadora da “Sociedade da Informação através da promoção de actividades de divulgação, qualificação e investigação”. Os novos estatutos da UMIC-I.P. foram aprovados pela Portaria n.º 551/2007, de 30 de Abril.

Por outro lado, quando a segurança da informação constitui um importante aspecto a considerar no contexto imposto pela Sociedade da Informação, torna-se crucial o estabelecimento de um enquadramento adequado à sua definição, implementação, operacionalização e monitorização, que envolva tanto quanto possível todos os legitimamente interessados neste tipo de actividades.

Todavia, o grau de sucesso deste tipo de actividade depende não só do Estado como entidade dinamizadora e reguladora, mas também de todos os intervenientes nos processos onde está em causa a segurança da informação, pessoal ou organizacional, e de todos os recursos que se encontram associados à recolha, tratamento, armazenamento, controlo e disponibilização de informação.

Neste mesmo contexto, a Estrutura Nacional de Segurança da Informação (ENSI), definiu em Fevereiro de 2005 a Carta de Segurança da Informação, constituindo esta o documento de topo da ENSI de Portugal. Esta Carta apresenta a visão da missão de toda a ENSI, onde todos os documentos, arquitecturas, processos e estruturas de segurança que fazem parte da ENSI devem estar em conformidade com esta Carta de Segurança da Informação [ENSI 2005a].

A existência de uma Estrutura de âmbito nacional, e respectivos documentos, definida para a segurança da informação reforça a pertinência desta temática, levando a que a mesma seja impreterivelmente considerada pelas organizações.

Os habituais receios acerca da segurança, muitas deles provavelmente decorrentes do desconhecimento dos principais aspectos envolvidos, permitem supor que as organizações que aderiram em primeiro lugar pertençam ao Estado ou com ele tenham contactos estreitos, ou então organizações de âmbito internacional, onde a atenção para

com o normativo de segurança e a legislação relacionada é já parte integrante da sua cultura.

A ENSI foi estabelecida pelo Governo Português no âmbito da Sociedade da Informação, visando a definição de objectivos de segurança e a especificação de uma política de topo para a Segurança da Informação. Nesse sentido, a Carta apresenta os seguintes constituintes [ENSI 2005a]:

- ⇒ Declaração da Missão;
- ⇒ Estratégia;
- ⇒ Objectivos de Segurança;
- ⇒ Estrutura;
- ⇒ Responsabilidades;
- ⇒ Liderança e Supervisão;
- ⇒ Plano de Acção.

Este modelo de enquadramento, implica a especificação de medidas e linhas de acção concretas, destinadas fundamentalmente a conduzir as actividades das Pessoas e das organizações sempre que possa ficar em causa a segurança da informação, independentemente da forma com que se apresente qualquer ameaça a essa mesma segurança. Refira-se por isso a necessidade de considerar não só a utilização dos meios electrónicos como suporte da informação, mas também qualquer outro meio que possa ser utilizado com o mesmo objectivo.

Por isso, no contexto identificado e no âmbito das actividades associadas à ENSI, são definidos sete objectivos relativamente à Segurança da Informação [ENSI 2005a]:

- Objectivo 1 – Proteger as infra-estruturas críticas portuguesas através de medidas eficazes e coordenadas de segurança da informação;
- Objectivo 2 – Assegurar de forma segura a interoperabilidade da infra-estrutura da informação portuguesa, através da aplicação consistente da segurança da informação nos sectores público e privado;
- Objectivo 3 – Melhorar a cultura da segurança da informação nas organizações públicas e privadas e acelerar a sua implementação;

- Objectivo 4 – Promover a pesquisa e melhorar as capacidades de análise de ameaças e vulnerabilidades relativamente à segurança da informação;
- Objectivo 5 – Desenvolver e executar uma infra-estrutura electrónica nacional de autenticação que abranja os sectores público e privado;
- Objectivo 6 – Proteger a privacidade e os interesses pessoais do consumidor na Sociedade da Informação;
- Objectivo 7 – Aumentar a consciência pública relacionada com os requisitos da segurança da informação em Portugal.

Com o objectivo de servir de guia para todas as questões relativas à segurança da informação, foi definida a Política Nacional de Segurança da Informação (PNSI), que estabelece os objectivos de segurança da informação a nível nacional. Esta definição serve como garantia a todos os membros da Sociedade da Informação de que existe um cumprimento efectivo do que foi definido [ENSI 2005b].

Como principais partes constituintes da PNSI [ENSI 2005b] foram definidos:

- ⇒ Objectivos Nacionais para a Segurança da Informação (o que cada membro da Sociedade da Informação pode esperar e contar a nível nacional);
- ⇒ Responsabilidade na Segurança da Informação (quem é responsável pela implementação da segurança da informação no país);
- ⇒ Organização da Segurança da Informação (estrutura definida para a segurança da informação);
- ⇒ Gestão (responsabilidade pelo estabelecimento, controlo e medição, gestão do risco e auditoria da segurança da informação);
- ⇒ Serviços de Segurança da informação (serviços fornecidos a nível nacional e quem os fornece).

Surge assim reforçada a pertinência da segurança da informação no contexto da Sociedade da Informação, e da importância que aquela assume no desenvolvimento desta sociedade em Portugal, enquadrando-se na estratégia de desenvolvimento nacional, estratégia esta consubstanciada no ‘Plano Tecnológico – Uma estratégia de crescimento com base no conhecimento, na tecnologia e na inovação’.

O Plano Tecnológico, aprovado pela Resolução do Conselho de Ministros nº 190/2005, de 24 de Novembro, é um plano de acção para levar à prática um conjunto articulado de políticas que visam estimular a criação, a difusão, a absorção e o uso do conhecimento como alavanca para transformar Portugal numa economia dinâmica e capaz de se afirmar na economia global [PlanoTec 2005].

Neste contexto de utilização dos SI e das Tecnologias de Informação⁷ (TI), onde a segurança da informação e dos seus suportes é essencial, o eixo 1 (Conhecimento – Qualificar os Portugueses para a Sociedade do Conhecimento) enquadra um conjunto de linhas de actuação de onde se destaca a ‘Mobilizar Portugal para a Sociedade da Informação e do Conhecimento’, na qual é especificada a necessidade de medidas para “Desenvolver uma política de segurança informática”, apresentando como objectivo central a “criação de um contexto favorável à utilização das TIC e da Internet”.

Em termos europeus refira-se a iniciativa *eEurope* (referenciada como ‘*eEurope 2002*’), aprovada pelo Conselho Europeu na sua reunião realizada em Portugal em Junho de 2000, apresentando um plano de acção assente em três objectivos fundamentais a saber:

- (1) Uma Internet mais barata, mais rápida e segura;
- (2) Investir nas Pessoas e nas qualificações;
- (3) Estimular a utilização da Internet.

Com vista à prossecução destes objectivos, foram definidos os seguintes métodos a aplicar:

- Acelerar a criação de um ambiente jurídico adequado;
- Apoiar as novas infra-estruturas e serviços em toda a Europa;
- Aplicar um método aberto de coordenação e avaliação do desempenho.

Esta iniciativa foi posteriormente reforçada (passando a ser referenciada como ‘*eEurope 2005: Uma Sociedade da Informação para todos*’), com um novo plano de acção, aprovado pelo Conselho Europeu na sua reunião realizada em Espanha em Junho de 2002, com o objectivo de proporcionar um ambiente favorável para o investimento privado e para a criação de novos empregos, aumentar a produtividade, modernizar os

⁷ Sendo actualmente ‘tecnologias de informação e comunicação’ o termo mais comum no contexto dos SI, por isso mesmo com utilização preferencial neste trabalho, considera-se também, desde que explicitamente referenciado por qualquer autor ou documento, a utilização do termo ‘tecnologias de informação’, atribuindo-se todavia, neste trabalho, o mesmo significado a ambos os termos.

serviços públicos e proporcionar a todos uma oportunidade de participação na Sociedade de Informação global.

Este plano de acção define dois grupos de actuação: estimular serviços, aplicações e conteúdos, assim como proporcionar uma infra-estrutura de banda larga com elevada disponibilidade, que atendam à necessidade de proporcionar a segurança adequada. Neste sentido, são consideradas as seguintes ferramentas:

- Medidas políticas (revisão e adaptação da legislação nacional e europeia);
- Boas práticas (partilha de experiências);
- Avaliação de desempenhos (apoiar a realização dos objectivos e das políticas de apoio aos mesmos);
- Coordenação global das políticas existentes (garantir sinergias entre as acções propostas).

A continuidade destas iniciativas é assegurada por um novo quadro estratégico (referenciado como ‘i2010 – Sociedade Europeia da Informação 2010’). Esta estratégia, designada como ‘Uma sociedade da informação europeia para o crescimento e o emprego’, “promove uma economia digital aberta e concorrencial e coloca a tónica nas TIC enquanto factor de inclusão e de qualidade de vida”.

Esta iniciativa suporta-se em três prioridades, propostas pela Comissão Europeia, para as políticas europeias da Sociedade da Informação e dos media. São então enquadrados três objectivos concretos:

- Objectivo 1 – Um espaço único europeu da informação que ofereça comunicações de elevada largura de banda, seguras e a um preço acessível, conteúdos ricos e diversificados, e serviços digitais;
- Objectivo 2 – Investigação e inovação de classe mundial nas TIC, aproximando o desempenho da Europa do desempenho dos seus principais concorrentes;
- Objectivo 3 – Uma Sociedade da Informação inclusiva, que ofereça serviços públicos de alta qualidade e promova a qualidade de vida.

Outra iniciativa, mais abrangente, relaciona-se com a declaração de compromisso de criar uma Sociedade da Informação centrada nas Pessoas e com um desenvolvimento orientado para a sua inclusão social, onde cada um possa criar, aceder, utilizar e

partilhar informação e conhecimento, permitindo que Pessoas e comunidades atinjam a totalidade do seu potencial na prossecução de um desenvolvimento sustentável e de melhoria da sua qualidade de vida, “previstas nos propósitos e princípios da Carta das Nações Unidas e no respeito total da Declaração Universal dos Direitos do Homem”, que constitui o foco central do *World Summit of the Information Society* realizado em Geneve em Dezembro de 2003 [WSIS 2003a], não faz mais do que reforçar a emergência de uma sociedade baseada na informação.

Considerando um ponto de vista socioeconómico perante a envolvente estabelecida, Amaral [2007] entende que a “Sociedade da Informação traz um novo modelo de desenvolvimento económico” provocando em simultâneo alterações profundas nos comportamentos, atitudes e valores das estruturas sociais e políticas da actualidade.

Esta Sociedade da Informação na qual vivemos, cada vez mais globalizada e determinada economicamente é, por natureza, fundada em tecnologias digitais, onde a informação como recurso é um bem de mercado [Zorrinho 2001], pelo que, além de ter como principal pilar de sustentação a informação, considerando-a como um dos elementos essenciais da actividade organizacional [Serrano e Fialho 2003], depende também dos sistemas que permitem o seu suporte e partilha, assim como de Pessoas capazes de utilizar esses sistemas em proveito das organizações onde se inserem.

Por outro lado, Almeida [2007] considera que o núcleo de uma Sociedade da Informação é constituído por três componentes fundamentais e pelas suas diferentes inter relações. As três componentes referidas são:

- (1) As Pessoas;
- (2) As TIC;
- (3) Os processos.

Neste contexto de actuação na Sociedade da Informação onde a informação é claramente um recurso crucial, torna-se fundamental que existam mecanismos capazes de garantir a segurança dessa mesma informação, com a segurança a ser entendida como “a capacidade de um sistema para proteger a informação e os seus recursos, no que diz respeito à confidencialidade e integridade” [Ross 1999] ou ainda como o conjunto de operações realizadas para proteger a informação e os SI, assegurando a sua disponibilidade, integridade, autenticação e não repudição [Herrmann 2003].

Esta necessidade de protecção não deve comprometer todavia a facilidade de aprendizagem e utilização desses sistemas, permitindo deste modo que aumente o número de potenciais utilizadores, onde este aspecto é um dos componentes dos princípios chave da referida Cimeira Mundial para a Sociedade da Informação, residindo no aumento da confiança e da segurança no uso das TIC um dos pilares fundamentais da Sociedade da Informação, constituindo a melhoria do acesso às infra-estruturas e tecnologias de comunicação, tal como à informação e ao conhecimento, outro dos principais pilares dessa sociedade [WSIS 2003b].

Neste âmbito, o incremento do número de Pessoas que utilizam a informação e do seu nível de exigência, associado à emergência de um conjunto de novas TIC de que a Internet e os dispositivos móveis são exemplo, tem comportado novas exigências e forçado acrescidas preocupações de segurança relativamente às Pessoas, às tecnologias e à sua interacção nos contextos pessoal, organizacional e social.

Assume-se assim a pertinência da informação para as actividades organizacionais, em particular se for tido em conta o entendimento de que “todas as empresas são empresas de informação” [Earl 2000] e ainda que “o acesso expedito à informação e a rapidez do seu tratamento pode ser um factor crítico de sucesso, se não mesmo de sobrevivência, das organizações” [Faria e Amaral 1998], conduzindo à necessidade de garantir que o seu controlo e protecção se processem de forma adequada.

Estes factores fazem emergir a necessidade de promover, desenvolver e implementar uma cultura global de cibersegurança⁸, num ambiente de cooperação entre todos os interessados, onde é importante garantir a segurança e proporcionar a protecção e privacidade dos dados [WSIS 2003b].

Neste sentido é essencial garantir a segurança do próprio SI e das TIC em que este se suporta, porque a qualidade do suporte prestado e o sucesso das organizações dependem também dos SI implementados, particularmente na sua adequação às necessidades de suporte e partilha de informação, assim como da capacidade das organizações em os utilizarem como forma de apoio às suas actividades.

Perante o reconhecimento de que as TIC estão a mudar progressivamente as práticas de trabalho, é fundamental a criação de um ambiente de trabalho seguro, saudável e digno

⁸ Aspectos de segurança relativos à utilização da *web* e das tecnologias que a suportam.

de confiança que seja apropriado à utilização das TIC, adequando-se às necessidades das Pessoas e das organizações, respeitando as normas nacionais e internacionais. Entende-se assim que as aplicações das TIC devem ser fáceis de usar, acessíveis a todos, passíveis de disponibilizar, adaptadas às necessidades locais em termos de cultura e língua, e capazes de suportar um desenvolvimento sustentável [WSIS 2003b].

Em termos genéricos, como ponto de partida para um adequado enquadramento do problema, torna-se necessário entender que associados à utilização de um SI estão alguns aspectos relevantes relativos à segurança da informação que suportam, nomeadamente:

- As implicações, para a organização e para o SI, de implementar segurança;
- A facilidade de utilização do SI após implementação de segurança;
- O papel das Pessoas na utilização dos SI e das TIC;
- O grau de aceitação das tecnologias implementadas;
- As implicações da segurança para as Pessoas que utilizam o SI;
- A percepção das Pessoas acerca da informação pessoal e organizacional;
- A eficiência e eficácia das políticas de segurança implementadas.

1.4. Abordagem à Investigação

O desenvolvimento do trabalho proposto e a prossecução dos seus objectivos, focalizando-se em actividades que envolvem Pessoas e a sua percepção de adopção de TIC em contextos de utilização dos SI, necessita que a definição da metodologia de investigação a adoptar tenha em atenção os aspectos de natureza social, intrinsecamente complexos e contingenciais, que afectam as Pessoas e são por estas afectadas.

Relativamente ao termo ‘percepção’, Neves [2001] considera-o genericamente “como o processo automático de organizar e estruturar as características oriundas de um conjunto complexo de estímulos num todo interpretável e com significado”.

Estes aspectos podem ser tanto mais críticos quanto afectam o posto de trabalho das Pessoas (ou mesmo as suas funções e estabilidade), ou até a sua percepção das mudanças que se pretendem concretizar. Torna-se assim claro que qualquer alteração a efectuar na organização que afecte o desempenho das Pessoas, deve ter em atenção o seu contributo no processo de mudança, em especial quando se pretendem implementar

SGSI, que, pela sua natureza e abrangência, tem implicações nas actividades humanas e organizacionais.

A investigação a desenvolver necessita de suporte empírico proveniente de áreas distintas (Pessoas, SI, TIC, informação e segurança da informação e dos SI), onde a componente social assume um papel relevante, tal como é proposto no presente trabalho, pelo que se considera que a opção pela abordagem qualitativa é a mais adequada às actividades a concretizar.

Segundo Caldeira e Romão [2002], a perspectiva filosófica do investigador (Positivismo, Realismo, Interpretativismo, etc.), os objectivos da investigação e o objecto de estudo, condicionam a adopção da estratégia de investigação, realçando ainda que a abordagem a utilizar não se encontra dependente da perspectiva filosófica, admitindo-se por isso a utilização dos diferentes métodos em qualquer das perspectivas.

Neste mesmo contexto Macedo *et al* [2005] referem como fundamentais as perspectivas Positivista (realidade é objectiva e independente do observador) e Interpretativista (realidade como resultante da interpretação do observador).

Numa perspectiva comum e amplamente utilizada, a investigação científica suporta-se em duas abordagens: a Quantitativa (quando é possível obter medidas quantificáveis de variáveis a partir de amostras de uma população), utilizada na investigação em ciências naturais e em engenharia, e a Qualitativa (quando o fenómeno que se pretende estudar é complexo e de natureza social), utilizada na investigação em ciências sociais para potenciar o estudo das Pessoas e a sua integração no meio envolvente [Myers 2003].

A transferência da investigação em SI, das suas componentes mais tecnológicas para os aspectos associados à gestão e à organização, contribuiu para aumentar o interesse nos métodos de investigação qualitativa.

A definição da estratégia de investigação terá vantagens e desvantagens específicas e, segundo Yin [1994], depende de três factores: do tipo de questão de investigação; do controlo que o investigador possui sobre os eventos; da focalização dos fenómenos actuais comparativamente com o seu histórico.

A problemática da segurança da informação organizacional coloca-se hoje de forma bastante diferente, comparativamente com o que acontecia à uma década atrás,

particularmente pela emergência de um novo conjunto de TIC que potenciam uma maior partilha dessa mesma informação, assim como maiores facilidades de acesso e utilização, colocando as Pessoas perante novos e mais complexos desafios.

Esta situação ganha relevância quando se considera que as Pessoas percebem as coisas de forma diferenciada, não apenas através da não sofisticação mas devido aos significados serem parcialmente determinados pela sua própria experiência [Stake 1995].

De entre as metodologias de investigação referenciadas por Macedo *et al* [2005], o Estudo de Caso é assumido como a melhor escolha na investigação em SI pela abordagem organizacional que permite no contexto de uma situação real, restringindo-se todavia a uma única organização, o que, segundo os autores dificulta a generalização dos resultados obtidos.

Os mesmos autores referem a Análise de Documentos e os Questionários como técnicas adequadas à metodologia referenciada. Neste sentido, descrevem a primeira delas como compreendendo a recolha, a leitura e a análise de documentos acerca da área de investigação, enquanto que a segunda se suporta na elaboração de perguntas relativas à área de investigação.

Considerando que, segundo Yin [1994], o estudo de casos como estratégia de investigação pode ser aplicado em situações de estudos sociológicos, de gestão e organizacionais, o trabalho proposto será concretizado através de estudos de casos, onde a recolha dos materiais empíricos é suportada pelo estudo de documentos, pela análise da diversa legislação aplicável e do normativo associado à segurança da informação e dos SI e TIC que a suportam, e ainda pela realização de um questionário sobre a temática a investigar.

1.5. Resultados e Contributos

Como resultado mais relevante deste trabalho referencia-se a definição de um Modelo que permita suportar a implementação de políticas de segurança e de SGSI, sem que os seus impactos condicionem as actividades das Pessoas e das organizações onde se inserem, recorrendo essencialmente ao estudo das normas de segurança e à revisão

bibliográfica da área da segurança da informação para sustentar as bases de suporte conceptual do Modelo a desenvolver.

Em termos de contributos, espera-se que este trabalho simplifique as actividades essenciais para suportar a implementação e a utilização de políticas de segurança e de SGSI, sempre que possível com estas actividades a decorrer em simultâneo com o planeamento e desenvolvimento dos SI.

Pretende-se ainda, com o objectivo de simplificar a aplicação do Modelo, proceder à definição de métricas que permitam proceder à validação das políticas de segurança da informação e do SGSI, métricas essas a serem suportadas nos referenciais que constituirão parte fundamental do Modelo.

Perante a criticidade da temática em estudo, segurança da informação, constata-se a escassez de trabalhos publicados que permitam uma sustentação completa de todas as vertentes cuja abordagem é necessária, quer porque a divulgação de informação (de negócio, privada e confidencial) pode afectar a credibilidade da organização, quer porque o seu conhecimento público pode potenciar um incremento do número de ameaças para a segurança da informação pessoal e organizacional.

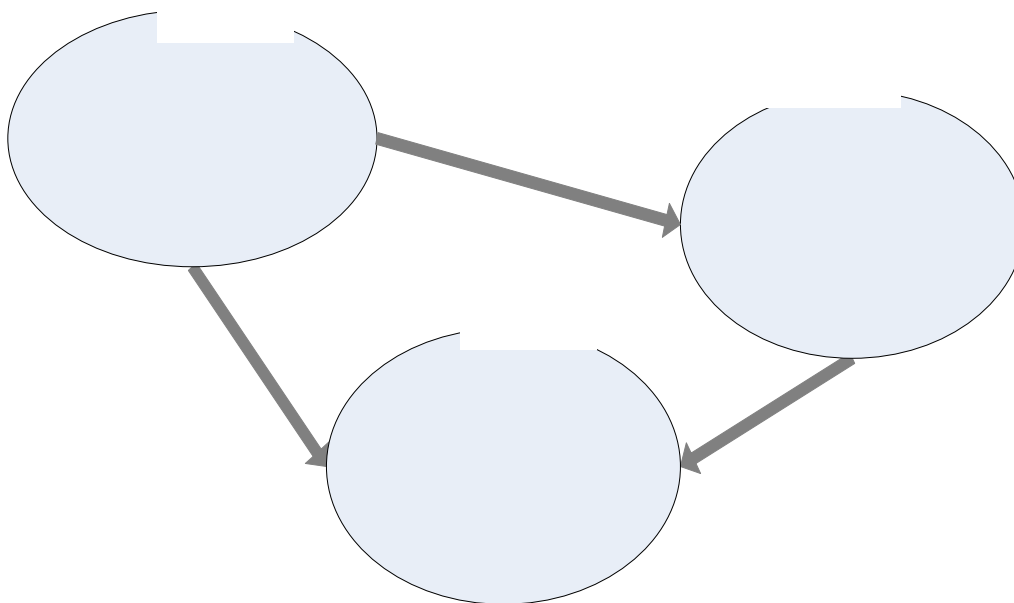


Figura 1.1 – Definição do projecto

Espera-se ainda que este trabalho contribua para incentivar uma maior participação das Pessoas nas actividades relacionadas com a utilização dos SI e das TIC, assumindo a necessidade de considerar as suas preocupações e contributos para uma melhor e mais

adequada utilização desses SI, com a aceitação implícita das políticas de segurança e dos SGSI a utilizar ou utilizadas na organização.

Neste âmbito, procurar-se-à que os seus resultados potenciem um maior envolvimento das Pessoas na aplicação prática do conjunto de recomendações daqui decorrentes para a concepção, implementação, utilização, manutenção e optimização dos SGSI que se pretendam integrar nas organizações, de modo a que os processos de transição se realizem com a minimização dos potenciais impactos nas actividades das Pessoas.

1.6. Estrutura do Trabalho

O presente trabalho estrutura-se em três partes, que agrupam os dez capítulos que o constituem. O que se pode considerar como a primeira parte, engloba os capítulos 1 a 4 e pretende proporcionar o enquadramento dos diferentes aspectos considerados fundamentais para a realização do trabalho (Normas e Legislação, Informação, SI e TIC e Segurança), enquanto que a segunda parte, capítulos 5 a 7, está relacionada com a resolução do problema apresentado (Pessoas, Métricas de Segurança, Criação do Modelo), já a terceira parte, que inclui os capítulos 8 a 10, aborda o Estudo de um Caso, a Validação do Modelo, apresentando-se também as Conclusões do trabalho desenvolvido.

A figura 1.2 apresenta a estrutura anteriormente referenciada, incluindo os principais tópicos associados a cada um dos capítulos mencionados, registando as relações estabelecidas entre os capítulos, procurando uma percepção dos contributos de cada um deles para a sequência de desenvolvimento do trabalho.

O capítulo 1 (**Introdução**) proporciona a definição dos objectivos do trabalho e as principais motivações para a sua realização, efectuando-se também um enquadramento conceptual do problema que se pretende investigar, apresentando-se ainda a abordagem utilizada, e os resultados e contribuições esperadas.

No capítulo 2 (**Enquadramento Normativo e Legal**) proporcionam-se os enquadramentos normativos e legais associados às políticas de segurança e aos sistemas de gestão da segurança da informação.

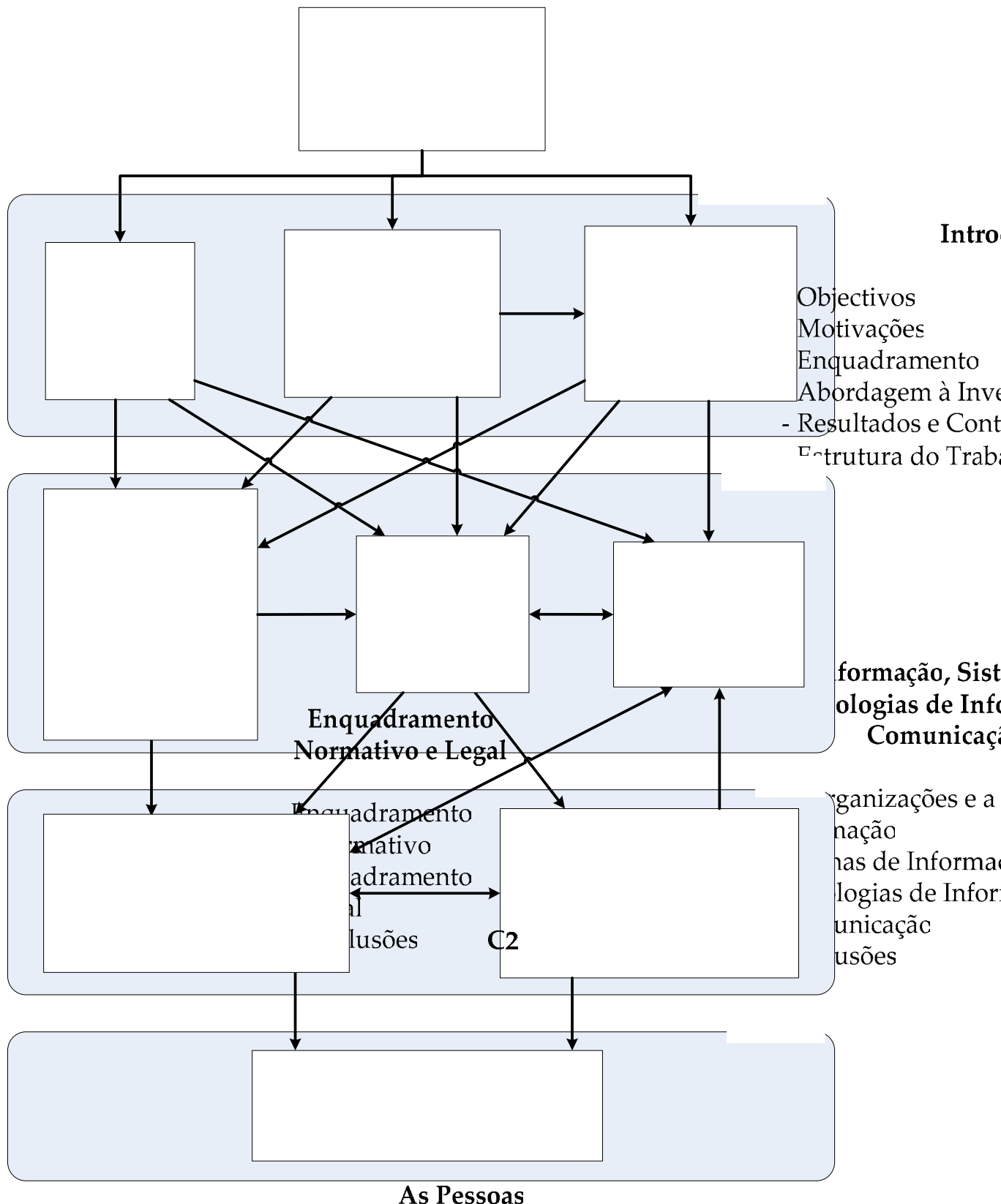


Figura 1.2 – Estrutura do trabalho

Com o capítulo 3 (**Informação, Sistemas e Tecnologias de Informação e Comunicação**) apresenta-se o conjunto de definições fundamentais para suportar o

- As Pessoas e as Tecnologias de Informação e Comunicação
- Caracterização e Tipificação dos Utilizadores
- As Pessoas e a Segurança da

Métricas

- Conceitos
- Tipificação
- Métricas

desenvolvimento do trabalho, nomeadamente acerca de informação, sistemas de informação e tecnologias de informação e comunicação.

O capítulo 4 (**Segurança da Informação**) proporciona a apresentação das definições de segurança da informação e dos sistemas de informação, e ainda as políticas e os sistemas de gestão de segurança da informação. Neste capítulo referencia-se também as implicações da segurança na utilização dos sistemas de informação.

O capítulo 5 (**As Pessoas**) proporciona a caracterização e tipificação dos utilizadores dos sistemas e tecnologias de informação e comunicação, relevando o seu contributo para o desenvolvimento das organizações e simultaneamente a importância do seu papel no contexto da segurança da informação.

O capítulo 6 (**Métricas de Segurança**) proporciona a caracterização e tipificação de métricas de segurança, procurando-se a definição de parâmetros e instrumentos de medição da segurança da informação, assim como a validação e o teste desses parâmetros.

No capítulo 7 (**Criação do Modelo**) definem-se os referenciais suportados na literatura, nas métricas de segurança e as normas normas de segurança, apresenta-se o enquadramento conceptual do problema em estudo, o Modelo nas suas diversas componentes, e as características e vantagens do Modelo proposto.

No capítulo 8 (**Estudo de Caso**) apresenta-se a selecção de casos, a metodologia de análise a ser aplicada enquadrando-se no âmbito do estudo. Apresenta-se ainda a elaboração dos questionários, os resultados dos questionários e os contributos obtidos do caso seleccionado.

O capítulo 9 (**Validação do Modelo**) proporciona a definição dos princípios de estruturação do Modelo, a sua metodologia de aplicação e a respectiva validação, recorrendo aos referenciais estabelecidos pelo Modelo e aos resultados obtidos através da apreciação das respostas aos questionários.

No capítulo 10 (**Conclusões**) apresentam-se os resultados do trabalho, os contributos organizacionais do Modelo. Apresentam-se ainda as tendências de evolução e os trabalhos futuros que podem resultar deste estudo, bem como as conclusões finais do trabalho.

No final de cada capítulo apresentam-se as referências bibliográficas utilizadas directamente em cada um deles. A bibliografia global de suporte ao estudo é apresentada no final deste documento.

Seguidamente, apresenta-se também um índice remissivo para facilitar a consulta do documento.

O presente trabalho é complementado por cinco anexos, referenciados de A a E, cujo conjunto é apresentado num volume separado.

O anexo A (Normativo de Segurança) apresenta a estrutura detalhada de cada uma das normas, enquanto o anexo B (Modelo do Questionário) apresenta cada uma das três versões do questionário final, já o anexo C (Modelo das Instruções de Entrega dos Questionários) apresenta o documento entregue com cada um dos questionários com algumas instruções de entrega dos mesmos, o anexo D (Resultados do Questionário – Grupo de Teste) apresenta um conjunto de tabelas com os resultados das respostas aos questionários entregues pelo grupo de teste, por último o anexo E (Resultados dos Questionários A, B e C) apresenta um conjunto de tabelas com os resultados das respostas aos questionários entregues pelos inquiridos de cada grupo.

Referências bibliográficas

- Almeida, J.M.G., “Controlar o Futuro”, in José Dias Coelho (Coordenador), *Sociedade da Informação – O percurso Português*, Edições Sílabo, 2007, p.189-199.
- Amaral, L.M., “A Sociedade da Informação”, in José Dias Coelho (Coordenador), *Sociedade da Informação – O percurso Português*, Edições Sílabo, 2007, p.85-92.
- Barman, S., *Writing Information Security Policies*, New Riders Publishing, 2002.
- Bishop, M., *Computer Security: Art and Science*, Addison-Wesley Professional, 2002.
- Caldeira, M. e Romão, M., “Estratégias de Investigação em Sistemas de Informação Organizacionais – A utilização de métodos qualitativos”, *Estudos de Gestão – Portuguese Journal of Management Studies*, 3 (1), 2002, p.77-97.
- Earl, M., “Todas as empresas são empresas de informação”, *O Domínio da Informação*, Diário Económico, 2000, p.12-15.

- ENSI, *Carta de Segurança da Informação (Versão 1.0)*, Estrutura Nacional de Segurança da Informação (ENSI), Unidade de Missão Inovação e Conhecimento (UMIC), Fevereiro de 2005.
- ENSI, *Política Nacional de Segurança da Informação (Versão 1.0)*, Estrutura Nacional de Segurança da Informação (ENSI), Unidade de Missão Inovação e Conhecimento (UMIC), Fevereiro de 2005.
- Faria, L. e Amaral, L., “Planeamento da Contingência e Recuperação”, *Revista da Associação Portuguesa de Sistemas de Informação*, 8, 1998, p.43-51.
- Herrmann, D.S., *A Practical Guide to Security Engineering and Information Assurance*, CRC Press, 2002.
- Herrmann, D.S., *Using the Common Criteria for IT Security Evaluation*, Auerbach Publications, 2003.
- Macedo, P., Zacarias, M.S. e Tribolet, J., “Técnicas e Métodos de Investigação em Engenharia Organizacional: Projecto de Investigação em Modelação de Processos de Produção”, Actas (formato digital) da 6ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade do Minho e pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança, Bragança, 26-28 de Outubro de 2005.
- Myers, M., “Qualitative Research in Information Systems”, *MISQ Discovery*, updated version, April 22, 2003, <http://www.qual.auckland.ac.nz> (16-05-2003).
- Neves, J., “Personalidade, Percepção e Aprendizagem”, in J.M. Carvalho Ferreira, José Neves e António Caetano (Editores), *Manual de Psicossociologia das Organizações*, McGrawHill, 2001.
- Parkinson, D. (Editor), *Oxford Business English Dictionary*, Oxford University Press, 2005.
- Peltier, T.R., *Information Security Policies, Procedures, and Standards*, CRC Press, 2002.
- Plano Tecnológico, Presidência do Conselho de Ministros, *Resolução do Conselho de Ministros n.º190/2005*, <http://www.portugal.gov.pt/Portal> (10-02-2006).
- Ross, S., “Computer Security: A practical definition”, 1999, <http://www.albion.com/security> (31-10-2003).
- Serrano, A. e Fialho, C., *Gestão do Conhecimento – O novo paradigma das organizações*, FCA, 2003.
- Stake, R.E., *The Art of Case Study Research*, Sage Publications, 1995.

Toffler, A., *A Terceira Vaga*, Edição Livros do Brasil, 1984.

UMIC, Unidade de Missão Inovação e Conhecimento, Presidência do Conselho de Ministros, *Resolução do Conselho de Ministros n.º 135/2002*, <http://www.unic.gov.pt> (22-01-2004).

UMIC, Unidade de Missão Inovação e Conhecimento, Presidência do Conselho de Ministros, “Plano de Acção para a Sociedade da Informação”, 2003.

UMIC, Unidade de Missão Inovação e Conhecimento, Presidência do Conselho de Ministros, 2003, <http://www.e-u.pt> (22-01-2004).

World Summit on the Information Society, “Declaration of Principles”, WSIS-03/Geneva/Doc/4-e, 12 December, 2003.

World Summit on the Information Society, “Plan of Action”, WSIS-03/Geneva/Doc/5-e, 12 December, 2003.

Yin, R. K., *Case Study Research: Design and Methods*, 2nd edition, Applied Social Research Methods Series. Thousand Oaks: SAGE Publications, 1994.

Zorrinho, C., *Ordem, Caos e Utopia – Contributos para a História do Século XXI*, Editorial Presença, 2001.

2

Enquadramento Normativo e Legal

A utilização dos SI e das TIC, quer ao serviço das Pessoas, das organizações ou mesmo da sociedade, necessita de ser regulamentada, quer através de publicação de legislação adequada a garantir direitos de propriedade, física ou intelectual, e um uso apropriado desses activos. Situação similar, embora sem uma obrigatoriedade legal, verifica-se na utilização de normas e *standards* destinados a facilitar a concepção e implementação de sistemas que potenciem o desempenho das Pessoas e das organizações.

A privacidade da informação pessoal e de negócio necessita de ser preservada, assim como também os SI e as TIC que permitem a sua partilha entre os parceiros de negócio. Neste âmbito, é necessário garantir a segurança da informação, pessoal ou organizacional, cumprindo as necessidades estratégicas das organizações, nomeadamente a prossecução da sua missão e objectivos, considerando sempre a legislação vigente e aplicável, assim como as normas aplicáveis, sejam genéricas ou específicas a uma actividade concreta.

Constatando-se estas necessidades, importa ter em atenção a legislação e o diverso normativo cuja utilização directa ou indirecta neste trabalho, podem e devem ser consideradas essenciais para uma melhor percepção da sua utilização e no como podem responder às questões colocadas.

2.1. Enquadramento Normativo

O enquadramento normativo da segurança da informação, assim como da gestão dos SI e das TIC que suportam a informação, é proporcionado por uma diversidade de normas que se sobrepõem ou complementam, em função dos propósitos delineados a quando do seu desenvolvimento.

Refira-se desde já que o termo ‘norma’ vai ser utilizado para referir todos estes documentos, mesmo aqueles que não correspondem a *standards* de facto.

Perante a diversidade de normas existentes, foram identificadas algumas que no seu conjunto se entendem como adequadas a suportar o desenvolvimento deste trabalho.

Com esse objectivo, foram seleccionadas as seguintes normas:

- ⇒ BS ISO/IEC 17799:2005 – Information Technology - Security Techniques - Code of Practice for Information Security Management
- ⇒ BS ISO/IEC 27001:2005 – Information Technology - Security Techniques - Information Security Management Systems - Requirements
- ⇒ BS 7799-3:2006 – Information - Management Systems - Guidelines for Information Security Risk Management
- ⇒ ISO/IEC 13335-1:2004 – Information technology - Guidelines for the management of IT security - Concepts and models for information and communications technology security
- ⇒ ISO/IEC 21827:2002 – Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM)
- ⇒ BS ISO/IEC 20000-1:2005 – Information Technology - Service Management - Specification
- ⇒ BS ISO/IEC 20000-2:2005 – Information Technology - Service Management - Code of practice
- ⇒ NIST SP800-12 – An Introduction to Computer Security: The NIST Handbook
- ⇒ NIST SP800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems
- ⇒ NIST SP800-16 – Information Technology Security Training Requirements: A Role -and Performance- Based Model
- ⇒ NIST SP800-18 – Guide for Developing Security Plans for Information Technology Systems
- ⇒ NIST SP800-26 – Security Self-Assessment Guide for Information Technology Systems
- ⇒ NIST SP800-27 – Engineering Principles for Information Technology Security (A Baseline for Achieving Security)
- ⇒ NIST SP800-30 – Risk Management Guide for Information Technology Systems

- ⇒ NIST SP800-33 – Underlying Technical Models for Information Technology Security
- ⇒ NIST SP800-34 – Contingency Planning Guide for Information Technology Systems
- ⇒ NIST SP800-55 – Security Metrics Guide for Information Technology Systems
- ⇒ NIST SP800-61 – Computer Security Incident Handling Guide
- ⇒ NIST SP800-64 – Security Considerations in the Information System Development Life Cycle
- ⇒ NIST SP800-80 – Guide for Developing Performance Metrics for Information Security
- ⇒ NIST SP800-100 – Information Security Handbook: A Guide for Managers
- ⇒ The Standard of Good Practice for Information Security (the Standard)
- ⇒ Cardholder Information Security Program (CISP)
- ⇒ Information Technology Infrastructure Library (ITIL)
- ⇒ OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security
- ⇒ Control Objectives for Information and related Technology (COBIT)
- ⇒ Generally Accepted Information Security Principles (GAISP)
- ⇒ Information Systems Security Assessment Framework (ISSAF)
- ⇒ IT Baseline Protection Manual
- ⇒ RFC 2196 – The Site Security Handbook

De entre este conjunto de normas, cuja síntese estrutural vai ser apresentada neste capítulo, as que forem identificadas como essenciais para o desenvolvimento do trabalho, serão objecto de uma especificação mais aprofundada, constando por isso do anexo A a este trabalho. O destaque a dar a qualquer das normas⁹ terá em atenção o seu enquadramento com as questões a que este trabalho pretende responder.

⁹ Todos os textos apresentados relativamente à estrutura das normas mencionadas são transcritos das próprias normas, de acordo com as citações mencionadas em cada uma delas.

2.1.1. BS ISO/IEC 17799:2005 – Code of Practice for Information Security Management

A norma BS ISO/IEC 17799:2005 [ISO 2005a], baseada na BS 7799-1 que foi desenvolvida pela *British Standard (BS) Institution (BSI)*, transformada em norma internacional pela *International Standard Organization (ISO)* e pela *International Electrotechnical Commission (IEC)*, define os procedimentos necessários a garantir a segurança da informação. Está prevista, de acordo com as especificações estabelecidas pela ISO, a substituição desta norma pela ISO 27002, mantendo-se todavia o essencial dos seus objectivos e estrutura.

A ordem das cláusulas nesta norma não tem a ver com a sua importância, mas sim com as circunstâncias de aplicação pelo que todas as cláusulas podem ser importantes, levando a que cada organização que utiliza esta norma possa identificar as cláusulas aplicáveis, a sua importância e aplicação aos processos de negócio individuais. Além disso, a não ser nos casos especificamente referenciados, a ordem pela qual os controlos surgem não define qualquer prioridade [ISO 2005a].

Como objectivos da norma definem-se o estabelecimento de linhas de orientação e princípios gerais para iniciação, implementação, manutenção e melhorias da gestão da segurança da informação numa organização, objectivos estes que proporcionam orientações gerais nas metas comumente aceites na gestão da segurança da informação.

Os objectivos de controlo e os controlos deste *standard* serão implementados para cumprir os requisitos identificados pela valorização do risco. Este *standard* pode servir como um guia de boas práticas para o desenvolvimento dos *standards* de segurança organizacional e práticas efectivas de gestão da segurança, e para ajudar a construir confiança nas actividades inter organizacionais.

Esta norma estrutura-se em 133 controlos que são agrupados em onze directrizes, que por sua vez são subdivididas em componentes:

- (1) Política de segurança – (i) Política de segurança da informação;
- (2) Organização da segurança da informação – (i) Organização interna; (ii) Parceiros externos;

- (3) Gestão dos activos – (i) Responsabilidade pelos recursos; (ii) Classificação da informação;
- (4) Segurança dos recursos humanos – (i) Antecedentes ao emprego; (ii) Durante o emprego; (iii) Finalização ou mudanças no emprego;
- (5) Segurança ambiental e física – (i) Áreas seguras; (ii) Segurança dos equipamentos;
- (6) Gestão das operações e das comunicações – (i) Responsabilidades e procedimentos operacionais; (ii) Gestão dos serviços de entrega de parceiros externos; (iii) Planeamento e aceitação do sistema; (iv) Protecção contra código malicioso e móvel; (v) Backup; (vi) Gestão de segurança da rede; (vii) Manuseamento dos meios; (viii) Troca de informação; (ix) Serviços de comércio electrónico; (x) Monitorização;
- (7) Controlo dos acessos – (i) Requisitos de negócio para controlo de acessos; (ii) Gestão de acessos dos utilizadores; (iii) Responsabilidades dos utilizadores; (iv) Controlo dos acessos à rede; (v) Controlo dos acessos ao sistema operativo; (vi) Controlo de acessos à informação e às aplicações; (vii) Computação móvel e tele-trabalho;
- (8) Manutenção, desenvolvimento e aquisição de sistemas de informação – (i) Requisitos de segurança dos sistemas de informação; (ii) Processamentos correctos nas aplicações; (iii) Controlos criptográficos; (iv) Segurança dos ficheiros de sistema; (v) Segurança no desenvolvimento e processos de suporte; (vi) Gestão das vulnerabilidades técnicas;
- (9) Gestão dos incidentes de segurança da informação – (i) Relatório dos eventos e das fraquezas de segurança da informação; (ii) Gestão dos incidentes e melhorias da segurança da informação;
- (10) Gestão da continuidade do negócio – (i) Aspectos de segurança da informação para a gestão da continuidade do negócio;
- (11) Conformidade – (i) Conformidade com os requisitos legais; (ii) Conformidade com standards e políticas de segurança e conformidade técnica; (iii) Considerações de auditoria de sistemas de informação.

2.1.2. BS ISO/IEC 27001:2005 – Information Security Management Systems - Requirements

A norma BS ISO/IEC 27001:2005 [ISO 2005b], baseada na BS 7799-2 que foi desenvolvida pela BSI, especifica os requisitos para o estabelecimento, implementação, operação, monitorização, revisão, manutenção e melhorias de um sistema de gestão de segurança da informação no contexto de todos os riscos de negócio numa organização. Estes requisitos podem ser adequados às necessidades da totalidade da organização ou apenas a partes dela. De forma similar ao que está previsto para a substituição da ISO/IEC 17799, também esta norma deverá ser brevemente substituída pela ISO 27005, mantendo-se mais uma vez o essencial dos objectivos e estrutura.

O SGSI é desenhado para assegurar a selecção dos controlos de segurança proporcionais e adequados à protecção dos activos informacionais, procurando simultaneamente proporcionar confiança aos interessados.

A sua estrutura tem em atenção uma abordagem de implementação baseada no Modelo PDCA (*Plan-Do-Check-Act*), encontrando-se organizada em cinco capítulos distintos mas complementares:

- (1) SGSI: (i) Requisitos genéricos; (ii) Estabelecimento e operação do SGSI (através de: a) *Estabelecer o SGSI*, b) *Implementar e operar o SGSI*, c) *Monitorizar e rever o SGSI*, d) *Manter e melhorar o SGSI*); (iii) Requisitos de documentação (através de: a) *Considerações genéricas*, b) *Controlo dos documentos*, c) *Controlo dos registos*);
- (2) Responsabilidade da Gestão: (i) Compromisso por parte da gestão; (ii) Gestão (e disponibilização) dos recursos necessários (através de: a) *Fornecimento de recursos*, b) *Treino, sensibilização e competência*);
- (3) Auditorias internas ao SGSI;
- (4) Revisão do SGSI por parte da gestão: (i) Considerações genéricas para este processo; (ii) *Inputs* para o processo de revisão; (iii) *Outputs* do processo de revisão;
- (5) Melhoria do SGSI: (i) Melhoria continuada; (ii) Acções ou medidas correctivas; (iii) Acções ou medidas preventivas.

2.1.3. BS 7799-3:2006 – Guidelines for Information Security Risk Management

Harmonizada com o estipulado nas principais normas de referência no que concerne à segurança da informação, nomeadamente a BS ISO/IEC 17799 (ex-BS 7799-1) e a BS ISO/IEC 27001 (ex-BS 7799-2), ao nível das boas práticas para a gestão da segurança da informação e dos requisitos para o estabelecimento de SGSI, respectivamente, a BS 7799-3 [BS 2006] apresenta um conjunto de directrizes que visam permitir uma gestão do risco mais eficiente nas organizações, considerando todos os aspectos do ciclo de gestão de riscos de um SGSI.

Este ciclo inclui valorizar e avaliar os riscos, implementar controlos para tratar os riscos, monitorizar e rever os riscos, e manter e melhorar o sistema de controlos do risco. Neste sentido, a BS 7799-3 foi especialmente desenvolvida para ser utilizada enquanto ferramenta por gestores de negócio e profissionais de segurança da informação directa ou indirectamente envolvidos com o desenvolvimento, implementação, operação, gestão, manutenção, revisão e/ou melhoria contínua do SGSI organizacional, pelo que deve ser adoptada seguindo uma abordagem por processos.

A estrutura da BS 7799-3 encontra-se dividida em 4 grupos de directrizes que permitem nomeadamente:

- (1) O enquadramento do conceito de ‘risco para a segurança da informação’ num contexto organizacional, considerando: (i) Política e propósito do SGSI (através de: a) *Caso de Negócio*, b) *Propósito do SGSI*, c) *Política do SGSI*); (ii) Filosofia/abordagem do risco;
- (2) O processo de análise e avaliação do risco na organização, considerando: (i) Processo de valorização do risco; (ii) Identificação de activos; (iii) Identificação dos requisitos legais e de negócio (através de: a) *Origem dos requisitos*, b) *Requisitos legais, regulamentares e contratuais*, c) *Princípios organizacionais, objectivos e requisitos de negócio*); (iv) Avaliação dos activos; (v) Identificação e valorização das ameaças e vulnerabilidades (através de: a) *Controlos implementados*, b) *Identificação de ameaças e vulnerabilidades*); (vi) Valorização das ameaças e vulnerabilidades; (vii) Cálculo e avaliação do risco; (viii) Avaliador do risco;

- (3) O processo de tratamento e gestão do risco, também no que respeita à tomada de decisão por parte da gestão organizacional, considerando: (i) Considerações genéricas; (ii) Tomada de decisão; (iii) Reduzir o risco; (iv) Aceitar objectivamente e com conhecimento o risco; (v) Transferir o risco; (vi) Evitar o risco; (vii) Risco residual; (viii) Plano de tratamento do risco;
- (4) Actividades continuadas de gestão de risco, no âmbito do SGSI da organização, considerando: (i) Gestão continuada do risco de segurança; (ii) Manutenção e monitorização; (iii) Revisão pela gestão; (iv) Revisão e revalorização do risco; (v) Auditorias; (vi) Controlo da documentação; (vii) Acções preventivas e correctivas; (viii) Comunicações e reporte (através de: a) *Plano de comunicações*, b) *Envolvimento e retorno*); (ix) Gestor do risco de segurança.

2.1.4. ISO/IEC FDIS 13335-1:2004 – Concepts and models for information and communications technology security

Esta norma internacional apresenta uma visão global dos conceitos e modelos fundamentais que podem ser utilizados para descrever a gestão da segurança das TIC [ISO 2004].

Este documento debruça-se assim sobre a problemática da insegurança das TIC, definindo conceitos e modelos para a segurança da informação e das tecnologias de comunicação, procurando garantir a prossecução deste objectivo, nomeadamente ao nível da manutenção da confidencialidade, da integridade, disponibilidade, não-repúdio, responsabilidade, autenticidade e fiabilidade dos recursos organizacionais.

Apresenta ainda uma breve introdução a possíveis áreas de salvaguardas, onde as técnicas apresentadas podem não ser imediatamente aplicáveis a todas as organizações, necessitando de uma análise prévia dos benefícios e constrangimentos associados à sua implementação e utilização.

2.1.5. ISO/IEC 21827:2002 – Systems Security Engineering - Capability Maturity Model (SSE-CMM)

A *International Systems Security Engineering Association* desenvolveu em 1999 o modelo SSE-CMM, que por sua vez foi publicado em 2002, enquanto referencial

internacional, sob a designação ISO/IEC 21827 - Systems Security Engineering - Capability Maturity Model (SSE-CMM).

Este referencial [ISO 2002] visa dotar as organizações de um conjunto de práticas que garantam a inclusão da segurança enquanto característica intrínseca de qualquer sistema ou aplicação por elas desenvolvido, apresentando ainda directrizes ou práticas específicas que possibilitam uma gestão efectiva da segurança na organização.

Suficientemente abrangente para ser adaptável a qualquer organização ligada ao desenvolvimento de sistemas e/ou de soluções de segurança, este modelo de capacitação e maturidade apresenta práticas específicas intimamente relacionadas com a engenharia de segurança e de sistemas, que podem ser aplicadas aos processos de concepção, desenvolvimento, construção, operação e manutenção de *software* e de sistemas, desenvolvimento de infra-estruturas, bem como à gestão de ambientes de produção.

Este modelo tem por principal objectivo garantir a manutenção de pelo menos quatro características que permitem o desenvolvimento de produtos e/ou serviços considerados ‘seguros’, nomeadamente:

- (1) A continuidade das práticas desenvolvidas e utilizadas, ou seja, a garantia de que esforços desenvolvidos no âmbito de um determinado projecto podem ser reaproveitados noutros;
- (2) A possibilidade de repetição de práticas e esforços bem sucedidos no âmbito de um projecto, adaptando-os a outros projectos de natureza semelhante;
- (3) A garantia da eficiência do processo de concepção e desenvolvimento de produtos e serviços, maximizando a eficiência deste processo e dos recursos a este afectos;
- (4) A garantia de que as necessidades e requisitos de segurança do sistema se encontram a ser contemplados e devidamente colmatados, desde o início do processo de concepção e desenvolvimento do referido sistema.

A estrutura da ISO/IEC 21827 encontra-se dividida em dois grupos de directrizes que permitem nomeadamente:

- (1) Arquitectura do Modelo: (i) Engenharia de segurança; (ii) Visão geral do processo de engenharia da segurança; (iii) Descrição da arquitectura do SSE-CMM®;

- (2) Práticas base de segurança: (i) PA01 – Controlos de Administração de Segurança; (ii) PA02 – Avaliar o Impacto; (iii) PA03 – Avaliar Risco de Segurança; (iv) PA04 – Avaliar Ameaça; (v) PA05 – Avaliar Vulnerabilidade; (vi) PA06 – Construir Argumentos do Grau de Conforto; (vii) PA07 – Coordenar a Segurança; (viii) PA08 – Monitorizar a Postura de Segurança; (ix) PA09 – Proporcionar *Inputs* de Segurança; (x) PA10 – Especificar as Necessidades de Segurança; (xi) PA11 – Verificar e Validar a Segurança.

Cada uma das áreas de processos (*Process Area* – PA) anteriormente referidas apresenta-se estruturada em práticas básicas (*Base Practices* – BP) consideradas essenciais para conduzir a engenharia de segurança, práticas estas que embora numeradas não se encontram sujeitas a aplicação de acordo com essa numeração.

2.1.6. BS ISO/IEC 20000-1:2005 – Service Management - Specification

Desenvolvida a partir da BS 15000-1, norma britânica preparada pela BSI, que descreve um conjunto integrado de processos de gestão que possibilitam a entrega eficaz de serviços de SI/TI quer à organização, quer aos seus clientes, estando alinhada com a abordagem por processos definida na *Information Technology Infrastructure Library* (ITIL), a BS ISO/IEC 20000-1 [BS 2005a] tem por objectivo a promoção da adopção de uma abordagem por processos para a gestão integrada e efectiva dos serviços de SI/TI das organizações, no sentido de ir de encontro aos requisitos e objectivos quer do negócio, quer dos seus clientes a este nível.

A implantação da BS ISO/IEC 20000-1 numa organização pressupõe a adopção de algumas das práticas estabelecidas pela BS ISO/IEC 20000-2 e possibilita às organizações a obtenção de uma certificação reconhecida internacionalmente no que diz respeito à gestão dos serviços de SI/TI que detém e/ou que disponibiliza a outrem.

A estrutura da BS ISO/IEC 20000-1, apresenta as especificações e requisitos para o estabelecimento de um sistema de gestão de serviços de SI/TI, alicerçado em processos de gestão de serviços intimamente relacionados entre si e que incidem, nomeadamente:

- no planeamento e implementação do processo de gestão de serviços na organização, com especial atenção no que concerne ao planeamento e implementação de novos serviços ou de alterações a serviços já existentes e em utilização;

- nos requisitos para o processo de entrega de serviço, incluindo a gestão de níveis de serviço, a gestão da continuidade e da disponibilidade de serviços, a gestão da capacidade de serviços e a gestão da segurança da informação;
- na clarificação de aspectos relacionados com processos de relação com terceiros, como é o caso de fornecedores; na definição de processos de resolução e gestão de incidentes e/ou problemas associados aos diferentes recursos alocados a serviços de SI/TI;
- na identificação de especificações no que diz respeito a processos de controlo (gestão da mudança e de configurações);
- no processo de disponibilização do serviço, novo ou alterado, para o mercado.

2.1.7. BS ISO/IEC 20000-2:2005 – Service Management - Code of practice

Baseando-se, à semelhança do que acontece com a BS ISO/IEC 20000-1, no referencial britânico BS 15000-2 desenvolvido pela BSI, a BS ISO/IEC 20000-2 [BS 2005b] apresenta um conjunto de práticas de referência para as organizações, no que concerne à gestão de serviços de SI/TI internos ou a disponibilizar a terceiros, mediante contrato de alojamento, suporte ou manutenção, por exemplo, encontrando-se alinhada com o estipulado não só na BS ISO/IEC 20000-1, mas também com a abordagem orientada a processos consubstanciada na ITIL.

A BS ISO/IEC 20000-2 estabelece o código de boas práticas, apresentando e descrevendo as diferentes práticas e processos reconhecidos pela indústria ao nível da qualidade dos processos de gestão de serviços de SI/TI no âmbito previamente definido pela BS ISO/IEC 20000-1. Esta norma apresenta-se de especial utilidade para as organizações que pretendam a certificação de acordo com os seus requisitos ou que se encontrem em processo de revisão e/ou de melhoria de serviços e processos a estes associados.

A BS ISO/IEC 20000-2 estabelece, num conjunto de oito capítulos, práticas de referência no que diz respeito à gestão de serviços de SI/TI, nomeadamente ao nível de:

- (1) Sistema de Gestão – estipula a necessidade da definição e implantação de um sistema de gestão (BS ISO/IEC 20000-1), que deverá incluir as políticas da

organização a este nível, bem como de uma *framework* que possibilite a gestão e implementação efectivas de todos os serviços de TI da organização.

- (2) Planeamento de implementação de gestão de serviços – identifica a necessidade da definição/realização de um processo de planeamento estruturado e sustentado que possibilite a gestão de serviços de SI/TI, com enfoque na sua implementação e entrega.
- (3) Planeamento e implementação de novos serviços ou de serviços alterados – visa o alcance da garantia de que novos serviços e alterações a serviços já existentes poderão ser alvo de entrega e gestão, cumprindo o estipulado de acordo com o estabelecido entre as partes, nomeadamente ao nível de custos e de qualidade dos serviços.
- (4) Processos de entrega de serviços – tem por objectivo assegurar que se encontram definidos, acordados, registados e geridos os diferentes níveis de serviço estabelecidos entre a organização e terceiros.
- (5) Processos de relação (com terceiros) – com vista a garantir que todas as partes envolvidas num acordo de disponibilização de serviços de SI/TI se encontram cientes, compreendem e vão de encontro a necessidades de negócio, compreendem quer as capacidades quer constrangimentos à disponibilização dos serviços acordados, e ainda que compreendem as suas responsabilidades e obrigações.
- (6) Processos de controlo – têm por objectivo assegurar a definição e controlo de componentes dos serviços e infra-estruturas, mantendo igualmente informação de configuração precisa.
- (7) Processos de disponibilização do serviço para o exterior – com vista a garantir a entrega, distribuição e acompanhamento adequados de uma ou mais alterações verificadas nos serviços em ambiente de produção.

2.1.8. NIST SP800-12 – An Introduction to Computer Security: The NIST Handbook

Esta publicação foi desenvolvida em 1998 no âmbito do *National Institute of Standards and Technology* (NIST), apresentando-se frequentemente como uma referência de âmbito mundial e proporcionando apoio na segurança dos recursos baseados em computadores (incluindo *hardware*, *software* e informação) através da explicação de

conceitos importantes, considerações acerca dos custos e inter relações de controlos de segurança, ilustrando os benefícios dos controlos de segurança, as principais técnicas ou aproximações a cada controlo, assim como as considerações relacionadas com estes controlos e que são relevantes [NIST 1998].

Proporciona assim uma visão alargada da segurança de computadores¹⁰, ajudando os utilizadores a entender as suas necessidades em termos de segurança de computadores e a desenvolver uma aproximação correcta para selecção dos controlos de segurança apropriados.

Não são assim descritos detalhadamente os passos necessários para implementar um programa de segurança de computadores, nem proporcionados procedimentos detalhados para implementação de controlos de segurança, ou guias para auditar a segurança de sistemas específicos.

Este manual estrutura-se em três grandes áreas: Controlos de Gestão, Controlos Operacionais e Controlos Técnicos.

Os Controlos de Gestão endereçam os tópicos de segurança que podem ser caracterizados como de gestão, focando-se na gestão do programa de segurança de computadores e da gestão do risco na organização. Estes controlos evidenciam essencialmente os seguintes componentes:

- ⇒ Política de Segurança de Computadores;
- ⇒ Gestão do Programa de Segurança de Computadores;
- ⇒ Gestão do Risco de Segurança de Computadores;
- ⇒ Planeamento e Segurança no Ciclo de Vida do Sistema de Computadores;
- ⇒ Grau de Conforto.

Os Controlos Operacionais endereçam os controlos de segurança, focando-se, genericamente nos que são implementados e executados por Pessoas, controlos estes que são aplicados para melhorar a segurança de sistemas (ou grupos de sistemas) específicos. A sua aplicação requer muitas vezes conhecimentos específicos e uma ligação estreita com controlos técnicos e de gestão. Estes controlos englobam os seguintes componentes:

¹⁰ Nas normas desenvolvidas pelo NIST utilizam o termo ‘segurança de computadores’ que, no contexto deste trabalho será entendido como segurança dos sistemas informáticos ou das TIC.

- ⇒ Aspectos pessoais/de utilizador;
- ⇒ Preparação para Desastres e Contingências;
- ⇒ Tratamento de Incidentes de Segurança de Computadores;
- ⇒ Sensibilização, Treino, e Educação;
- ⇒ Considerações de Segurança nas Operações e Suporte de Computadores;
- ⇒ Segurança Física e Ambiental.

Os Controlos Técnicos focam-se nos controlos de segurança que o sistema de computadores utiliza, e dependem do funcionamento adequado do sistema e da sua eficiência. A implementação destes controlos requer considerações operacionais significativas, obrigando à sua adequação com a gestão da segurança na organização. Estes controlos abrangem os seguintes componentes:

- ⇒ Identificação e Autenticação;
- ⇒ Controlo dos Acessos Lógicos;
- ⇒ Registos para Auditoria;
- ⇒ Criptografia.

2.1.9. NIST SP800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems

Este documento, desenvolvido em 1996 no âmbito do NIST, proporciona as bases que as organizações podem utilizar para estabelecer e rever os seus programas de segurança das TI, apresentando as fundações que as organizações podem referenciar quando conduzem negócios entre organizações assim como os negócios internos [Swanson and Guttman 1996].

A gestão, os auditores internos, os utilizadores, os técnicos e os profissionais de segurança podem utilizar as directrizes para obtenção de um entendimento dos requisitos de segurança básicos que muitos sistemas de TI devem conter. As fundações iniciam-se com os princípios geralmente aceites dos sistemas de segurança e continuam com as práticas comuns que são usadas na segurança dos sistemas de TI.

Estas práticas (derivadas do NIST SP800-12) devem ser usadas como um ponto de partida conducente ao desenvolvimento de práticas adicionais baseadas nos requisitos de sistemas ou organizacionais, de acordo com as necessidades únicas de cada organização.

Este documento engloba oito princípios e catorze práticas, aplicando-se cada um dos princípios a cada uma das práticas referenciadas, variando apenas a natureza das relações estabelecidas entre princípios e práticas, verificando-se que as práticas derivam de um ou mais princípios, ou podem ser condicionadas pelos princípios.

Os princípios contidos no documento são:

- (1) A Segurança de Computador suporta a Missão da Organização;
- (2) A Segurança de Computador é um elemento integrante de uma Gestão sólida;
- (3) A Segurança de Computador deve ter custos controlados;
- (4) Os donos dos sistemas têm responsabilidades de segurança no exterior das suas organizações;
- (5) As Obrigações e Responsabilidades na Segurança de Computador devem ser explicitadas;
- (6) A Segurança de Computador requer uma abordagem compreensiva e integrada;
- (7) A Segurança de Computador deve ser reavaliada periodicamente;
- (8) A Segurança de Computador é constrangida por factores sociais.

Relativamente às práticas, são utilizadas as que constam do SP800-12, ou seja:

- (1) Política de Segurança de Computadores;
- (2) Gestão do Programa de Segurança de Computadores;
- (3) Gestão do Risco de Segurança de Computadores;
- (4) Planeamento e Segurança no Ciclo de Vida do Sistema de Computadores;
- (5) Aspectos Pessoais/de Utilizador;
- (6) Preparação para Desastres e Contingências;
- (7) Tratamento de Incidentes de Segurança de Computadores;
- (8) Sensibilização, Treino, e Educação;
- (9) Considerações de Segurança nas Operações e Suporte de Computadores;
- (10) Segurança Física e Ambiental;
- (11) Identificação e Autenticação;
- (12) Controlo dos Acessos Lógicos;
- (13) Registos para Auditoria;
- (14) Criptografia.

2.1.10. NIST SP800-16 – Information Technology Security Training Requirements: A Role -and Performance- Based Model

Este documento, desenvolvido em 1998 no âmbito do NIST, substitui o SP500-172 e apresenta uma nova *framework* conceptual para proporcionar treino na segurança das TI [Wilson 1998]. Esta *framework* inclui os requisitos de treino em segurança da informação, apropriados para os actuais sistemas de computação distribuídos e proporciona flexibilidade de extensão para acomodar tecnologias futuras e as decisões de gestão de risco relacionadas.

A abordagem de aprendizagem apresentada neste documento segue os princípios a seguir apresentados, de modo a facilitar o processo de aprendizagem:

- ⇒ Focaliza-se nas funções de trabalho ou nos papéis e obrigações específicas de cada Pessoa, e não nos seus títulos, reconhecendo que cada Pessoa possui uma cultura própria e diferentes níveis de entendimento;
- ⇒ Define as diferenças entre sensibilização, treino e educação;
- ⇒ Proporciona uma *framework* integrada para identificação das necessidades de treino, assegurando que cada Pessoa recebe o treino apropriado;
- ⇒ Proporciona uma ferramenta de desenvolvimento do curso;
- ⇒ Proporciona uma estrutura para avaliar a eficácia da aprendizagem;
- ⇒ É expansível.

O objectivo global deste documento é o de facilitar o desenvolvimento ou melhoramento de um programa de segurança das TI que seja compreensivo, mensurável e com custos controlados, que suporte a missão da organização e seja gerido como um elemento integrado no planeamento e na gestão adequada das TI.

A aprendizagem é então assumida como um processo contínuo, baseando-se num modelo próprio para identificação de conhecimentos, competências e capacidades que as Pessoas, em termos individuais, necessitam para desempenhar as obrigações de segurança das TI que são específicas dos seus papéis na organização.

Este modelo baseia-se em quatro conceitos fundamentais:

- (1) Sensibilização para a Segurança (aplicável a todos os funcionários);
- (2) Segurança Básica e Literacia (para todos os funcionários, incluindo parceiros externos, envolvidos nos sistemas de TI);

- (3) Papéis e Obrigações relativas aos sistemas de TI (treino vocacionado, observando as diferenças entre competências básicas, intermédias e avançadas);
- (4) Educação e Experiência (desenvolvimento de capacidades e competências relacionadas com o desempenho de actividades multidisciplinares complexas na área da segurança das TI, que tenham em conta as ameaças e as mudanças tecnológicas que afectam a segurança).

2.1.11. NIST SP800-18 – Guide for Developing Security Plans for Information Technology Systems

Esta publicação, desenvolvida em 1998 no âmbito do NIST, proporciona directrizes para o desenvolvimento de planos de segurança que documentem os controlos de gestão, técnicos e operacionais para os SI baseados em computadores, visando a protecção dos recursos de TI [Swanson 1998].

Este documento constitui conjuntamente com as NIST SP800-12 e NIST SP800-14 a trilogia da NIST acerca das orientações no programa de níveis de segurança. Neste sentido, são apresentados conceitos importantes, considerações de custos e as inter relações entre os controlos de segurança, proporcionando simultaneamente uma visão alargada da segurança de computadores e o 'porquê' de muitos aspectos relacionados com segurança.

A SP800-12 é utilizada como modelo (obtenção de detalhes adicionais ou explicações em qualquer dos controlos listados) para derivar as práticas recomendadas que surgem na SP800-14, apresentando esta o 'que' deve ser feito (descrição dos controlos e guia para revisão do plano) para a segurança dos recursos de TI.

Este documento utiliza os controlos de Gestão, Operacionais e Técnicos definidos na SP800-12, apresentando dois formatos específicos para os controlos Operacionais e Técnicos. Estes dois formatos são estabelecidos para as Aplicações Principais (*Major Applications* – MA) e para os Sistemas de Suporte Geral (*General Support Systems* – GSS).

As Aplicações Principais necessitam de uma abordagem específica devido à informação que contêm, processam ou transmitem, ou devido à sua criticidade para a missão da organização, enquanto que os Sistemas de Suporte Geral possuem recursos de

informação sob o mesmo controlo de gestão e partilham funcionalidades comuns. Estes incluem *hardware*, *software*, informação, dados, aplicações, comunicações, facilidades e Pessoas que proporcionam suporte a uma variedade de utilizadores e aplicações.

2.1.12. NIST SP800-26 – Security Self-Assessment Guide for Information Technology Systems

Este guia, desenvolvido em 2001 no âmbito do NIST, providencia um método para avaliar a segurança de sistemas ou grupos de sistemas não classificados, conduzindo um desempenho de auto valorização em segurança das TI. Adicionalmente este documento providencia orientações na utilização dos resultados da auto valorização para confirmar a amplitude do programa de segurança [Swanson 2001].

A auto valorização conduzida num sistema (aplicação principal ou sistema de suporte geral) ou auto valorizações conduzidas por um grupo de sistemas inter conectados é um método utilizado para medir a garantia de segurança das TI. A garantia de segurança das TI é o grau de confiança que existe de que as medidas de segurança de gestão, técnicas e operacionais resultam como pretendido para proteger o sistema e a informação que ele processa. A segurança adequada destes activos é uma responsabilidade fundamental da gestão.

Neste guia é utilizado um questionário, disponibilizado como Apêndice A da norma, com objectivos de controlo específicos e técnicas sugeridas, contra as quais a segurança de um sistema ou grupo de sistemas inter conectados podem ser medidos. É sugerido que o questionário se baseie em primeiro lugar na análise da documentação relevante e numa avaliação rigorosa e no teste dos controlos.

Embora este guia não estabeleça novos requisitos de segurança, os objectivos dos controlos devem ser retirados directamente dos requisitos já existentes em estatutos, políticas e directrizes de segurança e privacidade, devendo este guia ser utilizado em conjunto com directrizes mais detalhadas que são apresentadas no Apêndice B da norma.

2.1.13. NIST SP800-27 – Engineering Principles for Information Technology Security (A Baseline for Achieving Security)

O propósito deste documento, desenvolvido em 2001 no âmbito do NIST, é apresentar uma lista de princípios de segurança ao nível de sistema, para serem considerados no desenho, desenvolvimento e operação de um SI [Stoneburner *et al* 2001b].

Idealmente os princípios aqui apresentados devem ser utilizados a partir da iniciação de um programa - no início ou durante a fase de desenho - empregando-os através do ciclo de vida do sistema. Todavia, estes princípios são também úteis na afirmação e confirmação de uma postura de segurança dos SI já usados.

Este documento apresenta-se estruturado em 33 princípios para a segurança de sistemas. Estes princípios proporcionam as bases para uma abordagem estruturada e consistente, para o desenho, desenvolvimento e implementação da segurança das TI.

Enunciam-se seguidamente os princípios definidos para a segurança de sistemas:

- Princípio 1. Estabelecer uma sólida política de segurança como a base para o desenho.
- Princípio 2. Tratar a segurança como uma parte integrante do desenho de todo o sistema.
- Princípio 3. Delinear claramente as fronteiras físicas e lógica, conduzidas pelas políticas de segurança associadas.
- Princípio 4. Reduzir o risco a um nível aceitável.
- Princípio 5. Assumir que os sistemas externos são inseguros.
- Princípio 6. Identificar as potenciais vantagens entre reduzir o risco e aumentar os custos, ou reduzir outros aspectos da eficácia operacional.
- Princípio 7. Implementar segurança por camadas (garantir que não existe um único ponto vulnerável).
- Princípio 8. Implementar medidas de segurança de sistemas adequadas à prossecução dos objectivos de segurança organizacional.
- Princípio 9. Procurar a simplicidade.
- Princípio 10. Desenhar e operar um sistema de TI para limitar a vulnerabilidade e para ser flexível nas respostas.
- Princípio 11. Minimizar os elementos do sistema em que se confia.

- Princípio 12. Implementar segurança através da combinação de medidas físicas e lógicas.
- Princípio 13. Proporcionar a certeza de que o sistema é, e continua a ser, flexível perante as ameaças esperadas.
- Princípio 14. Limitar ou conter a vulnerabilidades.
- Princípio 15. Formular medidas de segurança para endereçar os múltiplos domínios de informação sobrepostos.
- Princípio 16. Isolar os sistemas de acesso público relativamente aos recursos críticos da missão (por exemplo dados, processos, etc.).
- Princípio 17. Utilizar mecanismos de fronteira para separar os sistemas computacionais e as infra estruturas de rede.
- Princípio 18. Quando possível, basear a segurança em *standards* abertos à portabilidade e interoperabilidade.
- Princípio 19. Utilizar uma linguagem comum no desenvolvimento dos requisitos de segurança.
- Princípio 20. Desenhar e implementar mecanismos de auditoria para detector usos não autorizados e suportar a investigação de incidentes.
- Princípio 21. Desenhar a segurança para permitir a adopção regular de novas tecnologias, incluindo um processo seguro e lógico de actualização tecnológica.
- Princípio 22. Autenticar utilizadores e processos para garantir as decisões apropriadas no controlo de acessos, seja nos domínios ou através dos domínios.
- Princípio 23. Utilizar identidades únicas para garantir a responsabilidade.
- Princípio 24. Implementar a opção de privilégio mínimo.
- Princípio 25. Não implementar mecanismos de segurança desnecessários.
- Princípio 26. Proteger a informação enquanto está a ser processada, em trânsito ou em armazenamento.
- Princípio 27. Pugnar pela facilidade de uso operacional.
- Princípio 28. Desenvolver e testar procedimentos de contingência e de recuperação de desastres para garantir a disponibilidade apropriada.

Princípio 29. Considerar produtos personalizados para atingir a segurança adequada.

Princípio 30. Garantir a segurança apropriada em caso de o sistema ser encerrado ou disponibilizado.

Princípio 31. Proteger contra todas as prováveis classes de ataques.

Princípio 32. Identificar e prevenir erros e vulnerabilidades comuns.

Princípio 33. Assegurar que os técnicos são treinados em como desenvolver *software* seguro.

2.1.14. NIST SP800-30 – Risk Management Guide for Information Technology Systems

Este guia, desenvolvido em 2001 no âmbito do NIST, proporciona os fundamentos para desenvolvimento de um programa efectivo de gestão de risco, facultando as definições e as directrizes práticas necessárias para a valorização e mitigação dos riscos identificados nos SI e nas TIC, objectivando ajudar as organizações a gerir melhor os riscos dos SI e das TIC que estão associados à sua missão [Stoneburner *et al* 2001a].

Considerando que a gestão de risco é o processo de identificar, valorizar e tomar medidas para reduzir o risco a um nível aceitável, este guia proporciona informação para selecção de controlos efectivos de segurança, que podem ser utilizados para mitigar os riscos, visando uma melhor protecção da informação crítica e dos SI que processam, armazenam e transportam essa informação.

A gestão do risco, quando as organizações utilizam SI e TIC para processar a sua informação de negócio, desempenha um papel crucial na protecção dos activos informacionais da organização, pelo que o processo de gestão do risco é uma componente importante para o sucesso do programa de segurança, considerando-se que o principal objectivo do processo de gestão de risco na organização deve ser a protecção da organização e da sua capacidade para atingir os seus objectivos e não apenas a protecção dos seus activos de TIC. Neste sentido, o processo de gestão de risco não deve ser tratado primariamente como uma função técnica a desempenhar pelo pessoal técnico que opera e gere os SI e as TIC, mas essencialmente como uma função de gestão da organização.

O objectivo de utilizar a gestão de risco é permitir que a organização cumpra a sua missão através de: melhor segurança dos SI que armazenam, processam e transmitem informação organizacional; permitindo que a gestão tome decisões fundamentadas sobre a gestão do risco, que justifiquem as componentes do orçamento associadas ao SI; assistindo a gestão na autorização ou acreditação dos SI tendo por base a documentação de suporte resultante do desempenho da gestão de risco.

Este documento estrutura-se em nove etapas para valorização do risco, procurando determinar a extensão de potenciais ameaças e o risco associado com o sistema de TI, através do seu ciclo de vida de desenvolvimento de sistemas, com o objectivo de identificar os controlos apropriados à redução ou eliminação do risco durante o processo de mitigação de riscos.

As etapas definidas para assegurar a valorização do risco são:

- Etapa 1. Caracterização do sistema.
- Etapa 2. Identificação das ameaças.
- Etapa 3. Identificação das vulnerabilidades.
- Etapa 4. Análise dos controlos.
- Etapa 5. Determinação de semelhanças.
- Etapa 6. Análise do impacto.
- Etapa 7. Determinação do risco.
- Etapa 8. Recomendações de controlo.
- Etapa 9. Documentação dos resultados.

2.1.15. NIST SP800-33 – Underlying Technical Models for Information Technology Security

O propósito desta publicação, desenvolvida em 2001 no âmbito do NIST, é providenciar a descrição das fundações técnicas, referenciadas como modelos, que são os fundamentos de segurança das TI [Stoneburner 2001].

A intenção desta norma é proporcionar, de uma forma concisa, os modelos que devem ser considerados no desenho e desenvolvimento das capacidades técnicas de segurança, modelos esses que incluem as lições aprendidas, as boas práticas e as considerações técnicas específicas.

Este documento apresenta um modelo de serviços de segurança técnica, classificando esses serviços, de acordo com o seu principal objectivo, como se segue:

- Suporte. Estes serviços são genéricos e subjacentes à maioria das capacidades de segurança das TI. Como serviços deste tipo são identificados: (i) Identificação (e nomeação), (ii) Gestão de chaves criptográficas, (iii) Gestão da Segurança, (iv) Protecções do sistema;
- Prevenção. Estes serviços procuram a prevenção da ocorrência de quebras de segurança. Estes serviços englobam: (i) Comunicações protegidas, (ii) Autenticação, (iii) Autorização, (iv) Forçar o controlo de acessos, (v) Não-repudição, (vi) Privacidade das transacções;
- Recuperação. Estes serviços focam-se na detecção e recuperação de quebras de segurança. Identificam-se aqui os seguintes serviços: (i) Auditoria, (ii) Detecção e contenção de intrusões, (iii) Comprovação da abrangência total, (iv) Reposição de um ‘estado’ seguro.

2.1.16. NIST SP800-34 – Contingency Planning Guide for Information Technology Systems

Este guia, desenvolvido em 2002 no âmbito do NIST, relativo ao planeamento da contingência de TI, identifica os princípios e práticas do planeamento para ajudar as Pessoas no desenvolvimento e manutenção efectiva de planos de contingência de TI [Swanson *et al* 2002].

Estes princípios enquadram a maioria das necessidades organizacionais, admitindo no entanto que cada organização pode ter requisitos adicionais específicos para os seus próprios processos.

Este documento proporciona orientações para ajudar na avaliação dos SI e das operações, para determinar os requisitos e prioridades de segurança, proporcionando ainda uma aproximação estruturada para ajudar no desenvolvimento de soluções de custos controlados, que reflectam adequadamente os seus requisitos de TI, e integrem os princípios do planeamento da contingência em todos os aspectos das operações de TI.

As orientações apresentadas devem ser consideradas durante todas as etapas do planeamento da contingência, iniciando-se com a conceptualização dos esforços de

planeamento da contingência, passando pela manutenção do plano e indo até à sua disponibilização.

Se for utilizado como ferramenta de gestão do planeamento, através do processo de planeamento da contingência, este documento e os seus apêndices devem proporcionar práticas de reduções de custos e de tempo.

São ainda apresentadas recomendações específicas para sete tipos de plataformas de TI, proporcionando estratégias e técnicas comuns a todos esses sistemas. As plataformas abrangidas são:

- (1) Sistemas portáteis e de secretária;
- (2) Servidores,
- (3) Sites *web*;
- (4) Redes de área local;
- (5) Redes de área alargada,
- (6) Sistemas distribuídos;
- (7) *Mainframes*.

Neste documento definem-se ainda processos de contingência com sete etapas, que podem ser utilizados para desenvolver e manter um programa viável de planeamento da contingência dos sistemas de TI. Estas sete etapas progressivas, desenhadas para serem integradas em cada fase do ciclo de desenvolvimento de sistemas, compreendem:

Etapa 1. Desenvolver a declaração da política de planeamento da contingência.

Etapa 2. Conduzir a análise do impacto nos negócios.

Etapa 3. Identificar controlos preventivos.

Etapa 4. Desenvolver estratégias de recuperação.

Etapa 5. Desenvolver um plano de contingência das TI.

Etapa 6. Testar, treinar e exercitar o plano.

Etapa 7. Manter o plano.

Este documento apresenta um formato simples para o desenvolvimento de um plano de contingência das TI, definindo três fases para governar as acções a tomar na falha de um sistema.

⇒ A fase de Notificação/Activação descreve o processo de notificação do pessoal afecto à recuperação e de valorização dos danos.

- ⇒ A fase de Recuperação discute o percurso sugerido de acções para as equipas de recuperação e o pessoal para reposição das operações de TI, num local alternativo ou utilizando as capacidades de contingência.
- ⇒ A fase de Reconstituição estabelece acções a serem tomadas para retornar o sistema às suas condições de operação normal.

2.1.17. NIST SP800-55 – Security Metrics Guide for Information Technology Systems

Este documento, desenvolvido em 2003 no âmbito do NIST, pretende ser um guia para o desenvolvimento, selecção e implementação de métricas específicas ao nível dos sistemas de TI, para serem utilizadas na medida do desempenho dos controlos e técnicas de segurança da informação [Swanson *et al* 2003].

As métricas de segurança das TI são aqui apresentadas como ferramentas desenhadas para facilitar a tomada de decisão e melhorar o desempenho e a responsabilidade, através da recolha, análise, e reporte do desempenho relevante relativamente aos dados.

Este documento proporciona orientações no como uma organização, através do uso de métricas, identifica a adequação dos controlos, políticas e procedimentos de segurança em utilização, providenciando ainda uma aproximação para ajudar a gestão a decidir onde investir em recursos adicionais de protecção da segurança, ou identificar e avaliar os controlos não produtivos.

Esta publicação explicita o desenvolvimento de métricas e processos de implementação, e como as métricas podem ser utilizadas para justificar adequadamente os investimentos em controlos de segurança. Os resultados de um efectivo programa de métricas de segurança de TI podem proporcionar dados úteis para direccionar a alocação de recursos de segurança da informação, devendo simplificar a preparação de relatórios relacionados com desempenho. Os exemplos de métricas apresentadas baseiam-se nos elementos críticos e nas técnicas e controlos de segurança constantes da NIST SP800-26.

Os processos de desenvolvimento de métricas, apresentados neste documento, garantem que essas métricas são desenvolvidas com o propósito de identificar causas dos baixos desempenhos e apontam para as acções correctivas apropriadas. Podem assim ser desenvolvidas e recolhidas métricas de três tipos:

- (1) Métricas de implementação para medir a implementação de políticas de segurança;
- (2) Métricas de eficácia/eficiência para medir os resultados dos serviços de segurança entregues;
- (3) Métricas de impacto para medir o impacto dos eventos de segurança nos negócios ou na missão.

2.1.18. NIST SP800-61 – Computer Security Incident Handling Guide

Esta publicação, desenvolvida em 2004 no âmbito do NIST, substitui a SP800-3 e procura assistir as organizações na mitigação dos riscos derivados de incidentes da segurança da informação, providenciando orientações práticas na resposta eficaz e eficiente a incidentes [Grance *et al* 2004].

São assim apresentados guias para resposta a incidentes gerais que são independentes de plataformas particulares de *hardware*, sistemas operativos e aplicações, incluindo especificamente orientações no estabelecimento de programas efectivos de resposta a incidentes, embora o seu foco principal seja a detecção, análise, priorização e manuseamento de incidentes.

Este documento pretende apoiar as organizações no estabelecimento de capacidades de resposta a incidentes de segurança de computadores, e a tratar eficaz e eficientemente os incidentes, atendendo essencialmente aos seguintes aspectos:

- ⇒ Organizar as capacidades de resposta a incidentes de segurança, nomeadamente: (i) Estabelecer procedimentos e políticas de resposta a incidentes, (ii) Estruturar uma equipa de resposta a incidentes, incluindo *outsourcing*, (iii) Identificar que pessoal adicional pode ser chamado para participar na resposta a incidentes;
- ⇒ Tratar incidentes desde a preparação inicial através da fase de aprendizagem das lições de incidentes anteriores;
- ⇒ Tratar tipos específicos de incidentes, nomeadamente: (i) Negação de serviços, (ii) Códigos maliciosos, (iii) Acessos não autorizados, (iv) Utilização inapropriada, (v) Componentes múltiplos.

2.1.19. NIST SP800-64 – Security Considerations in the Information System Development Life Cycle

Este guia, desenvolvido em 2003 no âmbito do NIST, substitui a SP800-4 e apresenta uma *framework* para incorporação de segurança em todas as fases do processo do ciclo de desenvolvimento de SI, desde o início até à sua disponibilização [Grance 2003]. Este documento não é um substituto para a aquisição por parte de uma organização de regulamentos, políticas e orientações de segurança.

Um ciclo de vida de desenvolvimento de sistemas é aqui utilizado, genericamente, para enquadrar as considerações de segurança, recorrendo a cinco fases do processo. Com o objectivo de incorporar efectivamente a segurança no sistema durante o seu desenvolvimento, cada uma das cinco fases, a seguir apresentadas, inclui um conjunto mínimo de passos de segurança:

- (1) Fase de Iniciação. (i) Categorização da segurança; (ii) Valorização preliminar dos riscos;
- (2) Fase de Aquisição/Desenvolvimento. (i) Valorização do risco; (ii) Análise dos requisitos funcionais de segurança; (iii) Análise dos requisitos de garantia de segurança; (iv) Reporte e considerações de custos; (v) Planeamento da segurança; (vi) Desenvolvimento de controlos de segurança; (vii) Avaliação e teste dos desenvolvimentos da segurança; (viii) Outros componentes do planeamento;
- (3) Fase de Implementação. (i) Aceitação e inspecção; (ii) Integração dos controlos de segurança; (iii) Certificação da segurança; (iv) Acreditação da segurança;
- (4) Fase de Operação/Manutenção. (i) Controlo e gestão da configuração; (ii) Monitorização contínua;
- (5) Fase de Distribuição. (i) Preservação da informação; (ii) Limpeza de dados nos dispositivos; (iii) Disponibilização de *software* e *hardware*.

2.1.20. NIST SP800-80 – Guide for Developing Performance Metrics for Information Security

Esta publicação, desenvolvida em 2006 no âmbito do NIST, foca-se no desenvolvimento e implementação de métricas de desempenho da segurança da informação para um programa de segurança da informação [Chew *et al* 2006]. O

processo e metodologias descritos nestas orientações ligam o desempenho da segurança da informação com o desempenho da organização, através do suporte dos processos de planeamento estratégico, ajudando assim a demonstrar como a segurança da informação contribui para atingir os objectivos e metas da estratégia da organização.

São utilizados os controlos de segurança de sistemas identificados na *NIST SP800-53 – Recommended Security Controls for Federal Information Systems* [Ross *et al* 2005], como base para o desenvolvimento de métricas que suportem a avaliação de programas de segurança. Adicionalmente a proporcionar orientações no desenvolvimento de métricas, este guia lista um número de métricas candidatas que podem ser reduzidas, expandidas ou utilizadas como modelos para desenvolver outras métricas. Este guia apresenta pelo menos uma métrica candidata para cada uma das 17 famílias de controlos, proporcionando *templates* e métricas candidatas para facilitar a implementação e utilização das métricas de desempenho da segurança da informação.

Este documento orientador deve ser aplicado em conjunto com o SP800-55, e usa processos e metodologias descritas no SP800-55 como ponto de partida. Enquanto se focaliza nos controlos da SP800-53, o processo descrito neste guia pode ser aplicado para desenvolver métricas específicas para organizações, mesmo que estas estejam fora do foco da SP800-53.

De modo a facilitar a ligação das actividades de segurança da informação com o planeamento estratégico das organizações, podem ser utilizadas especificações para os requisitos mínimos de segurança como entradas para os objectivos de desenvolvimento de métricas de desempenho da segurança da informação. Estas especificações, correspondentes às 17 famílias de controlos de segurança definidas na SP800-53, são as seguintes:

- (1) Controlo de Acessos;
- (2) Sensibilização e Treino;
- (3) Auditoria e Responsabilização;
- (4) Certificação, Acreditação e Valorização da Segurança;
- (5) Gestão da Configuração;
- (6) Planeamento da Contingência;
- (7) Identificação e Autenticação;

- (8) Resposta a Incidentes;
- (9) Manutenção;
- (10) Protecção dos dispositivos de Dados;
- (11) Protecção Ambiental e Física;
- (12) Planeamento;
- (13) Segurança das Pessoas;
- (14) Valorização do Risco;
- (15) Aquisição de Serviços e Sistemas;
- (16) Protecção das Comunicações e Sistemas;
- (17) Integridade da Informação e dos Sistemas.

2.1.21. NIST SP800-100 – Information Security Handbook: A Guide for Managers

Este manual de segurança da informação, desenvolvido em 2006 no âmbito do NIST, proporciona uma visão alargada dos elementos do programa de segurança da informação para apoiar os gestores no entendimento de como estabelecer e implementar um programa de segurança da informação [Bowen *et al* 2006].

Tipicamente as organizações olham para o programa no sentido das obrigações globais, para garantir a selecção e implementação dos controlos de segurança adequados, e para demonstrar a eficácia de satisfação dos seus requisitos de segurança estabelecidos.

O material constante deste manual pode ser referenciado para informação geral acerca de um tópico em particular, ou pode ser utilizado no processo de tomada de decisão para o desenvolvimento de um programa de segurança da informação.

O propósito desta publicação é informar os membros da equipa de gestão de segurança da informação, acerca de variados aspectos da segurança da informação que se espera que venham a implementar e supervisionar nas respectivas organizações.

Adicionalmente, este manual providencia orientações para facilitar uma aproximação mais consistente aos programas de segurança da informação através do governo federal. Refira-se todavia, que mesmo tendo as terminologias deste documento sido geradas através do sector federal, o manual pode também ser utilizado para proporcionar orientações numa variedade de requisitos de segurança governamentais, organizacionais ou institucionais.

2.1.22. The Standard of Good Practice for Information Security (the Standard)

Este *standard*, desenvolvido pelo *Information Security Forum* (ISF), endereça a segurança da informação segundo uma perspectiva do negócio, providenciando uma base prática para valoração dos preparativos de segurança da informação de uma organização, focando-se nos aspectos a ter em conta na condução das organizações, para manter os riscos de negócio associados com os SI críticos sob controlo, nos actuais ambientes dinâmicos e competitivos [ISF 2005].

As principais secções deste *standard* proporcionam um conjunto de princípios de alto nível e objectivos para a segurança da informação em conjunto com a declaração de boas práticas associadas, a ser utilizado para melhorar o nível de segurança de uma organização de diversas formas.

Este *standard* foi estruturado para cobrir a globalidade dos tópicos de segurança, considerando cinco aspectos distintos que a seguir se apresentam, englobando cada um deles diversos controlos de segurança:

- (1) Gestão da Segurança: (i) Direcção de Topo; (ii) Organização da Segurança; (iii) Requisitos de Segurança; (iv) Ambiente de Segurança, (v) Ataques Maliciosos; (vi) Tópicos Especiais; (vii) Revisão pela Gestão;
- (2) Aplicações Críticas de Negócio: (i) Requisitos do Negócio para Segurança; (ii) Gestão Aplicacional; (iii) Ambiente dos Utilizadores; (iv) Gestão do Sistema; (v) Gestão da Segurança Local, (vi) Tópicos Especiais;
- (3) Instalação de Computadores: (i) Gestão da Instalação; (ii) Ambiente de Trabalho; (iii) Operação do Sistema; (iv) Controlo de Acessos; (v) Gestão da Segurança Local; (vi) Continuidade do Serviço;
- (4) Redes: (i) Gestão da Rede; (ii) Gestão do Tráfego; (iii) Operações da Rede; (iv) Gestão da Segurança Local; (v) Redes de Voz;
- (5) Desenvolvimento de Sistemas: (i) Gestão do Desenvolvimento; (ii) Gestão da Segurança Local; (iii) Requisitos do Negócio; (iv) Desenhar e Construir, (v) Testar; (vi) Implementar.

2.1.23. Cardholder Information Security Program (CISP)

O *Cardholder Information Security Program* (CISP) foi desenvolvido pela Visa USA (1999) com o objectivo de assegurar aos utilizadores de cartões que a informação da sua conta está salvaguardada, independentemente de onde são entregues para pagamento.

Com o objectivo inicial de tornar seguras as transacções com cartão de crédito conduzidas através da Internet, este programa [CISP 2004] foi posteriormente expandido (Junho 2001) e tornado obrigatório para aplicação em todos os canais de pagamento, incluindo retalho, ordens por correio, ordens telefónicas e comércio electrónico.

Este *standard* é o resultado da colaboração entre a Visa e a MasterCard, desenhada para criar requisitos comuns para a segurança da indústria, incorporando os requisitos do CISP. Este *standard* é também expandido a qualquer entidade que armazene ou transmita informação confidencial dos detentores dos cartões, tais como as instituições financeiras que detêm os cartões de crédito.

O CISP abrange seis áreas distintas, estruturando-se em 12 requisitos que a seguir se apresentam:

(1) Construir e Manter uma Rede Segura

Requisito 1. Instalar e manter uma configuração de *firewall* para proteger os dados.

Requisito 2. Não utilizar *passwords* de sistema e outros parâmetros de segurança proporcionados pelos fornecedores.

(2) Proteger os dados dos detentores de Cartões

Requisito 3. Proteger os dados armazenados.

Requisito 4. Encriptar transmissões dos dados dos detentores de cartões e a informação sensível que atravessa as redes públicas.

(3) Manter o Programa de Gestão de Vulnerabilidades

Requisito 5. Utilizar e actualizar regularmente o *software* de antivírus.

Requisito 6. Desenvolver e manter aplicações e sistemas seguros.

(4) Implementar Medidas Fortes de Controlo de Acessos

Requisito 7. Restringir o acesso aos dados apenas ao que as organizações necessitam de saber.

Requisito 8. Associar um único *ID* a cada pessoa com acesso aos computadores.

Requisito 9. Restringir o acesso físico aos dados dos detentores dos cartões.

(5) Monitorizar e Testar Regularmente as Redes

Requisito 10. Seguir e monitorizar todos os acessos aos recursos da rede e aos dados dos detentores de cartões.

Requisito 11. Testar regularmente os processos e os sistemas de segurança.

(6) Manter uma Política de Segurança da Informação

Requisito 12. Manter uma política que dirija a segurança da informação.

2.1.24. Information Technology Infrastructure Library (ITIL)

Desenvolvido no decorrer da década de 80, a ITIL, versão 2.0, consiste numa *framework* baseada numa abordagem por processos e fundamentada na implementação de boas práticas, visando facilitar o alcançar de serviços de SI/TI de elevada qualidade, quer para clientes externos, quer para a própria organização e respectivas áreas funcionais, de negócio ou departamentais [ITIL 2001].

Neste sentido, o ITIL determina e apresenta um conjunto de procedimentos de gestão, independentes dos fornecedores de uma dada organização, cujo objectivo é auxiliar as organizações na prossecução dos seus objectivos de negócio, no que concerne a aspectos como a qualidade e a geração de valor a partir de operações relacionadas com as TIC, dotando-as de directrizes no que concerne ao desenho, desenvolvimento, operação e manutenção de infra-estruturas de SI/TI.

Os aspectos tidos em consideração ou abrangidos pelo ITIL, publicado numa série de oito livros (cada um dos quais cobrindo uma disciplina ou processo associado à gestão de infra estruturas de serviços de SI/TI), e actualmente sobre a alçada do OGC britânico (*Office of Government Commerce*), prendem-se com duas disciplinas distintas mas complementares: a entrega ou disponibilização de serviços e o suporte de ou a serviços e o planeamento da implementação de processos de gestão de serviços de SI/TI.

Esta *framework*, na versão 3.0, engloba sete módulos [Rudd 2004]:

- (1) Entrega de Serviços – cobre os processos necessários para o planeamento e entrega de serviços de qualidade, tendo em atenção a longo prazo os processos que podem melhorar a qualidade dos serviços de TI.

- (2) Suporte dos Serviços – descreve os processos relacionados com as actividades diárias de suporte e manutenção associadas ao fornecimento de serviços de TI.
- (3) Gestão da infra-estrutura das TIC – engloba todos os aspectos desde a identificação dos requisitos do negócio até ao teste, instalação, disponibilização, operações continuadas e optimização dos componentes e serviços de TIC.
- (4) Planeamento da Implementação da Gestão de Serviços – examina os tópicos e actividades envolvidas no planeamento, implementação e melhoria dos processos de Gestão de Serviços numa organização.
- (5) Gestão de Aplicações – descreve como gerir as aplicações, desde as necessidades iniciais do negócio através de todas as etapas do ciclo de vida da aplicação.
- (6) Perspectiva dos Negócios – proporciona alertas e directrizes para ajudar o pessoal da TI a entender como podem contribuir para os objectivos do negócio.
- (7) Gestão da Segurança – detalha o processo de planeamento e gestão do nível de segurança definido para a informação e para os serviços de TI, incluindo todos os aspectos associados com a reacção a incidentes de segurança. Inclui ainda a valorização e gestão dos riscos e vulnerabilidades, assim como da implementação das contramedidas justificadas.

2.1.25. OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security

A Organização para a Cooperação e Desenvolvimento Económico (OCDE), ou *Organisation for Economic Co-operation and Development* (OECD), desenvolveu e publicou em 2002, um conjunto de directrizes ou guias que visam auxiliar os seus estados membros, entre os quais se inclui Portugal, no alcance da segurança dos seus SI e das suas redes de comunicação de dados (e por conseguinte da sua informação), fomentando uma cultura de segurança entre estes [OECD 2002].

O documento, denominado ‘*Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*’, sugere a necessidade crescente da sensibilização e alerta no que concerne a questões relacionadas com a (in)segurança da informação, motivadas por uma cada vez maior inter-conectividade dos SI e das redes

organizacionais, que por sua vez se traduz numa crescente exposição a potenciais e cada vez mais numerosas ameaças.

Este guia estabelece nove princípios que quer as organizações, quer os seus estados membros devem observar e cumprir, nomeadamente:

- (1) Sensibilização – todos os participantes devem estar cientes da necessidade da segurança dos SI e das redes, e do papel que podem desempenhar na sua melhoria;
- (2) Responsabilidade – todos os participantes são responsáveis pela segurança dos SI e das redes;
- (3) Resposta – os participantes devem agir atempadamente e cooperar entre si, no sentido de prever, detectar e responder a incidentes de segurança;
- (4) Ética – os participantes devem respeitar os interesses legítimos dos outros participantes;
- (5) Democracia – a segurança dos SI e das redes deve ser compatível com os valores essenciais de uma sociedade democrática;
- (6) Análise de Risco – os participantes devem realizar análises de risco;
- (7) Desenho e implementação da segurança – os participantes devem considerar a segurança como um elemento essencial dos SI e das redes;
- (8) Gestão da Segurança – os participantes devem adoptar uma abordagem compreensiva no que concerne à gestão da segurança;
- (9) Reavaliação – os participantes devem rever e reavaliar a segurança dos SI e das redes, e realizar as modificações apropriadas às políticas, práticas, medidas e procedimentos de segurança em vigor.

2.1.26. Control Objectives for Information and related Technology (COBIT)

Este *standard*, *Control Objectives for Information and related Technology* (COBIT) proporciona boas práticas através de um domínio e uma *framework* de processos, apresentando as actividades numa estrutura lógica e gerível [COBIT 2005]. As boas práticas referenciadas representam o consenso de peritos e focam-se fortemente no controlo e menos na execução, ajudando a otimizar os investimentos possíveis em TI, assegurando as entregas de serviços e providenciando uma medida contra a qual podem ser avaliados.

A orientação de negócios do COBIT consiste na ligação entre as metas de negócio e as metas de TI, proporcionando métricas e modelos de maturidade para medir a sua realização e identificar as responsabilidades associadas aos donos do negócio e dos processos de TI.

A *framework* de controlo COBIT contribui para as necessidades de sucesso das TI relativamente aos requisitos de negócio:

- estabelecendo ligações com os requisitos de negócio;
- organizando as actividades de TI num modelo de processos genericamente aceites;
- identificando os principais recursos de TI a serem aplicados;
- definindo os objectivos de controlo de gestão a serem considerados.

A estrutura do COBIT é ilustrada por um modelo de processos que subdivide as TI em 34 processos em linha, com responsabilidades nas áreas do planeamento, construção, execução e monitorização, proporcionando uma visão extremada das TI.

Esta estrutura de 34 processos é enquadrada em quatro tópicos específicos:

- (1) Planear e Organizar: (i) Definir um Plano Estratégico de TI; (ii) Definir a Arquitectura de Informação; (iii) Determinar o Rumo Tecnológico; (iv) Definir os Processos, Organização e Relações das TI; (v) Gestão dos Investimentos em TI; (vi) Comunicar as Directivas e Metas da Gestão; (vii) Gestão dos Recursos Humanos das TI; (viii) Gestão da Qualidade; (ix) Acesso e Gestão dos Riscos das TI; (x) Gerir Projectos;
- (2) Adquirir e Implementar: (i) Identificar Soluções Automatizadas; (ii) Adquirir e Manter Aplicações de Software; (iii) Aquisição e Manutenção da Infra-estrutura Tecnológica; (iv) Facilitar a Operação e Uso; (v) Obter Recursos de TI; (vi) Gestão das Mudanças; (vii) Instalar e Acreditar Soluções e Mudanças;
- (3) Entrega e Suporte: (i) Definir e Gerir os Níveis de Serviço; (ii) Gerir os Serviços de Terceiras Partes; (iii) Gerir o Desempenho e Capacidade; (iv) Garantir a Continuidade do Serviço; (v) Garantir a Segurança dos Sistemas; (vi) Identificar e Alocar Custos; (vii) Educar e Treinar Utilizadores; (viii) Gerir os Serviços e Incidentes; (ix) Gestão da Configuração; (x) Gerir Problemas; (xi) Gerir os Dados; (xii) Gerir o Ambiente Físico; (xiii) Gerir as Operações;

- (4) Monitorizar e Avaliar: (i) Monitorizar e Avaliar o Desempenho das TI; (ii) Monitorizar e Avaliar os Controlos Internos; (iii) Garantir Conformidade Regulamentar; (iv) Providenciar o Governo das TI.

Os conceitos de arquitectura organizacional ajudam a identificar os recursos essenciais para o sucesso dos processos, ou seja, aplicações, informação, infra estruturas e Pessoas, resumidamente, para proporcionar a informação que a organização necessita para atingir os seus objectivos, os recursos de TI devem ser geridos por um conjunto de processos agrupados de forma natural.

2.1.27. Generally Accepted Information Security Principles (GAISP)

Os *Generally Accepted Information Security Principles* (GAISP) suportam e reforçam os controlos derivados do facto da segurança da informação incluir medidas de educação, instrução e treino, que informam os utilizadores dos computadores dos princípios e práticas de 'uso aceitável' que suportam os activos de informação [GAISP 2003].

Estes princípios devem ser construídos para assegurar que o SI reduz o risco de uma ameaça e a potencial escala dos seus impactos adversos. Este é assumido como orientação para donos da informação, profissionais de SI, desenvolvedores de produtos de TI e organizações com larga experiência na definição e declaração de princípios de segurança da informação.

Os princípios referenciados pela norma estruturam-se em três níveis hierárquicos:

(1) Princípios Abrangentes:

- (i) *Princípio da Responsabilidade* – A responsabilidade e obrigação com a segurança da informação deve ser claramente definida e conhecida;
- (ii) *Princípio da Sensibilização* – Todos os envolvidos, incluindo mas não limitada aos donos da informação e profissionais de segurança da informação, com necessidade de conhecer, devem ter acesso aos princípios, *standards*, convenções ou mecanismos aplicados ou disponíveis para a segurança da informação e dos SI, e devem ser informados das ameaças aplicáveis à segurança da informação;
- (iii) *Princípio da Ética* – A informação deve ser usada, e a administração da segurança da informação deve ser executada de uma forma ética;

- (iv) *Princípio da Multidisciplinaridade* – Princípios, *standards*, convenções e mecanismos para a segurança da informação e dos SI, devem endereçar as considerações e pontos de vista de todas as partes interessadas;
- (v) *Princípio da Proporcionalidade* – Os controlos de segurança da informação devem ser proporcionais ao risco de modificação, recusa de utilização, ou disponibilização de informação;
- (vi) *Princípio da Integração* – Princípios, *standards*, convenções ou mecanismos para a segurança da informação devem ser coordenados e integrados uns com os outros e com as políticas e procedimentos organizacionais, para criar e manter segurança através do SI;
- (vii) *Princípio da Conveniência* – Todas as partes responsáveis devem actuar atempadamente e de forma coordenada para prevenir ou responder a quebras de segurança e ameaças à segurança da informação e dos SI;
- (viii) *Princípio da Valorização* – Os riscos para a informação e SI devem ser avaliados periodicamente;
- (ix) *Princípio da Equidade* – A gestão deve respeitar os direitos e dignidade dos indivíduos quando estabelecem políticas, e quando seleccionam, implementam e forçam medidas de segurança.

(2) Princípios de Funcionamento Alargado:

- (i) *Política de Segurança da Informação* – A gestão deve assegurar que a política, *standards*, níveis base, procedimentos, e instruções de suporte são desenvolvidas e mantidas para endereçar todos os aspectos da segurança da informação. Estas orientações devem designar obrigações, o nível de descrição, e a quanto risco cada indivíduo ou entidade organizacional está autorizada a assumir;
- (ii) *Educação e Sensibilização* – A gestão deve comunicar a política de segurança da informação a todo o pessoal e garantir que todos estão apropriadamente avisados. A educação deve incluir *standards*, níveis base, procedimentos, instruções, obrigações, medidas forçadas relacionadas, e consequências de falhas de concordância;
- (iii) *Responsabilização* – A gestão deve assegurar que todas as partes são responsáveis pelo seu acesso e uso da informação, por exemplo, adições,

modificações, cópias e eliminações, e recursos de TI de suporte. Deverá ser possível fixar data, tempo, e obrigações, ao nível de um indivíduo, para todos os eventos significativos;

- (iv) *Gestão dos Activos de Informação* – A gestão deve rotineiramente catalogar e avaliar os activos de informação, e designar níveis de sensibilidade e criticidade. A informação, como um activo, deve ser identificada de forma única e atribuída a sua responsabilidade;
- (v) *Gestão Ambiental* – A gestão deve considerar e compensar pelos riscos inerentes ao ambiente físico interno e externo, onde os activos de informação e os recursos e activos de TI que os suportam são armazenados, transmitidos, processados ou utilizados;
- (vi) *Qualificações do Pessoal* – A gestão deve estabelecer e verificar as qualificações relativas a integridade, conhecimentos, e competências técnicas de todas as partes às quais são proporcionados acessos aos activos de informação ou aos recursos de TI de suporte;
- (vii) *Gestão de Incidentes* – A gestão deve proporcionar a capacidade de resolver e responder expedita e eficazmente a incidentes de segurança da informação, de forma a garantir que qualquer impacto no negócio é minimizado e que a probabilidade de experimentar incidentes similares é reduzida;
- (viii) *Ciclo de Vida dos Sistemas de Informação* – A gestão deve garantir que a segurança é dirigida a todas as fases do ciclo de vida do sistema;
- (ix) *Controlo de Acessos* – A gestão deve estabelecer os controlos apropriados a balancear o acesso a activos de informação e recursos de TI de suporte, contra o risco;
- (x) *Planeamento da Contingência e Continuidade Operacional* – A gestão deve planear e operar as TI de um modo que preserve a continuidade das operações organizacionais;
- (xi) *Gestão do Risco da Informação* – A gestão deve garantir que as medidas de segurança da informação são apropriadas para avaliação dos activos e das ameaças às quais aqueles são vulneráveis;

- (xii) *Segurança da Internet e da Rede* – A gestão deve considerar o impacto potencial na infra-estrutura global partilhada, por exemplo, a Internet, redes comutadas públicas, e outros sistemas conectados, quando se estabelecem medidas de segurança da rede;
 - (xiii) *Requisitos Legais, Regulamentares e Contratuais da Segurança da Informação* – A gestão deve caminhar para estar ciente de, e dirigir todos os requisitos legais, regulamentares e contratuais, pertencentes aos activos de informação;
 - (xiv) *Práticas Éticas* – A gestão deve respeitar os direitos e a dignidade dos indivíduos, quando criam políticas e quando seleccionam, implementam e forçam medidas de segurança.
- (3) Princípios Detalhados de Segurança: estes princípios são derivados da utilização integrada dos anteriores princípios.

Pretende-se ainda a criação, manutenção, monitorização dos GAISP, e a adesão a estes princípios, para a segurança da informação num contexto alargado, a um nível internacional, unificando e expandindo sobre os recursos autorizados existentes.

Como objectivos referenciam-se:

- Identificar e desenvolver GAISP detalhados, penetrantes e de funcionamento alargado numa *framework* compreensiva de princípios emergentes, *standards*, convenções e mecanismos que preservem a disponibilidade, confidencialidade e integridade da informação;
- Ser uma fonte autorizada para opiniões, práticas e princípios para donos da informação, profissionais de SI, produtos de TI e SI;
- Definir, implementar e operar de acordo com a infra-estrutura dos GAISP;
- Definir e estabelecer ligações com o projecto de *Common Criteria*;
- Manter uma ligação próxima e coordenada com os corpos de outras autoridades internacionais que desenvolveram trabalhos relacionados, para estabelecer e manter os GAISP baseados nesses esforços;
- Definir e estabelecer ligações com entidades responsáveis pela certificação de profissionais para encorajar a convergência;
- Promover uma instrução alargada da segurança da informação e dos GAISP;

- Endereçar a preocupação da gestão, dos utilizadores e de outros interessados a todos os níveis para obter uma aceitação alargada.

2.1.28. Information Systems Security Assessment Framework (ISSAF)

A *Information Systems Security Assessment Framework* (ISSAF) é uma *framework* estruturada que categoriza a valorização da segurança de SI em vários domínios e detalha a avaliação específica do teste de critérios para cada um desses domínios, procurando proporcionar entradas de valorização da segurança que reflectam cenários da vida real [ISSAF 2005].

Esta *framework* deve ser utilizada em primeiro lugar para preencher os requisitos de valorização da segurança organizacional, e adicionalmente como referencial para atingir outras necessidades de segurança da informação. Esta inclui os aspectos cruciais dos processos de segurança e a sua valorização e consolidação para obter uma imagem completa das vulnerabilidades que podem existir.

A referida *framework* é constituída por quatro fases:

- (1) Fase I – Planeamento: (i) Reunião de Informação; (ii) Execução do Diagrama do Projecto; (iii) Identificação dos Recursos; (iv) Orçamentação; (v) Preparação de *cash flow* simulado; (vi) Trabalhar a estrutura de falhas; (vii) Arranque do Projecto;
- (2) Fase II – Valorização: (i) Valorização do Risco Inerente; (ii) Valorização dos Controlos;
- (3) Fase III – Tratamento;
- (4) Fase IV – Acreditação: (i) Estabelecimento do Contexto; (ii) Avaliação; (iii) Apresentação de Relatório; (iv) Certificação.

Na ISSAF a informação é organizada em critérios de avaliação bem definidos, cada um dos quais foi submetido a revisão por parte de especialistas no domínio. Estes critérios de avaliação incluem:

- ⇒ A descrição do critério de avaliação;
- ⇒ Os seus fins e objectivos;
- ⇒ Os pré-requisitos para conduzir as avaliações;
- ⇒ O processo para avaliação;
- ⇒ A apresentação dos resultados esperados;

- ⇒ As contra-medidas recomendadas;
- ⇒ Referências a documentos externos.

2.1.29. IT Baseline Protection Manual

Este manual, desenvolvido pela BSI (*Bundesamt für Sicherheit in der Informationstechnik*), apresenta um conjunto *standard* de salvaguardas ou medidas de segurança recomendadas para sistemas típicos de TI [BSI 2004].

O fim destas recomendações de protecção das TI é atingir um nível de segurança para os sistemas de TI que seja razoável e adequado a satisfazer os requisitos de protecção normais, podendo ainda servir para os sistemas de TI e aplicações que requeiram um elevado grau de protecção.

As salvaguardas listadas no manual são medidas de segurança *standard*, ou seja, medidas que podem ser implementadas para os módulos respectivos, utilizando a última tecnologia para atingir um nível razoável de segurança. Em muitos casos estas salvaguardas proporcionam também um elevado nível de protecção, necessitando simplesmente da implementação de um nível básico de protecção, no entanto, estas são as precauções mínimas de segurança que são razoáveis de implementar nas áreas de interesse.

Para facilitar a estruturação e o processamento de áreas de TI altamente heterogéneas, incluindo o ambiente operacional, o manual é estruturado em módulos, reflectindo cada um deles as áreas típicas onde os activos de TI são utilizados. Cada um destes módulos inicia-se com a descrição das ameaças típicas esperadas nessa área, em conjunto com as probabilidades de ocorrência que são assumidas.

2.1.30. RFC 2196 – The Site Security Handbook

Este manual é um guia para o desenvolvimento de procedimentos e políticas de segurança de computadores para *sites* de sistemas na Internet, apresentando como propósito principal proporcionar orientações práticas para os administradores tentarem garantir a segurança da sua informação e serviços [Fraser 1997].

Os assuntos cobertos por este documento incluem a política de conteúdos e formação, um leque alargado de sistemas técnicos e tópicos de segurança de redes, e resposta a incidentes de segurança.

Este guia apresenta uma listagem de aspectos e factores que um *site* deve considerar quando estabelece as suas próprias políticas, apresentando recomendações e proporcionando a discussão das áreas relevantes.

2.2. Enquadramento Legal

Em termos de enquadramento legal, considerando a necessidade de qualquer norma respeitar a legislação aplicável a cada organização, entende-se como crucial identificar as leis aplicáveis em Portugal, para que seja possível proporcionar a correcta e adequada aplicação das normas de segurança às necessidades de segurança da informação identificadas, sem que sejam violadas as leis em vigor.

Com objectivo similar, deve também ser abordada a legislação internacional com relevância neste contexto, considerando aqui dois contextos distintos: a perspectiva europeia e a perspectiva internacional que não europeia.

2.2.1. Legislação Nacional

Embora se verifique que a legislação portuguesa em vigor não contempla a totalidade dos aspectos relacionados com a segurança da informação, frequentemente dispersos em diversa legislação, considera-se pertinente conhecer aquelas que mais directamente dizem respeito à problemática da segurança da informação, e como tal, influenciam a utilização do diverso normativo de segurança da informação.

O enquadramento legislativo da segurança da informação é proporcionado por um conjunto de legislação, onde se destaca:

- ⇒ Lei da Criminalidade Informática – Lei nº 109/91, de 17 de Agosto;
- ⇒ Lei da Protecção Jurídica de Programas de Computador – Lei nº 252/94, de 20 de Outubro;
- ⇒ Lei da Protecção de Dados Pessoais – Lei nº 67/98, de 26 de Outubro;
- ⇒ Lei das Comunicações Electrónicas – Lei nº 5/2004, de 10 de Fevereiro;
- ⇒ Lei da Protecção da Privacidade no Sector das Comunicações Electrónicas – Lei nº 41/2004, de 18 de Agosto.

A legislação referenciada atende a um princípio constitucional constante do seu artigo 35º (Utilização da Informática) e que estabelece que “todos os cidadãos têm o direito de

acesso aos dados informatizados que lhe digam respeito ...” (ponto 1), que “a informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do seu titular, ...” (ponto 3) e ainda que “é proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei” (ponto 4) [Veiga 2004], que permitem um enquadramento do que é permitido acerca da segurança da informação detida pelas organizações, quer esta diga respeito aos seus clientes, aos seus funcionários ou até aos seus parceiros de negócio.

2.2.1.1. Lei da Criminalidade Informática

A Lei da Criminalidade Informática (109/91, de 17 de Agosto) proporciona o enquadramento em termos do Código Penal dos crimes no âmbito da Informática, apresentando uma tipificação desses crimes e a respectiva moldura penal [AR 1991].

Perante estes pressupostos, são identificados seis crimes ligados à informática:

- (1) Falsidade informática (artigo 4º);
- (2) Dano relativo a dados ou programas informáticos (artigo 5º);
- (3) Sabotagem informática (artigo 6º);
- (4) Acesso ilegítimo (artigo 7º);
- (5) Intercepção ilícita (artigo 8º);
- (6) Reprodução ilegítima de programa protegido (artigo 9º).

2.2.1.2. Protecção Jurídica de Programas de Computador

Esta Lei (252/94, de 20 de Outubro) transpõe para a ordem jurídica portuguesa a Directiva nº 91/250/CEE, do Conselho Europeu, de 14 de Maio, relativa à protecção jurídica de programas de computador.

Esta Lei [AR 1994], de acordo com o estabelecido no seu artigo 1º, atribui protecção, “aos programas de computador que tiverem carácter criativo”, análoga à que é conferida às obras literárias, com equiparação a “programa de computador o material de concepção preliminar daquele programa”.

A Autoria, a Reprodução e Transformação, os Direitos do Utente, a Descompilação, os Direitos, a Apreensão, a Vigência e a Tutela, são algumas das temáticas abrangidas por esta Lei.

2.2.1.3. Lei da Protecção de Dados Pessoais

A Lei da Protecção de Dados Pessoais (67/98, de 26 de Outubro) transpõe para a ordem jurídica portuguesa a Directiva nº 95/46/CE, do Parlamento Europeu e do Conselho Europeu, de 24 de Outubro de 1995, relativa à protecção de Pessoas singulares no respeitante ao tratamento de dados pessoais¹¹ e à livre circulação desses dados.

Esta Lei [AR 1998], de acordo com o estabelecido no seu artigo 4º, “aplica-se ao tratamento de dados pessoais por meios total ou parcialmente automatizados, bem como ao tratamento por meios não automatizados de dados pessoais contidos em ficheiros manuais ou a estes destinados”.

Refira-se ainda a sua aplicação à “videovigilância e outras formas de captação, tratamento e difusão de som e imagens que permitam identificar pessoas”.

2.2.1.4. Lei das Comunicações Electrónicas

A Lei das Comunicações Electrónicas (5/2004, de 10 de Fevereiro) transpõe para a ordem jurídica portuguesa as Directivas nºs 2002/19/CE, 2002/20/CE, 2002/21/CE e 2002/22/CE do Parlamento Europeu e do Conselho, de 7 de Março, e a Directiva 2002/77/CE, da Comissão, de 16 de Setembro.

Esta lei [AR 2004a] “estabelece o regime jurídico aplicável às redes e serviços de comunicações electrónicas e aos recursos e serviços conexos e define as competências da entidade reguladora¹² nacional neste domínio”.

2.2.1.5. Lei da Protecção da Privacidade no Sector das Comunicações Electrónicas

A Lei da Protecção da Privacidade no Sector das Comunicações Electrónicas (41/2004, de 18 de Agosto) transpõe para a ordem jurídica portuguesa a Directiva nº 2002/58/CE, do Parlamento Europeu e do Conselho Europeu, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas. Esta lei [AR 2004b] especifica e complementa as disposições constantes da Lei nº 67/98, de 26 de Outubro.

¹¹ Conceito apresentado no artigo 3º desta Lei.

¹² Instituto das Comunicações de Portugal – Autoridade Nacional de Comunicações (ICP-ANACOM), com os estatutos aprovados pelo Decreto-Lei nº 309/2001, de 7 de Dezembro.

Esta Lei considera um conjunto de aspectos que devem ser tidos em atenção pelas organizações que operam neste sector. Esses aspectos são:

- (1) Segurança (artigo 3º);
- (2) Inviolabilidade das comunicações electrónicas (artigo 4º);
- (3) Armazenamento e acesso à informação (artigo 5º);
- (4) Dados de tráfego (artigo 6º);
- (5) Dados de localização (artigo 7º);
- (6) Facturação detalhada (artigo 8º);
- (7) Identificação da linha chamadora e da linha conectada (artigo 9º);
- (8) Excepções (artigo 10º);
- (9) Reencaminhamento automático de chamadas (artigo 11º);
- (10) Centrais digitais e analógicas (artigo 12º);
- (11) Listas de assinantes (artigo 13º).

2.2.1.6. A Segurança da Informação na Legislação e Regulamentação Nacional

Embora não directamente relacionada com a problemática da segurança da informação, a utilização crescente da utilização de SI e de TIC no suporte à aquisição, tratamento, armazenamento e partilha de informação implica que muita da legislação nacional enquadre no seu articulado, referências à ‘segurança da informação’.

A referência apresentada [Veiga 2004] aplica-se na seguinte legislação e regulamentação: Base da Dados Pessoais da Guarda Nacional Republicana (Decreto Regulamentar n.º2/95 de 25 de Janeiro – artigo 12º); Base da Dados Pessoais do Serviço de Estrangeiros e Fronteiras (Decreto Regulamentar n.º4/95 de 31 de Janeiro – artigo 12º); Base da Dados Pessoais da Polícia de Segurança Pública (Decreto Regulamentar n.º5/95 de 31 de Janeiro – artigo 12º); Base da Dados Pessoais da Secretaria-Geral do Ministério da Administração Interna no âmbito da Actividade de Segurança Privada (Decreto-Lei n.º309/98 de 14 de Outubro – artigo 11º).

“Tendo em vista a segurança da informação, deve observar-se o seguinte:

- a) A entrada nas instalações utilizadas para o tratamento de dados pessoais será objecto de controlo, a fim de impedir o acesso de qualquer pessoa não autorizada;

- b) Os suportes de dados são objecto de controlo, a fim de impedir que possam ser lidos, copiados, alterados ou retirados por qualquer pessoa não autorizada;
- c) A inserção de dados será objecto de controlo para impedir a introdução, bem como qualquer tomada de conhecimento, alteração ou eliminação não autorizada de dados pessoais;
- d) Os sistemas de tratamento automatizado de dados serão objecto de controlo para impedir que possam ser utilizados por pessoas não autorizadas, através de instalações de transmissão de dados;
- e) O acesso aos dados é objecto de controlo para que as pessoas autorizadas só possam ter acesso aos dados que interessem ao exercício das suas atribuições legais;
- f) A transmissão de dados é objecto de controlo para garantir que a sua utilização seja limitada às autoridades autorizadas;
- g) A introdução de dados pessoais nos sistemas de tratamento automatizado é objecto de controlo, de forma a verificar-se que dados foram introduzidos, quando e por quem;
- h) O transporte de suportes de dados é objecto de controlo para impedir que os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada.”

Outra referência apresentada [Veiga 2004] aplica-se na seguinte legislação: Regime Jurídico dos Ficheiros Informáticos dos Institutos de Medicina Legal de Lisboa, Porto e Coimbra (Decreto-Lei n.º395/99 de 13 de Outubro – artigo 9º).

“Sem prejuízo do disposto no artigo 15º da Lei n.º 67/98, de 26 de Outubro, são objecto de controlo, tendo em vista a segurança da informação:

- a) Os suportes de dados e o respectivo transporte, a fim de impedir que possam ser lidos, copiados, alterados ou eliminados por qualquer pessoa ou formas não autorizadas;
- b) A inserção de dados, a fim de impedir a introdução, bem como qualquer tomada de conhecimento, alteração ou eliminação não autorizada de dados pessoais;
- c) Os sistemas de tratamento automatizado de dados, para impedir que possam ser utilizados por pessoas não autorizadas, através de instalações de transmissão de dados;

- d) O acesso aos dados, para que as pessoas autorizadas só possam ter acesso aos dados que interessem ao exercício das suas atribuições legais;
- e) A transmissão de dados, para garantir que a sua utilização seja limitada às entidades autorizadas;
- f) A introdução de dados pessoais nos sistemas de tratamento automatizado, de forma a verificar-se que dados foram introduzidos, quando e por quem.”

A referência apresentada [Veiga 2004] aplica-se na seguinte legislação: Base de Dados da PGR sobre Pedidos de Transferência de Pessoas Condenadas (Decreto-Lei n.º293/99 de 3 de Agosto – artigo 11º); Base de Dados da PGR sobre Processos Crime contra Agentes de Autoridade (Decreto-Lei n.º294/99 de 3 de Agosto – artigo 11º); Base de Dados da PGR sobre Extradicações Activas e Passivas (Decreto-Lei n.º295/99 de 3 de Agosto – artigo 11º); Base de Dados da PGR sobre Fixação de Competência do Tribunal Singular, nos termos do artigo 16.º, n.º 3, do CPP (Decreto-Lei n.º298/99 de 4 de Agosto – artigo 11º); Base de Dados da PGR sobre a Suspensão Provisória de Processos Crime (Decreto-Lei n.º299/99 de 3 de Agosto – artigo 11º).

“Tendo em vista a segurança da informação, e sem prejuízo do disposto no artigo 15º da Lei n.º 67/98, de 26 de Outubro, são objecto de controlo:

- a) A entrada nas instalações utilizadas para o tratamento de dados pessoais, a fim de impedir o acesso aos dados por pessoa não autorizada;
- b) Os suportes utilizados, a fim de impedir que possam ser lidos, copiados, alterados ou retirados por pessoa não autorizada;
- c) A inserção de dados, para impedir a introdução, assim como qualquer tomada de conhecimento, alteração ou eliminação não autorizadas de dados pessoais;
- d) Os sistemas de tratamento automatizado de dados, para impedir que possam ser utilizados por pessoas não autorizadas, através de instalações de transmissão de dados;
- e) O acesso aos dados, para que as pessoas autorizadas só possam ter acesso aos dados que interessem ao exercício das suas atribuições legais;
- f) A transmissão de dados, para garantir que o envio destes, através de instalações de transmissão de dados, se limite às entidades autorizadas;
- g) A introdução de dados pessoais nos sistemas de tratamento automatizado, de forma a verificar-se que dados foram introduzidos, quando e por quem;

- h) A transmissão de dados e o transporte de suportes de dados, para impedir que os dados possam ser lidos, copiados, alterados ou eliminados por forma não autorizada.”

Uma outra referência apresentada [Veiga 2004] aplica-se na seguinte legislação: Base de Dados da Direcção-Geral dos Serviços Prisionais (Decreto-Lei n.º144/2001 de 26 de Abril – artigo 10º).

“Tendo em vista a segurança da informação, e sem prejuízo do disposto no artigo 15º da Lei n.º 67/98, de 26 de Outubro, são objecto de controlo:

- a) A entrada nas instalações utilizadas para o tratamento de dados pessoais, para impedir o acesso aos dados de pessoa não autorizada;
- b) Os suportes de dados, para impedir que possam ser lidos, copiados, alterados ou eliminados por pessoa não autorizada;
- c) A inserção de dados, para impedir a introdução e tomada de conhecimento, alteração ou eliminação não autorizadas de dados pessoais;
- d) O acesso aos dados, para que só as pessoas autorizadas e no exercício das suas competências possam aceder àqueles;
- e) A transmissão e a comunicação de dados, para garantir que sejam limitadas às entidades autorizadas;
- f) A introdução de dados pessoais, para se poder verificar que dados foram introduzidos, quando e por quem;
- g) O transporte de suportes de dados, para impedir que os dados possam ser lidos, copiados ou eliminados de forma não autorizada.”

A referência apresentada [Veiga 2004] aplica-se na seguinte legislação: Regime Jurídico dos Ficheiros Informáticos em matéria de Identificação Criminal e de Contumazes da Direcção-Geral dos Serviços Judiciários (Decreto-Lei n.º 62/99 de 2 de Março – artigo 11º).

“1 – O director-geral dos Serviços Judiciários deve adoptar as medidas de segurança referidas no artigo 15.º, n.º 1, da Lei n.º 67/98, de 26 de Outubro.

2 – É aplicável a todos os ficheiros informáticos a que se refere o presente diploma o disposto no artigo 29.º, do Decreto-Lei n.º 381/98, de 27 de Novembro.”

A referência apresentada [Veiga 2004] aplica-se na seguinte legislação: Cartão de Identificação do Utente do Serviço Nacional de Saúde (Decreto-Lei n.º 198/95 de 29 de Julho – artigo 18º, com as alterações introduzidas pelo Decreto-Lei n.º 48/97 de 27 de Fevereiro).

“São objecto de controlo, tendo em vista a segurança da informação:

- a) A entrada nas instalações utilizadas para o tratamento de dados pessoais, a fim de impedir o acesso de qualquer pessoa não autorizada;
- b) Os suportes de dados, a fim de impedir que possam ser lidos, copiados, alterados ou retirados por qualquer pessoa não autorizada;
- c) A inserção de dados, para impedir a introdução, bem como qualquer tomada de conhecimento, alteração ou eliminação não autorizadas na base de dados;
- d) Os sistemas de tratamento automatizado de dados, para impedir que possam ser utilizados por pessoas não autorizadas, através de instalações de transmissão de dados;
- e) O acesso aos dados, para que as pessoas autorizadas só possam ter acesso aos dados que interessem ao exercício das suas atribuições legais;
- f) A transmissão de dados, para garantir que a sua utilização seja limitada às entidades autorizadas;
- g) O transporte de suportes de dados, para impedir que os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada.”

Esta referência [Veiga 2004] aplica-se na seguinte legislação: Registo Nacional de Não Dadores (Decreto-Lei n.º 244/94 de 26 de Setembro – artigo 8º).

“O responsável pelo ficheiro automatizado e as entidades autorizadas a aceder ao ficheiro, nos termos do artigo anterior¹³, adoptarão as medidas técnicas necessárias para garantir que a informação não possa ser obtida indevidamente ou usada para outros fins que não os consentidos no presente diploma.”

A referência apresentada [Veiga 2004] aplica-se na seguinte legislação: Registo Individual do Condutor (Decreto-Lei n.º 317/94 de 24 de Dezembro – artigo 13º).

“Tendo em vista a segurança da informação, cabe ao responsável pelas bases de dados a que se refere o presente diploma garantir a observação das seguintes regras:

¹³ Comunicação dos dados – artigo 7.º.

- a) A entrada nas instalações utilizadas para o tratamento de dados pessoais é objecto de controlo, a fim de impedir o acesso de qualquer pessoa não autorizada;
- b) Os suportes de dados são objecto de controlo, a fim de impedir que possam ser lidos, copiados, alterados ou retirados por qualquer pessoa não autorizada;
- c) A inserção de dados é objecto de controlo para impedir a introdução, bem como qualquer tomada de conhecimento, alteração ou eliminação não autorizada de dados pessoais;
- d) Os sistemas de tratamento automatizado de dados são objecto de controlo para impedir que possam ser utilizados por pessoas não autorizadas, através de instalações de transmissão de dados;
- e) O acesso aos dados é objecto de controlo para que as pessoas autorizadas só possam ter acesso aos dados que interessem ao exercício das suas atribuições legais;
- f) A transmissão dos dados é objecto de controlo para garantir que a sua utilização seja limitada às autoridades autorizadas;
- g) A introdução de dados pessoais nos sistemas de tratamento automatizado é objecto de controlo, de forma a verificar-se que todos foram introduzidos, quando e por quem;
- h) O transporte de suportes de dados é objecto de controlo para impedir que os dados possam ser lidos, copiados, alterados ou eliminados de forma não autorizada.”

A referência apresentada [Veiga 2004] aplica-se na seguinte legislação: Base de Dados de Emissão dos Passaportes (Decreto-Lei n.º 86/2000 de 12 de Maio – artigo 14º).

“1 – À BADEP devem ser conferidas as garantias de segurança necessárias a impedir a consulta, a modificação, a supressão, o adicionamento, a destruição ou a comunicação de dados por forma não consentida pelo presente diploma.

2 – Será garantido o controlo, tendo em vista a segurança da informação:

- a) Dos suportes de dados e respectivo transporte, a fim de impedir que possam ser lidos, copiados, alterados ou retirados por qualquer pessoa ou por forma não autorizada;

- b) Da inserção de dados, a fim de impedir a introdução, bem como qualquer tomada de conhecimento, alteração ou eliminação não autorizada de dados pessoais;
- c) Dos sistemas de tratamento automatizado de dados, para impedir que possam ser utilizados por pessoas não autorizadas, através de instalações de transmissão de dados;
- d) Do acesso aos dados, para que as pessoas autorizadas só possam ter acesso aos dados que interessam ao exercício das suas atribuições legais;
- e) Da transmissão dos dados, para garantir que a sua utilização seja limitada às entidades autorizadas;
- f) Da introdução de dados pessoais nos sistemas de tratamento automatizado, de forma a verificar-se que dados foram introduzidos, quando e por quem.”

A referência apresentada [Veiga 2004] aplica-se na seguinte legislação: Registo Central dos Processos de Contra-Ordenação previstos na Lei n.º 30/2000, de 29 de Novembro (Portaria n.º 604/2001 de 12 de Junho – artigo 11º).

“1 – Sem prejuízo do disposto na legislação aplicável, são objecto de controlo, tendo em vista a segurança da informação:

- a) Os suportes de dados e os meios de transporte, a fim de impedir que possam ser lidos, copiados, alterados ou retirados por qualquer pessoa ou por qualquer forma não autorizadas;
- b) A manipulação de dados, a fim de impedir a inserção, bem como qualquer tomada de conhecimento, alteração ou eliminação, não autorizada, de dados pessoais;
- c) Os sistemas de tratamento automatizado de dados, para impedir que possam ser utilizados por pessoas não autorizadas;
- d) O acesso aos dados, para que as pessoas autorizadas só possam ter acesso aos dados que interessem ao exercício das suas atribuições legais;
- e) A transmissão de dados, para garantir que a sua utilização seja limitada a quem está para tal autorizado;
- f) A inserção, alteração e eliminação de dados pessoais no sistema, de forma a verificar-se por quem foram inseridos, alterados e eliminados, como e quando.

2 – O gestor do registo central promoverá o registo aleatório de acessos à informação, na razão de 1 para 20.”

Em termos genéricos, constata-se que, na legislação nacional, a segurança da informação é definida considerando a pertinência de controlo dos seguintes aspectos:

- (i) Acessos às instalações de tratamento de dados pessoais;
- (ii) Acessos aos suportes de dados;
- (iii) Introdução, alteração ou eliminação não autorizada de dados pessoais;
- (iv) Acesso aos sistemas de tratamento automatizado de dados;
- (v) Acesso aos dados;
- (vi) Transmissão dos dados;
- (vii) Dados introduzidos, quem introduz e quando o faz;
- (viii) Controlo da movimentação dos suportes de dados.

2.2.2. Regulamentos e Recomendações

A Comissão Nacional de Protecção de Dados (CNPd) foi criada pela Lei n.º 67/98, de 26 de Outubro, como “uma entidade administrativa independente, com poderes de autoridade, que funciona junto da Assembleia da República”. Esta Comissão foi criada como autoridade nacional cuja principal atribuição é controlar e fiscalizar o cumprimento da legislação em termos da protecção de dados pessoais, tendo como uma das principais competências a emissão de pareceres nas suas áreas de actuação [AR 1998].

Neste sentido, pela pertinência das competências definidas e pelo enquadramento que permitem da protecção da informação, deve considerar-se a relevância das recomendações da CNPD, nomeadamente as que a seguir se referenciam:

- ⇒ Princípios sobre a privacidade no local de trabalho – 29 de Outubro de 2002;
- ⇒ Princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade – 26 de Fevereiro de 2004;
- ⇒ Princípios sobre o tratamento de videovigilância – 19 de Abril de 2004.

Os princípios sobre a privacidade no local de trabalho aprovados pela CNPD [2002], consideram o tratamento de dados em centrais telefónicas, o controlo do *e-mail* e do acesso à Internet, que estabelecem um conjunto de princípios a observar por todas as partes envolvidas, assumindo a realidade dos impactos que as novas tecnologias têm na vida social e económica.

Os princípios sobre a utilização de dados biométricos no âmbito do controlo de acessos e de assiduidade aprovados pela CNPD [2004a] apresentam um conjunto de aspectos a serem considerados no respeito pelos princípios de protecção de dados, considerando a especificidade associada ao tratamento dos dados biométricos, reforçando a necessidade de cumprimento do estabelecido na Lei nº 67/98, de 26 de Outubro.

Os princípios sobre o tratamento de videovigilância aprovados pela CNPD [2004b] enquadram os aspectos associados à utilização de sistemas de videovigilância, nomeadamente a necessidade de garantir a protecção de pessoas e bens, de acordo com o especificado pela Lei nº 67/98, de 26 de Outubro.

As referidas recomendações especificam alguns dos aspectos mais importantes quando se procura enquadrar a legislação adequada à protecção de dados pessoais, particularmente no respeitante à emergência e aplicação das TIC nas sociedades e nas organizações, no âmbito das suas competências, estabelecidas pela Lei nº 43/2004, de 18 de Agosto, que define a organização e o funcionamento da CNPD.

2.2.3. Directivas da Comunidade Europeia

A referência a Directivas da Comunidade Europeia é essencial neste contexto pelo enquadramento que proporcionam acerca da problemática da segurança, e ainda pelo facto de proporcionarem as bases para o desenvolvimento de muita da legislação portuguesa acerca da segurança.

Com esse objectivo, são apenas mencionadas as Directivas com uma relação mais estreita com a problemática da segurança.

2.2.3.1. Directiva 91/250/CEE do Conselho

Esta Directiva, aprovada em 14 de Maio de 1991, é relativa à protecção jurídica dos programas de computador, englobando os direitos de autor e incluindo o respectivo material de concepção.

A sua aprovação suportou-se, entre muitas outras considerações, nos investimentos em “recursos humanos, técnicos e financeiros”, na importância crescente do papel desempenhado pelos programas de computador, nos direitos de autor, que a expressão ‘programa de computador’ “inclui qualquer tipo de programa, mesmo os que estão

incorporados no equipamento”, e que a utilização desses programas deve obedecer a critérios que não violem os direitos de autor [Dir 1991].

Referira-se no entanto que ficam salvaguardadas algumas excepções, nomeadamente a possibilidade de dispor de uma cópia de apoio, os testes e estudo do programa e mesmo a possibilidade de corrigir erros do programa.

2.2.3.2. Directiva 95/46/CE do Parlamento Europeu e do Conselho

Esta Directiva, aprovada em 24 de Outubro de 1995, é relativa à protecção das Pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses mesmos dados.

A aprovação da Directiva suportou-se essencialmente na necessidade dos “sistemas de tratamento de dados respeitarem as liberdades e os direitos fundamentais das pessoas singulares independentemente da sua nacionalidade ou da sua residência”, assim como no facto de “o recurso ao tratamento de dados pessoais nos diversos domínios das actividades económicas e sociais ser cada vez mais frequente na Comunidade”, atendendo a que “o progresso registado nas TI facilita consideravelmente o tratamento e a troca dos referidos dados” [Dir 1995].

Fora do âmbito desta Directiva ficam o tratamento de dados de som e de imagem, tais como os de vigilância por vídeo, se esse tratamento “for executado para fins de segurança pública, de defesa, de segurança do Estado ou no exercício de actividades do Estado relativas a domínios de direito penal ou no exercício de outras actividades não abrangidas pelo âmbito de aplicação do direito comunitário”.

2.2.3.3. Directiva 2002/58/CE do Parlamento Europeu e do Conselho

Esta Directiva, aprovada em 12 de Julho de 2002, é relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das Comunicações Electrónicas, revogando a Directiva 97/66/CE do Parlamento Europeu e do Conselho, de 15 de Dezembro de 1997, relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das telecomunicações, que por sua vez transpôs os princípios estabelecidos na Directiva 95/46/CE em regras específicas para o sector das telecomunicações [Dir 2002].

A Directiva foi aprovada face à necessidade de suprir os “requisitos específicos de protecção de dados pessoais e da privacidade do utilizador”, devido ao facto de estarem a “ser introduzidas nas redes de comunicações públicas da Comunidade novas tecnologias digitais avançadas”, particularmente quando o actual desenvolvimento da Sociedade da Informação se caracteriza “pela introdução de novos serviços de comunicações electrónicas”.

Esta Directiva reforça a componente de segurança, ao estabelecer que os prestadores de serviços devem adoptar as “medidas técnicas e organizativas adequadas para garantir a segurança dos seus serviços”, medidas essas que devem ter “em conta o estado da técnica e os custos da sua aplicação”, garantido assim que “essas medidas asseguram um nível de segurança adequado aos riscos existentes”.

2.2.4. Legislação Internacional

A referência a legislação internacional, maioritariamente focalizada para regulação de sectores de actividade específicos, tem como objectivo enquadrar alguns aspectos que podem ser relevantes para conhecer alguns contextos importantes na área da segurança da informação, mesmo que esses aspectos não sejam aplicados em Portugal.

Além disso, considerando-se que, em termos genéricos, o normativo da segurança da informação obriga ao cumprimento da legislação em vigor, em qualquer país ou sector de actividade, entende-se crucial mencionar alguma dessa legislação, particularmente pelo seu reconhecimento como relevante em alguns sectores de actividade.

Reconhecendo-se o elevado número de leis existentes a nível internacional, referem-se apenas algumas delas, particularmente as existentes em países onde a pertinência da segurança da informação é um factor crítico de sucesso das suas organizações e sociedades.

2.2.4.1. *Sarbanes-Oxley Act of 2002 (SOX)*

Esta lei, referenciada como Sarbanes-Oxley Act of 2002 (SOX), foi aprovada pelo Senado e Câmara de Representantes dos Estados Unidos da América, em 2002.

Com um claro impacto nas instituições financeiras, esta lei torna obrigatórios controlos e *standards* para as declarações financeiras, de modo a assegurar a integridade da informação dos relatórios financeiros [SOX 2002].

Esta lei torna os gestores de topo das empresas públicas responsáveis pelas falhas em providenciar informação atempada, completa e precisa para os interessados no estado do desempenho das organizações.

Enquanto que esta lei não é específica acerca dos requisitos tecnológicos, outra legislação implica que as instituições implementem e mantenham um ambiente de controlo das TI, para apoiar a confiança, a transparência e a exactidão da informação financeira.

Esta lei implica por isso que os processos devem estar nos seus lugares, permitindo que auditores, gestores de topo e administradores adquiram um entendimento detalhado do desempenho dos negócios e dos números reportados a pedido.

2.2.4.2. Health Insurance Portability and Accountability Act (HIPAA)

Esta lei foi aprovada pelo Senado e Câmara de Representantes dos Estados Unidos da América, em 1996, sendo referenciada como *Health Insurance Portability and Accountability Act* (HIPAA, Lei Pública 104-191).

Posteriormente, em 2003, foi aprovada uma Regra de Segurança (referenciada como *HIPAA Security Rule*) que constitui os *standards* de segurança para uma informação de confiança em saúde [Hash *et al* 2005].

Adicionalmente ao assegurar a portabilidade do seguro de saúde, a HIPAA estipula um número de requisitos respeitantes à segurança e privacidade da informação do paciente [HIPAA 1996].

Embora isto pareça apenas relevante para a indústria dos cuidados de saúde, qualquer organização que transmita e armazene informação de saúde de pacientes, incluindo informação de benefícios e reclamações de funcionários, está sujeita às regras da HIPAA.

O principal objectivo desta Regra de Segurança é assegurar que a informação de saúde de qualquer pessoa está adequadamente protegida, enquanto é permitido o fluxo da informação de saúde necessária a proporcionar e promover cuidados de saúde de alta qualidade e para proteger a saúde e o bem-estar públicos.

Esta Regra procura um compromisso que permita usos importantes da informação, enquanto protege a privacidade das Pessoas que procuram cuidados de saúde,

obedecendo o seu desenho à indispensabilidade de ser flexível e compreensível de modo a cobrir uma variedade de usos e descobertas que necessitam de ser dirigidas.

2.2.4.3. *Personal Information Protection and Electronic Documents Act (PIPEDA)*

Aprovada em 13 de Abril de 2000 pelo Senado e Câmara dos Comuns do Canada, esta lei é referenciada como *Personal Information Protection and Electronic Documents Act* (PIPEDA).

Esta lei é constituída por cinco partes [PIPEDA 2000]:

Parte 1 – Estabelece o direito de protecção da informação pessoal recolhida, utilizada e divulgada no decurso de actividades comerciais definindo princípios relacionados, tais como: responsabilidade, identificação dos propósitos, obtenção de consentimento, limitações à recolha e utilização, disponibilização e retenção, segurança, proporcionando ainda o acesso das Pessoas aos seus dados pessoais.

Parte 2 – Define o esquema legislativo pelo qual os requisitos dos estatutos federais e outra legislação podem contemplar ou não o uso de papel ou tecnologia electrónica, garantindo a autoridade para legislar acerca de como os requisitos podem ser satisfeitos por meios electrónicos.

Parte 3 – Altera o *Canada Evidence Act* para facilitar a admissibilidade dos documentos electrónicos e outros pressupostos relacionados com as assinaturas digitais.

Parte 4 – Altera o *Statutory Instruments Act* para autorizar a publicação da Gazeta do Canada por meios electrónicos.

Parte 5 – Altera o *Statute Revision Act* para autorizar a publicação e distribuição de uma versão electrónica dos Estatutos e Leis do Canada.

Posteriormente, em 2004, foram elaborados e disponibilizados dois guias com as responsabilidades enquadradas por esta lei: um para os Negócios e Organizações e outro para as Pessoas.

2.3. Conclusões

A utilização do normativo adequado a suportar a definição e implementação de políticas de segurança ou dos mais abrangentes SGSI, apresenta-se como uma opção viável para responder a muitos dos problemas em termos de segurança com que as organizações actualmente se deparam.

Com esse objectivo foram analisadas 30 normas relacionadas directa ou indirectamente com a temática referida, procurando-se entender os principais aspectos abrangidos, considerando a necessidade, num estudo desta natureza, de obter um enquadramento normativo adequado ao suporte das políticas de segurança da informação.

No respeitante aos aspectos legais relativos à segurança (entendida aqui em termos genéricos, uma vez que se relacionam com a utilização das TIC e das prova cidade dos dados pessoais), constata-se a existência de mecanismos legais, quer em termos nacionais quer em termos europeus, adequados a suportar as necessárias directrizes para as actividades organizacionais.

Neste âmbito considera-se também importante a obtenção de uma perspectiva global acerca da diversa legislação sobre esta temática, assumindo a necessidade, de acordo com o estabelecido nas normas de boas práticas, considerar essa legislação a quando da concepção e implementação de SGSI.

Referências bibliográficas

Assembleia da República, “Lei da Criminalidade Informática”, Lei n.º109/91, de 17 de Agosto, Diário da República n.º188, I Série-A.

Assembleia da República, “Lei da Protecção Jurídica de Programas de Computador”, Lei n.º 252/94, de 20 de Outubro, Diário da República n.º243, I Série-A.

Assembleia da República, “Lei da Protecção de Dados Pessoais”, Lei n.º67/98, de 26 de Outubro, Diário da República n.º247, I Série-A.

Assembleia da República, “Lei das Comunicações Electrónicas”, Lei n.º5/2004, de 10 de Fevereiro, Diário da República n.º34, I Série-A.

Assembleia da República, “Lei da Protecção da Privacidade no Sector das Comunicações Electrónicas”, Lei n.º41/2004, de 18 de Agosto, Diário da República n.º194, I Série-A.

- Bowen, P., Hash, J. and Wilson, M., *Information Security Handbook: A Guide for Managers*, Special Publication 800-100, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2006.
- BS, *BS ISO/IEC 20000-1 – Information Technology - Service Management – Specification*, British Standard Institution, 2005.
- BS, *BS ISO/IEC 20000-2 – Information Technology - Service Management - Code of practice*, British Standard Institution, 2005.
- BS, *BS 7799-3 – Information - Management Systems - Guidelines for Information Security Risk Management*, British Standard Institution, 2006.
- BSI, *IT Baseline Protection Manual*, Bundesamt für Sicherheit in der Informationstechnik (BSI, Federal Office for Information Security), 2004.
- Chew, E., Clay, A., Hash, J., Bartol, N. and Brown, A., *Guide for Developing Performance Metrics for Information Security*, Special Publication 800-80 (Initial Public Draft), National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2006.
- CISP, *Cardholder Information Security Program (CISP)*, Visa U.S.A. Inc., 2004.
- COBIT, *Control Objectives for Information and related Technology (Version 4.0)*, IT Governance Institute, 2005.
- Comissão Nacional de Protecção de Dados, “Princípios sobre a privacidade no local de trabalho”, 29 de Outubro de 2002, <http://www.cnpd.pt/bin/orientacoes/principiostrabalho.htm> (10-05-2005).
- Comissão Nacional de Protecção de Dados, “Princípios sobre a utilização de dados biométricos”, 26 de Fevereiro de 2004, <http://www.cnpd.pt/bin/orientacoes/principiosbiometricos.htm> (10-05-2005).
- Comissão Nacional de Protecção de Dados, “Princípios sobre o tratamento de dados por videovigilância”, 19 de Abril de 2004, <http://www.cnpd.pt/bin/orientacoes/principiosvideo.htm> (10-05-2005).
- Directiva 91/250/CEE do Conselho, 14 de Maio de 1991, “Protecção jurídica dos programas de computador”, Jornal Oficial das Comunidades Europeias n.º L 122 de 17 de Maio de 1991.
- Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, “Protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à

livre circulação desses dados”, Jornal Oficial das Comunidades Europeias n.º L 281 de 23 de Novembro de 1995.

Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, “Privacidade e comunicações electrónicas”, Jornal Oficial das Comunidades Europeias n.º L 201/37 de 31 de Julho de 2002.

Fraser, B. (Editor), *RFC 2196 The Site Security Handbook*, Software Engineering Institute - Carnegie Mellon University, 1997.

GAISP, *Generally Accepted Information Security Principles (Version 3.0)*, Information Systems Security Association (ISSA), 2003.

Grance, T., Hash, J. and Stevens, M., *Security Considerations in the Information System Development Life Cycle*, Special Publication 800-64, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2003.

Grance, T., Kent, K. and Kim, B., *Computer Security Incident Handling Guide*, Special Publication 800-61, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2004.

Hash, J., Bowen, P., Johnson, A., Smith, C.D. and Steinberg, D.I., *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, Special Publication 800-66, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2005.

HIPAA, *Health Insurance Portability and Accountability Act*, Public Law 104-191, Senate and House of Representatives of the United States of America, 1996.

ISF, *The Standard of Good Practice for Information Security (Version 4.1)*, Information Security Forum (ISF), 2005.

ISO, *ISO/IEC 21827 – Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM)*, International Standard Organization, 2002.

ISO, *ISO/IEC FDIS 13335-1 – Information technology - Guidelines for the management of IT security - Concepts and models for information and communications technology security*, International Standard Organization, 2004.

ISO, *BS ISO/IEC 17799 (BS 7799-1:2005) – Information Technology - Code of practice for information security management*, British Standard Institution, 2005.

- ISO, *BS ISO/IEC 27001 (BS 7799-2:2005) – Information Technology - Security Techniques - Information Security Management Systems - Requirements*, British Standard Institution, 2005.
- ISSAF, *Information Systems Security Assessment Framework (draft 0.2)*, Open Information Systems Security Group, 2005.
- ITIL, *Information Technology Infrastructure Library (Version 2.0)*, Office of Government Commerce of United Kingdom Government, 2001.
- National Institute of Standards and Technology (NIST), *An Introduction to Computer Security: The NIST Handbook*, Technology Administration - U.S. Department of Commerce, Special Publication 800-12, 1998.
- OECD, *Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*, Organisation for Economic Co-operation and Development, 2002.
- PIPEDA, *Personal Information Protection and Electronic Documents Act*, House of Commons of Canada, 2000.
- Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G. and Lee, A., *Recommended Security Controls for Federal Information Systems*, Special Publication 800-53, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2005.
- Rudd, C., *An Introductory Overview of ITIL*, IT Service Management Forum (itSMF), 2004.
- SOX, *Sarbanes-Oxley Act*, Senate and House of Representatives of the United States of America, 2002.
- Stoneburner, G., *Underlying Technical Models for Information Technology Security*, Special Publication 800-33, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2001.
- Stoneburner, G., Goguen, A. and Feringa, A., *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2001.
- Stoneburner, G., Hayden, C. and Feringa, A., *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, Special Publication 800-27, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2001.

- Swanson, M., *Guide for Developing Security Plans for Information Technology Systems*, Special Publication 800-18, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 1998.
- Swanson, M., *Security Self-Assessment Guide for Information Technology Systems*, Special Publication 800-26, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2001.
- Swanson, M., Bartol, N., Sabato, J., Hash, J. and Graffo, L., *Security Metrics Guide for Information Technology Systems*, Special Publication 800-55, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2003.
- Swanson, M. and Guttman, B., *Generally Accepted Principles and Practices for Securing Information Technology Systems*, Special Publication 800-14, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 1996.
- Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J. and Thomas, R., *Contingency Planning Guide for Information Technology Systems*, Special Publication 800-34, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2002.
- Veiga, A., *Legislação de Direito da Informática*, Coimbra Editora, 2004.
- Wilson, M. (editor), Zafra, D., Pitcher, S., Tressler, J. and Ippolito, J., *Information Technology Security Training Requirements: A Role -and Performance- Based Model*, Special Publication 800-16, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 1998.

3

Informação, Sistemas e Tecnologias de Informação e Comunicação

A relevância da informação para as necessidades humanas tem sido um factor fundamental ao longo do processo evolutivo, mas a assumpção plena desse facto apenas foi feita nas últimas décadas, mercê do contributo proporcionado pela evolução das TIC, que possibilitaram saltos qualitativos e quantitativos na aquisição, tratamento e partilha da informação.

No actual contexto de relevância da informação, Zorrinho [1991] considera-a como um factor crítico de sucesso para as organizações que apostam em mercados turbulentos e altamente concorrenciais, referenciando no entanto que a informação só pode ser útil na prossecução dos objectivos da organização se for fiável e oportuna.

Esta focalização na pertinência, adequação e importância da informação para as actividades organizacionais, impõe uma atenção especial para com os recursos organizacionais (humanos, tecnológicos e financeiros) que são afectados à sua utilização, assim como para os SI e para as TIC que possibilitam essa utilização.

Acresce ainda a necessidade da relevância, formato e qualidade da informação que é partilhada, particularmente quando essa informação se destina a utilizadores que não possuem competências específicas em SI e TIC.

3.1. As Organizações e a Globalização

Ao longo da sua evolução os seres humanos têm adaptado as tecnologias às suas necessidades, produzindo instrumentos que, de forma gradual e contínua, lhes permitiram ultrapassar as suas naturais limitações e melhorar a qualidade de vida. Esta adaptação das tecnologias tem abrangido todas as actividades humanas, ganhando especial relevância com a emergência de uma Sociedade da Informação que, potenciada pela globalização, trouxe novos desafios onde a informação assume claramente o papel

central, comportando novos e mais exigentes desafios a que as Pessoas procuram responder.

Este novo contexto, globalização, é encarado por Giddens [2000], como sendo político, tecnológico e cultural, além de também considerar a globalização como sendo económica, fazendo notar que esta não é um processo simples mas sim uma rede complexa de processos, pelo que entende dever ser feita uma distinção entre globalização vista em termos gerais e a globalização económica (que apenas é controlada por organizações de âmbito mundial).

Numa definição formal de globalização, esta é apresentada como o processo de integração dos mercados resultante da expansão da concorrência e dos impactos das TIC a uma escala planetária [APDSI 2005].

Conduzindo à abolição de barreiras às importações e à movimentação de recursos humanos, a globalização económica impõe, segundo Caldeira e Romão [2002b], a definição de mecanismos que permitam reduzir custos e diferenciar produtos e serviços no sentido de competir num mercado mais alargado.

Assumindo o papel central no contexto anteriormente referido, a informação constitui-se assim como um aspecto essencial à vida humana desde os seus primórdios, quer na identificação dos locais de alimentação e habitação, quer para utilização do que a natureza disponibilizava, independentemente das dificuldades associadas a essas actividades. Todavia, a evolução tecnológica possibilitou que, através da utilização das TIC, o processo de partilha de informação fosse simplificado, permitindo assim aumentar a sua disponibilidade e rapidez de partilha, acompanhando as necessidades colocadas pelo surgimento de novos interesses.

Segundo Zorrinho [1991], a informação, seja como matéria-prima, como produto intermédio ou como componente essencial do produto final, força a existência de “uma forte polarização da empresa em torno das unidades elementares que são os seus trabalhadores e em torno da rede complexa que entre eles se estabelece”.

Neste contexto, as TIC são consideradas como uma componente activa de aquisição de vantagens competitivas na organização, pois segundo Ciborra and Andreu [1998] permitem transformar recursos em capacidades e por vezes em capacidades distintivas

assumindo-se como marcadoras da diferença e factor diferenciador na aquisição de vantagens competitivas.

Deve por isso atender-se ao facto de a qualidade de utilização do sistema envolver não só as Pessoas mas também as TIC e as organizações, de acordo com a missão e objectivos de negócio definidos e ainda com os recursos disponibilizados para a prossecução das suas actividades.

Este conjunto de aspectos surge reforçado por Anunciação e Zorrinho [2006], que identificam três factores como os principais responsáveis pelo novo enquadramento das organizações:

- (1) A globalização dos mercados e das actividades;
- (2) As TIC;
- (3) As Pessoas.

Estes autores referem ainda que destes três factores resultam como consequências imediatas “o aumento dos níveis de eficiência das actividades económicas, dos índices de inovação e do poder dos clientes”. Esta envolvente estabelecida, permite a percepção de novos e mais exigentes desafios com que as organizações se confrontam, exigindo novas abordagens e soluções que envolvam claramente as TIC e as Pessoas como factores críticos de sucesso no novo contexto da sociedade.

Os desafios são então colocados num contexto onde, segundo Santos e Ramos [2006], é difícil o estabelecimento de fronteiras claras entre a organização e o seu ambiente, dificultando a percepção da direcção (interna ou externa) atribuída às actividades, em especial quando são cada vez mais próximas as ligações da organização com os seus diversos parceiros (concorrentes, fornecedores, clientes), perante as vantagens adquiridas, em termos de conhecimento, capacidades, competências e experiência, pela sua actuação conjunta.

Martin *et al* [2002] entendem uma organização como sendo um conjunto funcional e integrado de quatro componentes fundamentais, cuja identificação e interacções podem ser observadas na figura seguinte.

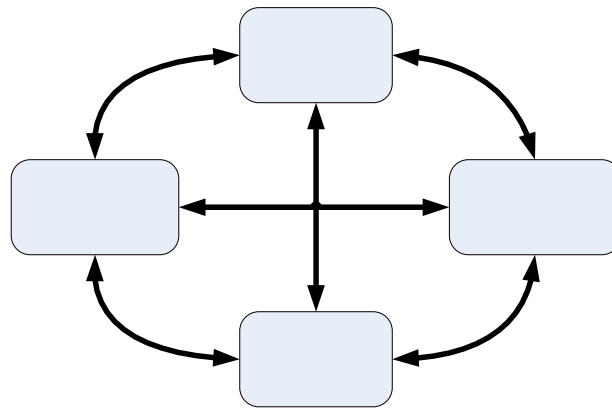


Figura 3.1 – Componentes fundamentais de uma organização
(Adaptado de Martin et al [2002])

De entre estes componentes de uma organização torna-se importante verificar que a relevância das Pessoas e das TIC se apresenta com significado capaz de afectar os contextos em que se aplicam. As inter relações que se estabelecem tornam-se um factor de contextualização dos seus impactos e contributos que proporcionam às organizações.

ESTRUTURA ORGANIZACIONAL

Segundo Drucker [2000], existem diferenças de gestão entre organizações diferentes, considerando que “a missão define, afinal, a estratégia e a estratégia define a estrutura”. O autor refere ainda que as organizações não são algo de absoluto, constituindo um instrumento destinado a “rendibilizar o trabalho conjunto dos recursos humanos”, ou seja, numa organização, uma dada estrutura “é adequada a determinadas tarefas em determinadas condições e em determinadas alturas”.

PROCESSOS NEGOCIAIS

Considerando este enquadramento proporcionado por Drucker, onde a missão e a estratégia da organização definem a sua estrutura, pode inferir-se que, de modo idêntico, também as Pessoas, as TIC e os processos, são afectados pela estratégia organizacional.

Neste âmbito, Pipkin [2006] entende missão como a razão de ser da organização, definindo claramente o que a organização deve cumprir, enquanto que à estratégia compete definir como os planos devem cumprir a sua missão, ou seja, escolher que actividades ou programas são apropriados para atingir os seus propósitos.

Este contexto permite considerar que os SI e as TIC viabilizam “a consolidação de visões, estratégias e objectivos económicos e sociais” que emergem como os principais alicerces nas respostas “das organizações económicas ao mercado” [Anunciação e Zorrinho 2006].

Cabe assim aos SI, considerando a globalização dos mercados, as TIC e as Pessoas, actuar como congregadores das necessidades organizacionais, permitindo que as Pessoas utilizem eficiente e eficazmente as TIC para responder aos desafios organizacionais colocados pelo actual contexto de globalização.

Neste âmbito, Serrano *et al* [2004] referem um ambiente complexo e turbulento (motivado pela crescente globalização dos mercados, aumento das exigências dos consumidores, e uma maior concorrência), onde a informação emerge como recurso fundamental para a sobrevivência das organizações, ao possibilitar a ultrapassagem da incerteza associada à tomada de decisão, assumindo um papel estratégico na obtenção de vantagens competitivas.

Paralelamente com o crescimento e evolução das organizações, Rodrigues [2002] refere um aumento da sua complexidade e das necessidades de informação, o que implica maiores exigências em termos do desempenho dos SI no sentido de responder adequada e atempadamente aos desafios a que necessitam de responder.

Pode assim constatar-se que a evolução das TIC, complementarmente com o reconhecimento da importância da informação como factor crítico de sucesso das organizações, permite que aquelas suportem a evolução necessária dos SI, em resposta ao referido crescimento das exigências que se lhes colocam.

Relativamente aos SI, a sua integração nas organizações comporta desafios a que importa responder e que tem implicações na actividade organizacional, onde o nível de integração e adequação às suas necessidades é certamente um factor determinante. Laudon and Laudon [2000] referem a propósito que os gestores se confrontam actualmente com cinco desafios fundamentais:

- (1) Negócios estratégicos: como se pode utilizar as TIC para desenhar organizações que sejam competitivas e eficazes?
- (2) Globalização: como podem as empresas entender os negócios e requisitos de sistemas num ambiente económico global?
- (3) Arquitectura de Informação: como podem as organizações desenvolver uma arquitectura de informação e uma infra-estrutura tecnológica para suportar os seus objectivos de negócio?

- (4) Investimentos em SI: como podem as organizações determinar o valor de negócio dos SI?
- (5) Responsabilidade e Controlo: como podem as organizações desenhar sistemas que as Pessoas possam controlar e entender?

Face ao exposto é possível concluir que a usabilidade dos SI e a segurança da informação partilhada pelos SI, assim como a sua adequação à estratégia das organizações, podem constituir factores de sucesso, desempenhando papéis fundamentais no suporte às suas actividades de negócio, o que reforça a necessidade de perceber os impactos provocados pelas mudanças impostas.

3.2. Informação

Referenciando a complexidade do mundo moderno e a sua evolução, Cerveira [1967] considera que o homem depende “quase exclusivamente das informações que recebe e da rapidez com que pode contar com essas informações”.

Neste sentido, a compreensão do papel da informação nas organizações requer que se proceda previamente à definição do que se entende por informação. De entre a diversidade de definições, informação é entendida como sendo dados tratados e “dotados de relevância e de um objectivo” [Drucker 1993], ou ainda como dados com um significado particular e colocados num contexto específico [Haag *et al* 1998, Zwass 1998, Alter 1999], podendo, segundo Zorrinho [1991], constituir-se como um factor crítico de sucesso em mercados turbulentos e altamente concorrenciais, ou então como um recurso que pode ser reutilizado, partilhado, distribuído ou trocado sem que inevitavelmente haja uma perda de valor [Earl 2000].

Neste contexto, Cerveira [1967] menciona que a “aquisição de informação acerca de um sistema complexo” é realizada através da recolha de dados, que segundo refere nem sempre fornecem de forma directa a informação pretendida, pelo que se torna necessário efectuar o seu processamento para a obtenção de informação utilizável, considerando que “os dados recolhidos (mensagens) são simplesmente o veículo da mesma informação”

Todavia, para ser possível um entendimento cabal de informação torna-se necessário que se defina previamente o que são dados, assumindo por exemplo a definição de

Laudon and Laudon [2000] que apresentam dados como sendo conjuntos de factos simples representando eventos ocorridos numa organização ou no seu ambiente físico, antes de serem organizados e ordenados num formato que as Pessoas possam entender e usar. Já Serrano e Fialho [2003] entendem dados como “um conjunto de factos discretos e objectivos sobre os acontecimentos”.

De forma similar, Dinis [2005] define dados como “conjuntos de elementos discretos, não organizados, compostos por números, palavras, sons ou imagens independentes, e que podem ser facilmente estruturados”, e informação como “um conjunto de dados organizados, padronizados, agrupados e/ou categorizados que dizem respeito a uma descrição, definição ou perspectiva”. Este autor refere ainda o facto de o nível de estruturação dos dados e da informação aumentarem com a intervenção das Pessoas sobre esses dados e informação.

Estas definições possibilitam a constatação de que os ‘dados’ são os factos simples, por si só, permitindo assumir que ‘informação’ são ‘dados’ com um significado particular num contexto específico, onde estes podem constituir a matéria-prima para a obtenção de ‘informação’, com a conversão dos ‘dados’ em ‘informação’ a ser concretizada pelos SI.

Perante isto, na perspectiva de Serrano e Fialho [2003], é a atribuição de significado aos dados, a sua contextualização, tratamento, combinação, e também o estabelecimento de relações resultantes dessas actividades que permitem a sua caracterização como informação.

Pode então constatar-se que informação, numa definição comumente aceite, corresponde ao resultado obtido com o tratamento de dados considerados relevantes e que atendem a um âmbito previamente determinado. Pode todavia considerar-se uma definição formal, onde informação são dados organizados e comunicados de forma coerente e com um significado, retirando-se conclusões desses mesmos dados [APDSI 2005].

Esta situação é tanto mais relevante quanto, segundo Drucker [1999], as necessidades de informação estão em mudanças constantes levando a que se tenha em atenção não apenas a informação interna, como era usual, mas também a informação externa. Estes

factos conduzem à existência de maiores volumes de informação e fazem emergir a necessidade de métodos mais rigorosos para tratar e analisar essa informação.

A figura seguinte apresenta um enquadramento genérico que perspectiva a informação nas suas diversas envolventes, considerando o ponto de vista das organizações e a dimensão global que a informação detêm actualmente, com esta a ser entendida em três domínios distintos: de negócio, interno e externo.

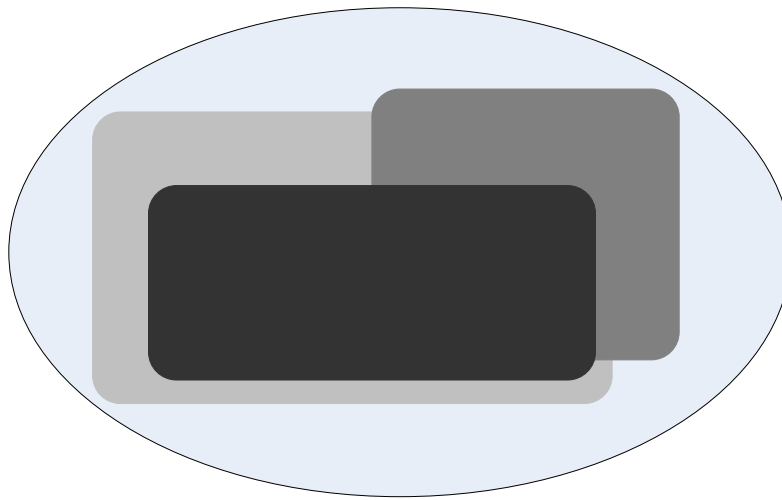


Figura 3.2 – Contexto informacional
(Adaptado de Drucker [1999])

A informação de negócio engloba tudo o que diz respeito a clientes, produtos, fornecedores, ou seja, tudo o que se relaciona estritamente com o negócio. A informação interna comporta todos os processos internos não relacionados com o negócio, onde se engloba toda a informação relacionada com os aspectos comunicacionais e organizacionais internos. A informação externa por seu lado enquadra a envolvente da organização e pode constituir a maior fonte de informação.

Informação externa

Neste contexto torna-se importante garantir a integridade e segurança da informação nos seus diversos domínios. A recolha, selecção, tratamento, armazenamento e disponibilização de informação assumem aspectos distintos perante cada um dos domínios da informação, anteriormente especificados.

Deve todavia referenciar-se que a definição de informação é feita habitualmente segundo perspectivas e interesses específicos, de cada um dos seus potenciais utilizadores ou dos interessados na sua utilização, conduzindo a que o entendimento da

necessidade da sua gestão e relevância tenha perspectivas e importâncias diferentes em cada caso concreto.

Por seu lado, Garcia [2005] considera a informação como uma “unidade cognitiva envolvida em processos de comunicação nos quais o contexto, a intencionalidade e a motivação dos actores são atributos fundamentais”, assumindo valores diferentes em função das Pessoas que a utilizam. Desta perspectiva resulta que a informação será sempre condicionada pelo contexto em que for utilizada e pela actuação dos intervenientes nos respectivos processos, considerando essencialmente a relevância que a informação assume para as actividades organizacionais.

Por conseguinte, segundo Correia [2006], o importante é que a informação seja integrada nas diversas áreas organizacionais, independentemente do modo como essa informação é entregue, referenciando todavia a necessidade desta ser “apresentada de forma precisa, consistente e viável para todos os que necessitam dela”.

Considerando a informação como um recurso estratégico da organização, Reis e Amaral [2002] referem ser fundamental, em termos estratégicos, identificar a informação importante e as respectivas fontes, de forma a assegurar que essa informação chega a todos os envolvidos, procurando assim aumentar a eficiência e eficácia do seu processamento, de modo a possibilitar a optimização do negócio.

Contexto no qual, segundo Anunciação e Zorrinho [2006], “a informação, ao assumir o papel de recurso principal”, surge como recurso económico cuja facilidade de aquisição, manipulação e distribuição condiciona as actividades das Pessoas nas organizações.

Uma perspectiva similar considera que a informação constitui o recurso estratégico da organização, entendendo-a como mais do que um mero factor de produção, ao permitir uma combinação e utilização eficaz dos outros factores de produção, potenciando o desempenho organizacional [Choo 2003].

Pelo que o reconhecimento da informação como um recurso obriga à sua gestão como tal, levando à necessidade de uma estrutura que possibilite a sua disponibilização no momento exacto, com o formato adequado e na quantidade necessária, considerando como relevante o facto de apenas nos últimos anos se ter reconhecido a sua importância estratégica [Oliveira e Amaral 2000].

Considerando-se a pertinência de proceder à gestão da informação, Haag *et al* [1998] entendem essencial considerar a relevância dos seguintes aspectos:

- Papel da informação na organização;
- Acesso da gestão à informação;
- Direcção da protecção da informação relativamente a perdas e avarias (segurança) e de abusos (privacidade).

Neste contexto, de acordo com os mesmos autores, a informação pode desempenhar o papel de matéria-prima (quando está na base de desenvolvimento de um produto) ou como capital (quando é usada para providenciar um produto que vai de encontro aos desejos do cliente). O capital informação pode assim ser considerado como um dos mais importantes e universais tipos de capital numa organização, particularmente quando se verifica o facto muito simples de nem todas as organizações construírem ou desenvolverem produtos, mas todas elas terem informação, o que levanta desde logo o problema da determinação do valor desta.

Em termos de valor da informação, Rodrigues [2002] considera a sua variação em função dos factores influenciadores da sua interpretação e uso, para além da sua necessidade e utilização. Neste sentido, além do anteriormente referenciado, identifica como relevantes os seguintes factores: acessibilidade, actualidade, oportunidade, precisão, flexibilidade, facilidade de interpretação, ambiguidade, vulnerabilidade, quantificação, agregação, estruturação, abrangência, relevância, posse e custo.

Neste âmbito, segundo Zorrinho [1999], perante o contexto actual do que define como um “mundo saturado de informação”, o valor da informação para as organizações não existe na disponibilização bruta dos dados mas sim na “capacidade de os usar de forma útil”.

Esta percepção é reforçada por Correia [2006] ao assumir o facto de a obtenção de informação ser sempre importante, com o grande desafio a residir em encontrar informação relevante, em tempo útil, perante as elevadas velocidades com que esta surge e aos volumes de informação que se encontra disponível.

Sendo a informação, segundo Zorrinho [1999], entendida como “um modelo de representação do real” mas também como um suporte da decisão e a respectiva envolvente, a gestão da informação deve ser encarada como uma função de nível

estratégico, que permite a interligação da concepção dos SI com a concepção dinâmica da organização. Por seu lado, Rodrigues [2002] considera que o contributo da gestão do recurso informação para o sucesso das organizações reside na disponibilização da “informação necessária para as pessoas certas, no tempo certo e da maneira mais eficiente e com os menores custos”.

Pode assim considerar-se que, perante a quantidade e a diversidade de informação que actualmente se encontra disponível, particularmente devido às potencialidades apresentadas pelas TIC, emerge a necessidade de dedicar especial atenção à sua escolha e utilização. Neste âmbito, a velocidade a que se processa a aquisição, processamento e partilha de informação, força a que os problemas inerentes à sua gestão venham a fazer parte das preocupações dos decisores organizacionais.

Numa perspectiva complementar, informação é definida no Relatório FRISCO (*Framework of Information Systems Concepts*) [Falkenberg *et al* 1998], como a diferença entre os conceitos interpretados de uma mensagem recebida e o conhecimento antes da acção de recepção, verificando-se assim um incremento do conhecimento ao dispor da organização.

Passando de mero instrumento de apoio às actividades organizacionais para o centro das “actividades das económicas, sociais, culturais, políticas e mesmos militares”, a informação surge como um activo organizacional, considerando-se que a sua transformação em conhecimento pode constituir um valor em termos de capital intelectual, “associado aos processos, às pessoas e às tecnologias” [Dinis 2005].

Conhecimento é aliás referenciado por Dinis [2005] como a “informação associada a uma experiência, que compreende uma estratégia, uma prática, um método ou uma abordagem”, referindo a sua especificação em dois tipos: conhecimento explícito (documentos e outros suportes de informação) e conhecimento tácito (Pessoas).

Neste mesmo âmbito, Garcia [2005] refere conhecimento como sendo o desfecho de um processo complexo que vai desde a emissão de informação até à interpretação dessa informação, considerando as aptidões e competências das Pessoas, através das quais o conhecimento existe na organização, realçando ainda que o conhecimento também pode existir em documentos, normas, rotinas, práticas, etc.

Por seu lado, Serrano e Fialho [2003] entendem Conhecimento como “a interpretação dos dados e da informação”, considerando-o um conjunto de experiências, valores e criatividade aplicado num adequado contexto de informação, referenciando ainda que este se encontra “na rotina, na prática, no comportamento”.

Esta situação é tanto mais relevante quando, segundo Peltier [2002], as TIC e a informação que suportam são muitas vezes consideradas como activos críticos que suportam a missão da organização, pelo que a sua protecção é tão importante quanto a protecção de outros recursos organizacionais como sejam os financeiros, os activos físicos ou os próprios funcionários.

3.3. Sistemas de Informação

Conhecer e utilizar SI pressupõe um entendimento claro e objectivo do que é um sistema e em que consistem os seus componentes. Assim sendo, o entendimento de sistema confronta-se desde logo com a existência de diversas definições e perspectivas.

Um sistema é então entendido como um conjunto de componentes interligados que actuam concertadamente com um determinado propósito [Zwass 1998, Alter 1999]. Com sentido idêntico, refira-se a perspectiva de Rivas [1989], que se lhe refere como um conjunto de elementos, relacionados entre si, actuando num determinado ambiente, com o fim de alcançar objectivos comuns e com capacidade de auto controlo.

As definições anteriores permitem assumir que sistema é, considerando a sua forma mais simples, um conjunto de componentes que actuam de forma concertada visando a prossecução de um objectivo comum. A organização é um exemplo comum de sistema, frequentemente entendida como um sistema formal (um exemplo comum de sistema informal é proporcionado pelas Pessoas e pelas interacções que estas estabelecem entre si), ou seja, como um sistema que se suporta em definições fixas e consensuais de dados e procedimentos, operando segundo regras previamente estabelecidas. Os componentes dos sistemas podem ser elementares ou subsistemas¹⁴ e os seus objectivos podem ser múltiplos.

Note-se todavia, como aspectos fundamentais para uma percepção clara do seu funcionamento, que todos os sistemas possuem um Propósito (razão de ser para a sua

¹⁴ Subsistema é um componente de um sistema que também pode por si só ser considerado um sistema.

existência), uma Fronteira (definindo o que está fora e o que está dentro do sistema), um Ambiente (tudo o que está fora das suas fronteiras e é pertinente para o sistema) e um conjunto de Inputs (objectos ou informação que vinda do ambiente atravessa as fronteiras do sistema) e Outputs (objectos ou informação que vão do sistema para o ambiente) [Alter 1999].

Referenciando as organizações como sistemas sociais, Ferreira [2001] entende que são o resultado de interdependências e interações “entre os seus subsistemas estruturais e funcionais”, referindo neste mesmo âmbito que as organizações, enquanto sistemas abertos, “interagem de forma sistemática com o ambiente circundante, importando e exportando energia, informação e matéria na forma de *outputs* e *inputs*”.

Refira-se ainda a existência, frequente e praticamente indissociável do contexto, de mecanismos de controlo e auto regulação que procedem aos ajustes necessários interferindo nas actividades do sistema, de acordo com o funcionamento pretendido, através da validação dos *outputs*.

Genericamente, um sistema destina-se a suportar os processos de negócio das organizações, onde processo de negócio pode ser entendido como um conjunto relacionado de tarefas ou actividades que usam Pessoas, informação e outros recursos para criar valor para os seus clientes internos e externos.

Estas tarefas estão relacionados no tempo e no espaço, tem princípio e fim, assim como *inputs* e *outputs*. Um esquema básico de sistema pode ser observado na figura seguinte e inclui frequentemente (como já observado), além de entradas, processamento (actividade desenvolvida pelo sistema) e saídas, a possibilidade de controlar se as saídas estão de acordo com o pretendido.

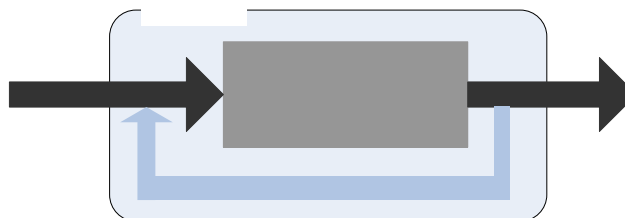


Figura 3.3 – Esquema básico de um sistema
(Adaptado de Alter [1999])

Constata-se assim, tal como acontece com a informação e com os sistemas, cujas definições atendem a perspectivas pessoais e culturais, também os SI são objecto de vários entendimentos. Zwass [1998], por exemplo, considera-os como conjuntos organizados de componentes para recolher, transmitir, armazenar e processar dados com vista ao fornecimento de informação para suporte às actividades organizacionais, enquanto que Alter [1999] os entende como sistemas que usam as TIC para capturar, transmitir, armazenar, recuperar ou disponibilizar informação, ou ainda como sendo uma função que visa a gestão do recurso informação e o como esta é recolhida, armazenada, processada e distribuída segundo a perspectiva de Carvalho e Amaral [1993], Ward [1995] por seu lado, apresenta uma perspectiva idêntica considerando-o como parte integrante dos processos de qualquer organização que procede à recolha, armazenamento e processamento de informação. Verificando-se assim que o objectivo fundamental de qualquer SI é processar a informação e disponibiliza-la segundo critérios definidos e recorrendo às TIC para suportar essas funções.

Antes da automatização por computador, os dados acerca das Pessoas ou organizações eram mantidos e salvaguardados como registos em papel, dispersos em unidades de negócio e organizacionais distintas. Todavia, a situação alterou-se radicalmente uma vez que os SI concentram dados em ficheiros de computador, que potencialmente podem ser acedidos mais facilmente por um largo número de Pessoas e por indivíduos ou grupos de fora da organização. Consequentemente, dados automatizados são mais susceptíveis à destruição, fraude, erro e má utilização [Laudon and Laudon 2000].

Esta situação comportou novas necessidades e forçou alterações profundas e radicais nas actividades organizacionais, que se reflectiram não só nos processos de negócio, mas também na sua estrutura interna e consequentemente nos SI e nas TIC que suportam essas actividades.

Considerando a dependência dos negócios relativamente aos SI, Reis e Amaral [2002] referem a necessidade de se proceder a um equacionamento rigoroso dessa dependência, assumindo que os decisores devem preocupar-se com a recuperação rápida e eficiente da actividade após um acidente, procurando simultaneamente a minimização dos efeitos desse acidente.

Neste âmbito, Coelho [2005] considera que a especificação dos SI deve atender às necessidades dos processos de negócio, procurando cumprir a estratégia organizacional, referindo no entanto a necessidade de partir da estratégia para os processos de modo a, seguidamente, identificar os requisitos de informação. Este desenvolvimento tem como objectivo permitir que os SI “sejam um instrumento potenciador do desempenho e diferenciação das organizações”.

Refira-se todavia que, de acordo com Lopes *et al* [2005], o termo ‘sistema de informação’ pode referir-se ou não aos sistemas que utilizam as TI, pelo que sugerem, no caso dos que se suportam nas TI, a sua referenciação como Sistemas de Informação Baseados em Computadores (SIBC), notando que estes constituem um subsistema do SI organizacional. Neste mesmo âmbito consideram a utilização do termo ‘sistema informático’¹⁵ como sinónimo de SIBC (excluindo no entanto, deste contexto, os sistemas operativos).

Perspectiva idêntica é assumida por Serrano *et al* [2004], para quem o sistema informático constitui a parte do SI cujas actividades são realizadas através da utilização de computadores, realçando ainda o facto do conceito de SI ser estritamente organizacional, evitando-se a confusão com a introdução das TI para tratamento de dados, quando se pretendia apenas a sua automatização. Os autores referem ainda que o SI organizacional não é o sistema informático, embora assumam ser fundamental que essa diferença seja entendida de forma correcta, de modo a “que a informatização das organizações se realize de harmonia com os objectivos organizacionais”.

Refira-se aliás que a Lei nº109/91 (Criminalidade Informática) define, no seu artigo 2º, sistema informático como “um conjunto constituído por um ou mais computadores, equipamento periférico e suporte lógico que assegura o processamento de dados”.

Neste sentido, embora se entenda SI como um conceito amplo, deve atender-se, sempre que possível e tal seja entendido como necessário, à grande diversidade de sistemas existentes, considerando as necessidades particulares de cada um deles na sua aplicação ao cumprimento da especificidade das necessidades organizacionais.

¹⁵ Face ao âmbito assim definido, os sistemas informáticos serão referidos como tal, nas componentes de investigação deste trabalho, quando isso for considerado como essencial para uma especificação adequada no contexto em análise. Em contextos mais abrangentes será utilizada a designação SI.

Considerando o SI como um meio de transmissão de informação e as TIC como o suporte técnico que permite aos SI desempenhar as suas funções, Daniels [1997] realça a sua importância no desempenho das organizações, nomeadamente no “desenvolvimento de novos produtos e negócios”.

Um SI é então definido como um subsistema de um sistema organizacional, que engloba a concepção de como são constituídos os aspectos de comunicação e de informação, e como esses aspectos são operacionalizados através das acções e regras estabelecidas na organização [Falkenberg *et al* 1998].

Em termos genéricos os SI possuem as características inerentes a qualquer sistema e não estão condicionados pela inclusão das TIC que os suportam, todavia, face aos actuais desafios com que as organizações se confrontam, o facto de estes sistemas serem suportados pelas TIC pode ser uma vantagem competitiva a não descurar. Nesse sentido, assume-se a identificação proporcionada por Zwass [1998], na qual se podem identificar como principais componentes dos SI os seguintes: *hardware*; *software*; bases de dados; telecomunicações; Pessoas; procedimentos.

Deve assim ter-se em atenção que os SI não devem, face à emergência crescente de novas TIC, ser entendidos única e exclusivamente como *hardware* e *software*, mas sim num contexto mais abrangente que inclui Pessoas e a sua especificidade na utilização desses sistemas em prol dos objectivos organizacionais, cumprindo as regras especificadas para a sua plena utilização.

Martin *et al* [2002] consideram, nesta perspectiva, que os SI podem ser definidos de uma forma abrangente, como um conjunto de TI, de procedimentos e de Pessoas responsáveis pela aquisição, gestão, fluxos e distribuição de dados e informação, onde é fundamental que todos estes componentes funcionem, de forma correcta e adequada, em conjunto.

O alinhamento do SI e das TI com a organização e com a sua estratégia, implica conhecê-la, nomeadamente conhecer a sua missão, os seus recursos e processos, os seus clientes e concorrentes, os problemas com que se depara, os pontos fortes e as oportunidades de negócio, envolvendo todos os membros da organização na sua construção [Lopes e Amaral 2000]. Os autores referem ainda que a utilização

estratégica dos SI obriga a um entendimento das necessidades e potencialidades da organização, com “os SI vistos como uma das alavancas da mudança organizacional”.

Pelo que, de acordo com a perspectiva apresentada por Serrano [1997], a estratégia dos SI e das TIC deve ser encarada em duas vertentes: uma para os SI, definindo as necessidades de informação para as funções ou unidades de negócio e para o “cumprimento da missão da organização”, e outra para as TIC definindo como serão satisfeitas as necessidades organizacionais, face ao que foi estabelecido para a estratégia do SI.

Âmbito no qual, Anunciação e Zorrinho [2006] consideram que o alinhamento organizacional implica a adequação estrutural, contemplando a integração entre actividades de negócio, SI e TIC, cabendo “à informação, enquanto recurso, a condução deste alinhamento”. Os autores entendem ainda que os investimentos e a afectação das TI ao processamento, armazenamento e distribuição da informação, devem ser conduzidos de igual forma.

Segundo Reis [2001], o sucesso na gestão dos SI e das TIC relaciona-se directamente com a conjugação de factores como a maximização do retorno do investimento efectuado e da utilização da informação considerando a estratégia da organização, procurando obter vantagens competitivas, ou mesmo atenuar ou eliminar ameaças.

Neste contexto onde a estratégia do SI emerge como factor crítico de sucesso das organizações, Luz [2000] considera uma perspectiva mais abrangente onde os SI se revelam essenciais para a definição de uma estratégia global para a organização, salientando o facto de estes terem um papel crucial na internacionalização e globalização da organização centrada nesse mesmo SI. Por outro lado, entende que a utilização das TI no suporte aos SI permite um sistema integrado capaz de gerir as diferentes actividades organizacionais.

O estabelecimento dos requisitos, dos SI, permite definir o que é necessário fazer e o que deve ser transferido para uma solução baseada nas tecnologias, o que possibilita, por sua vez, definir como podem ser satisfeitas as necessidades previamente identificadas. Neste sentido, se ‘o que deve ser feito’ corresponde à estratégia dos SI e ‘o como podem ser satisfeitas as necessidades’ corresponde à estratégia das TI, torna-se

então essencial enquadrar as estratégias dos SI e das TI na estratégia de negócio da organização [Edwards *et al* 1995].

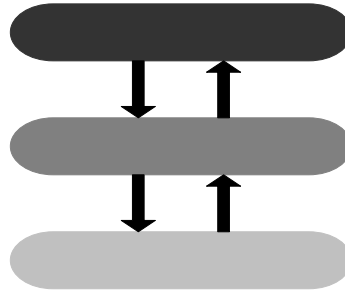


Figura 3.4 – Adequação estratégica
(adaptado de Edwards *et al* [1995])

Perspectiva similar é apresentada por Coelho [2005] que, para que os SI contribuam para o desempenho organizacional, considera como factores críticos de sucesso os seguintes aspectos:

- ⇒ Definir o papel estratégico dos SI;
- ⇒ Identificar as necessidades de informação para o desempenho dos processos;
- ⇒ Definir os requisitos de informação;
- ⇒ Seleccionar, receber e implementar os sistemas informáticos;
- ⇒ Formar na sua utilização no contexto dos processos.

Estratég

Perante esta envolvente, onde os SI e a sua relevância para as organizações, entende-se pertinente a perspectiva de Tavares e Pereira [2000] que apresentam os SI como estruturas complexas, cujo desenvolvimento se deu essencialmente para suporte dos processos de gestão e também para aumentar o conhecimento relevante no sentido de atingir os objectivos relevantes para a organização.

Estratég

Entendimento similar é apresentado por Cunha e Figueiredo [2000], que referem o facto de os SI da actualidade serem mais complexos do que aqueles que eram utilizados há alguns anos atrás, devido essencialmente às diferentes abordagens aos SI por parte das pressões dos negócios.

3.4. Tecnologias de Informação e Comunicação

Segundo Antunes [2001], estudar SI sem estudar as tecnologias que os suportam é o mesmo que estudar economia e gestão sem considerar os mercados, as unidades económicas e os recursos: visão, estratégia, capital, trabalho, energia e tecnologia”.

Esta visão consagra desde logo, considerando a importância das TIC nos diversos contextos de utilização da informação para suportar, com as consequentes vantagens competitivas, o desempenho das organizações, a necessidade de um correcto entendimento das potencialidades das TIC e da sua utilização, de acordo com as necessidades especificadas.

De forma idêntica ao que ocorre quando se pretende apresentar a definição de um conceito abrangente e logo objecto de diferentes visões, também as TIC são alvo de grande número de definições possíveis.

Numa definição formal, as TIC correspondem a uma “integração de métodos, processos de produção, *hardware* e *software*”, proporcionando a recolha, processamento, disseminação e utilização da informação [APDSI 2005], onde perante a actual evolução tecnológica, foi adoptado em substituição das TI.

Pode assim entender-se as TIC como veículo de disponibilização da informação [Reis 1993], como qualquer ferramenta baseada em computadores que as Pessoas podem usar para trabalhar, suportar e processar a informação [Haag *et al* 1998], ou então como factor crítico de sucesso nos intercâmbios de informação [Reis 2000].

Nesta mesma sequência, Serrano *et al* [2004] referem que as TI englobam, cada vez mais, não só *hardware* e *software* (componente informática tradicional), mas também os sistemas de telecomunicações, levando por isso a uma utilização mais frequente, assumindo a abrangência do termo TIC.

Informática corresponde à “ciência que se ocupa do processamento da informação que é a base do conhecimento em vários domínios (técnico, económico, social e outros) de forma a poder ser utilizada eficientemente pelo homem” [Cerveira 1967].

A compreensão do papel da informação e a utilização eficaz das TIC é fundamental no funcionamento interno das organizações e na concretização dos seus objectivos e negócios [Marcelino 1994]. Pode assim verificar-se que as TIC constituem a infra-

estrutura que suporta os fluxos de informação no interior da organização, com a sua gestão a ser entendida como essencial ao desempenho da organização, independentemente de o serem em termos de características físicas das TIC ou em termos das funções dessas mesmas TIC.

Considerando que os negócios e as organizações actuais são distintas das que existiam à alguns anos, Martin *et al* [2002] entendem as TI como encorajadoras das actividades das organizações de todas as dimensões, pequenas, médias ou grandes, quer sejam públicas ou privadas, referindo que as actuais são mais complexas e capazes de oferecer produtos e serviços adequados, encontrando-se por isso fortemente dependentes de um fluxo de informação correcto e atempado.

Segundo Laudon and Laudon [2000], os avanços nas telecomunicações e no *software* de computador aumentaram as vulnerabilidades dos sistemas, em particular quando, através das redes de telecomunicações, os SI em diferentes locais podem ser interligados, o que leva a que o potencial dos acessos não autorizados, abusos, ou fraude não se limite a um local mas possa ocorrer em qualquer ponto de acesso na rede.

Isto é tanto mais crítico quanto, de acordo com Zorrinho [2001], cada vez menos os sistemas de informação e comunicação são meros instrumentos ao serviço dos sistemas organizacionais, e cada vez mais o desenho destes é subordinado a objectivos de integração em plataformas informacionais mais vastas e à concretização de estratégias de posicionamento das empresas ou instituições nos mercados globais e nos sistemas competitivos alargados.

Se os SI são o meio de adquirir, tratar e partilhar informação entre as Pessoas, então as TIC devem assumir o papel de suporte a essas actividades constituindo-se como o dispositivo que permite aos SI desempenharem as suas tarefas. Verifica-se assim que a infinidade de novas tecnologias que as organizações têm ao seu dispor, torna claro o papel das TIC na infra-estrutura de suporte à estratégia de negócio, assumindo-se muitas vezes como a ‘chave’ para a sua sobrevivência [Earl and Feeny 2000].

Llufriu [2005] refere aliás que, para as TIC não provocarem “situações irreversíveis, técnicas ou humanas, ou do simples foro da eficácia ou a eficiência, torna-se necessária uma mudança na forma de fazer e de pensar, sendo essencial um período de mentalização/adaptação”. Neste contexto, o autor conclui que o plano de utilização das

TIC deve ser parte integrante do projecto organizacional, incluindo desde logo os profissionais a envolver na implementação.

Verificando-se deste modo que utilizar as TI para suportar as actividades humanas, seja na disponibilização de informação e outras facilidades, na inovação das actividades e estruturas organizacionais ou em intervenções inovadoras nas relações com os parceiros de negócio ou na actuação nos mercados, têm sido uma constante nos nossos dias [Santos e Ramos 2006].

De forma similar ao que sucede com os SI também a escolha das TIC depende de perspectivas pessoais e de necessidades específicas das organizações, particularmente quando as TIC possuem potencialidades que possibilitam a recuperação de atrasos estruturais, suportando-se na maior acessibilidade que permite aos dados, à informação e ao conhecimento [Soete 2000].

Constata-se então que na sociedade actual, o ciclo de vida das organizações e dos produtos sofreu reduções, tornando-se fácil verificar os impactos desse facto nas actividades de negócio das organizações e nas interacções pessoais, organizacionais e sociais. As mudanças registadas devem-se essencialmente à evolução verificada em termos de TIC e à crescente globalização dos mercados suportada por essas tecnologias, referindo Bosworth and Jacobson [2002] o facto de se verificar um crescimento muito elevado em termos de propagação e integração das TIC nas actividades humanas.

Considerando a importância da informação “no actual contexto económico e social” como um paradigma intimamente associado ao paradigma tecnológico, Anunciação e Zorrinho [2006] entendem que “a tecnologia permite agilizar” o tratamento da informação, suportando e moldando “muitos dos processos organizacionais e económicos”.

Lourenço e O'Neill [2002] referem a propósito que a gestão empresarial, considerando os âmbitos estratégico e operacional, deve entender as potencialidades das TIC para modificar e/ou renovar as competências da organização, referenciando ainda a necessidade de envolver toda a estrutura humana para um amplo aproveitamento das potencialidades mencionadas.

Neste contexto, a criação, memorização, tratamento e disponibilização de informação em tempo oportuno, pretende como objectivo a minimização do erro no processo de

tomada de decisão, desempenhando os SI/TI um papel central que se relaciona directamente com o desenvolvimento organizacional [Serrano *et al* 2004].

3.5. Conclusões

A globalização económica e social a que actualmente se assiste, fez emergir novos mercados forçando as organizações, e as Pessoas que as constituem, a responder a novos e complexos desafios, implicando a necessidade de aquisição de novas e melhores competências capazes de potenciar o desempenho das organizações.

No contexto de globalização referenciado, a informação, tal como as Pessoas, assume um papel importante como um dos principais activos organizacionais, concluindo-se que a adequada e atempada utilização da informação é fundamental para o desempenho das organizações.

Perante isto, considerando a necessidade de garantir a segurança do activo ‘informação’, conclui-se da pertinência de assegurar que os aspectos associados à segurança são tidos em consideração na escolha e utilização dos SI e das TIC, assim como em garantir que as Pessoas são adequadamente envolvidas nestes processos.

Neste sentido, os SI pela sua capacidade de suportar as necessidades organizacionais, facilitando a utilização da informação por parte das Pessoas, tornam-se um instrumento fundamental para a organização, requerendo por isso uma concepção, desenvolvimento e implementação adequados à missão, estratégia e objectivos definidos para a organização.

Assim, considerando as actividades de utilização dos SI e das TIC em que este se suporta, a sua capacidade de possibilitar os fluxos inter e intra organizacionais da informação, constitui um factor de sucesso desde que a sua aplicação se adeque às actividades de negócio.

Referências bibliográficas

Alter, S., *Information Systems: A Management Perspective*, 3rd Edition, Addison-Wesley Publishing Company, 1998.

- Antunes, I., “A Problemática da Avaliação e da Maturidade nos Processos de Desenvolvimento de Aplicações Informáticas”, *Informação & Informática*, 26, 2001, p.45-52.
- Anunciação, P. e Zorrinho, C., *Urbanismo Organizacional – Como gerir o choque tecnológico nas empresas*, Edições Sílabo, 2006.
- APDSI, *Glossário da Sociedade da Informação*, José Palma Fernandes (Coordenador), Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI), Outubro de 2005.
- Bosworth, S. and Jacobson, R., “Brief History and Mission of Information System Security”, in S. Bosworth and M.E. Kabay, (Editors), *Computer Security Handbook*, 4th Edition, John Wiley & Sons, 2002.
- Caldeira, M. e Romão, M., “Porque falham os sistemas e tecnologias de informação nas PMEs Portuguesas”, Actas (formato digital) da 3^a Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.
- Carvalho, J.Á. e Amaral, L., “Matriz de Actividades: Um Enquadramento Conceptual para as Actividades de Planeamento e Desenvolvimento de Sistemas de Informação”, *Revista da Associação Portuguesa de Sistemas de Informação*, 1 (1993), p.37-48.
- Cerveira, A.G., “Informática e Mecanografia”, *Associação Internacional de Estudos sobre Mecanografia*, IV Encontro Internacional de Mecanografia e Informática, Outubro de 1967, p.45-50.
- Choo, C.W., *Gestão da Informação para a Organização Inteligente*, Editorial Caminho, 2003.
- Ciborra, C. and Andreu, R., “Organizational Learning and Core Capabilities Development: The Role of IT”, in Robert D. Galliers and Walter R. J. Baets (Organization), *Information Technology and Organizational Transformation: Innovation for the 21st Century Organization*, London, John Wiley & Sons, 1998, p.87-106.
- Coelho, J., “Arquitectura da Empresa Centrada nos Processos: O Factor determinante para o Alinhamento Estratégico dos SI”, in Luís Amaral, Rodrigo Magalhães, Carlos Campos Morais, António Serrano e Carlos Zorrinho (Editores), *Sistemas de Informação Organizacionais*, Edições Sílabo, 2005, p.141-197.
- Correia, E., *Novas Tecnologias – Presente e Futuro*, volume 2, Edições Sílabo, 2006.
- Cunha, P.R., Figueiredo, A.D., “Information Systems Planning for Emerging Challenges”, in Luís Valadares Tavares e Manuel João Pereira (Organizadores), *Nova Economia e*

- Tecnologias de Informação: Desafios para Portugal*, Universidade Católica Editora, 2000, p.22-29.
- Daniels, C., *Estratégias Empresariais e Tecnologias de Informação*, Biblioteca de Economia e Gestão – Editorial Caminho, 1997.
- Dinis, J.A., *Guerra de Informação – Perspectivas de Segurança e Competitividade*, Edições Sílabo, 2005.
- Drucker, P., *Gerindo para o Futuro*, Difusão Cultural, 1993.
- Drucker, P., *Peter Drucker sobre a Profissão de Gestão*, Publicações Dom Quixote, 1999.
- Drucker, P., *Desafios da Gestão para o Século XXI*, Editora Civilização Livraria, 2000.
- Earl, M., “Todas as empresas são empresas de informação”, *O Domínio da Informação*, Diário Económico, 2000, p.12-15.
- Earl, M. and Feeny, D., “How To Be a CEO for the Information Age”, *Sloan Management Review*, Winter 2000, p.11-23.
- Edwards, C., Ward, J. and Bytheway, A., *The Essence of Information Systems*, 2nd Edition, Prentice Hall, 1995.
- Falkenberg, E., Hesse, W., Lindgreen, P., Nilssen B., Oei, J., Rolland, C., Stamper, R., Van Assche, F., Verrijn-Stuart, A. and Voss, K., *FRISCO: A Framework of Information Systems Concepts*, IFIP WG 8.1 Task Group FRISCO, 1998.
- Ferreira, J.M.C., “Teoria Geral dos Sistemas e Abordagem Sociotécnica”, in J.M. Carvalho Ferreira, José Neves e António Caetano (Editores), *Manual de Psicossociologia das Organizações*, McGrawHill, 2001.
- Garcia, C., “A Notável Intangibilidade das Organizações: O Capital Intelectual e os Sistemas de Informação”, in Luís Amaral, Rodrigo Magalhães, Carlos Campos Morais, António Serrano e Carlos Zorrinho (Editores), *Sistemas de Informação Organizacionais*, Edições Sílabo, 2005, p.199-222.
- Giddens, A., *O mundo na era da globalização*, Editorial Presença, 2000.
- Haag, S., Cummings, M. and Dawkins, J., *Management Information Systems for the Information Age*, Irwin/McGraw-Hill, 1998.
- Laudon, K. and Laudon, J., *Management Information Systems: Organization and Technology in the Networked Enterprise*, 6th Edition, Prentice-Hall, 2000.

- Llufriu, M., “Impacte das Tecnologias de Informação e Comunicação na Sociedade do Conhecimento”, in Luís Amaral, Rodrigo Magalhães, Carlos Campos Morais, António Serrano e Carlos Zorrinho (Editores), *Sistemas de Informação Organizacionais*, Edições Sílabo, 2005, p.95-112.
- Lopes, F.C. e Amaral, L.A., “Actividades de Intervenção de Sistemas de Informação”, Actas (formato digital) da 1ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade do Minho, Guimarães, 25-27 de Outubro de 2000.
- Lopes, F. C., Morais, M. P. e Carvalho, A. J., *Desenvolvimento de Sistemas de Informação*, FCA, 2005.
- Lourenço, R.T. e O'Neill, H., “As Tecnologias de Informação e Comunicação na Gestão Empresarial e o papel dos Recursos Humanos na sua Potenciação”, Actas (formato digital) da 3ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.
- Luz, N., “Impacto da Internet sobre a Estratégia de Internacionalização das Empresas”, in Luís Valadares Tavares e Manuel João Pereira (Organizadores), *Nova Economia e Tecnologias de Informação: Desafios para Portugal*, Universidade Católica Editora, 2000, p.378-397.
- Marcelino, H., “Potencialidades e limites das Tecnologias de Informação” in *Dossier: Gestão da Informação, Pequena e Média Empresa*, 12, (1994), IAPMEI, p.53-61.
- Martin, E.W., Brown, C.V., DeHayes, D.W., Hoffer, J.A. and Perkins, W.C., *Managing Information Technology*, 4th Edition, Prentice Hall, 2002.
- Oliveira, J. e Amaral, L., “O Papel da Qualidade da Informação nos Sistemas de Informação”, in Luís Valadares Tavares e Manuel João Pereira (Organizadores), *Nova Economia e Tecnologias de Informação: Desafios para Portugal*, Universidade Católica Editora, 2000, p.168-184.
- Peltier, T.R., *Information Security Policies, Procedures, and Standards*, CRC Press, 2002.
- Pipkin, D.L., “Linking Business Objectives and Security Directions”, in Michael E. Whitman and Herbert J. Mattord (Editors), *Readings and Cases in The Management Information Security*, Thomson Course Technology, 2006, p.8-16.
- Reis, C., *Planeamento Estratégico de Sistemas de Informação*, Editorial Presença, 1993.
- Reis, L., *Planeamento de Sistemas de Informação e da Contingência e da Recuperação*, Tese de Doutoramento, Universidade do Minho, 2000.

- Reis, L., “Manual Electrónico de Apoio ao Desenvolvimento de Planos de Contingência e Recuperação em Sistemas de Informação para PME”, in Armando Pires (Organizador), *Projectos de Investigação IPS*, Instituto Politécnico de Setúbal, 2001, p.89-101.
- Reis, L. e Amaral, L., “Gestão de Riscos num contexto de Planeamento da Contingência e Recuperação”, Actas (formato digital) da 3ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.
- Rivas, F., *Estruturas Organizativas e Informação na Empresa*, Editorial Domingos Barreira, 1989.
- Rodrigues, L.S., *Arquitecturas dos Sistemas de Informação*, FCA, 2002.
- Santos, M.Y. e Ramos, I., *Business Intelligence – Tecnologias da Informação na Gestão de Conhecimento*, FCA, 2006.
- Serrano, A., *Sistemas de Informação de Potencial Estratégico – Modelo Referencial para Exploração em PME*, Tese de Doutoramento, Universidade de Évora, 1997.
- Serrano, A., Caldeira, M. e Guerreiro, A., *Gestão de Sistemas e Tecnologias de Informação*, FCA, 2004.
- Serrano, A. e Fialho, C., *Gestão do Conhecimento – O novo paradigma das organizações*, FCA, 2003.
- Soete, L., “A Economia Baseada no Conhecimento num Mundo Globalizado: Desafios e Potencial”, in Maria João Rodrigues (Coordenadora), *Para Uma Europa da Inovação e do Conhecimento*, Celta Editora, 2000, p.3-31.
- Tavares, L.V., Pereira, M.J., “The Value of an Information Systems”, in Luís Valadares Tavares e Manuel João Pereira (Organizadores), *Nova Economia e Tecnologias de Informação: Desafios para Portugal*, Universidade Católica Editora, 2000, p.4-21.
- Ward, J., *Principles of Information Systems Management*, Routeledge, 1995.
- Zorrinho, C., *Gestão da Informação*, Editorial Presença, 1991.
- Zorrinho, C., “O Mundo Virtual”, *Cadernos de Gestão de Sistemas e Tecnologias da Informação Henrique Marcelino*, Instituto de Informática, 1999, p.27-35.
- Zorrinho, C., *Ordem, Caos e Utopia – Contributos para a História do Século XXI*, Editorial Presença, 2001.
- Zwass, V., *Foundations of Information Systems*, Irwin/McGraw-Hill, 1998.

4

Segurança da Informação

Constatando-se a crescente dependência das organizações perante as TIC, essencialmente para suportar a utilização de SI que permitam aumentos no seu desempenho quando procuram responder ao actual ambiente competitivo e contingencial, onde os negócios maioritariamente se concretizam, torna-se óbvia a necessidade de novas atitudes perante os desafios que se colocam às organizações, quer seja por parte dos seus clientes, por parte dos seus concorrentes ou ainda por força de imposições legais.

Segurança, privacidade e confiança são conceitos interrelacionados com que se confronta no dia a dia quem manipula informação pessoal, social ou organizacional, particularmente pelas ameaças a que a informação e os SI que a suportam se encontram sujeitos. Emerge assim a necessidade de obter um entendimento concreto dos aspectos adequados a garantir que a informação, independentemente de como e onde vai ser utilizada, a quem pertence ou quem a pode utilizar, apenas é aplicada na prossecução dos objectivos que presidiram à sua criação.

As Pessoas utilizam a informação a que têm acesso porque possuem a percepção de que essa utilização lhes permitirá um melhor desempenho. O facto de a informação disponível ter aumentado exponencialmente coloca-os perante alguns dilemas: Que informação escolher? Como e porque escolher? Como, onde e porque utilizar?

Assumir de forma clara e inequívoca que a informação constitui um dos mais importantes activos organizacionais, torna-se um importante contributo para lidar com as dificuldades acerca de como ‘manusear’ a informação para adquirir vantagens competitivas, evidenciando a necessidade de se garantir a segurança do que aparentemente está ao alcance de qualquer pessoa.

4.1. Evolução Histórica

Em termos holísticos, as preocupações com a segurança apenas surgem quando algo ou alguém fica sujeito a uma qualquer ameaça que possa ser concretizada através da exploração de uma qualquer vulnerabilidade.

Identificar como tiveram início as preocupações com a segurança parece ser uma tarefa difícil de concretizar, no entanto, garantir a segurança (privacidade) da informação, particularmente quando dessa informação dependia a sobrevivência do homem, foi uma preocupação sempre presente ao longo da evolução humana. Todavia, o gradual aumento da interacção social comportou maiores necessidades e uma ampla partilha de informação, implicando assim que as preocupações com a sua privacidade tivessem tendência para aumentar.

O que leva, de acordo com Cerveira [1967], a que o trabalho do homem possa ficar comprometido se não receber de forma atempada e rotineira as informações de que necessita para executar o seu trabalho, passando a depender de outros para a obtenção dessa informação, tal como aconteceu “com o homem primitivo” segundo refere.

Evoluindo de um comércio baseado em trocas segundo as necessidades, para um ambiente sustentado em organizações vocacionadas para a geração de lucro, a obtenção de informação que permitisse incrementar esse mesmo lucro tornou-se uma necessidade das Pessoas e das organizações, reforçando desse modo a obrigatoriedade de assegurar que a informação de negócio se mantinha segura.

A situação referenciada ganha relevância especial com a emergência de um conjunto de novas TIC, que potenciaram claros aumentos na quantidade de informação disponível e nas ferramentas adequadas à sua partilha e utilização, de acordo com objectivos definidos pelas organizações.

O que parece não suscitar qualquer dúvida é o facto de as preocupações de segurança, quer seja em termos globais (afectadas por ameaças de ataques ‘terroristas’, por ‘guerras’ locais com tendência crescente para atingirem um nível quase global, ou mesmo a ‘fome’, causada por secas, guerras ou alterações climáticas), quer em termos pessoais (custos e disponibilidade de cuidados de saúde, garantia e estabilidade no emprego, transacções electrónicas, necessidades de novas e melhores competências) ou

mesmo organizacionais (ameaças de espionagem e mesmo desaparecimento de informação essencial para o negócio, competências das Pessoas e confiança acerca dos seus comportamentos, custos associados aos novos desafios dos mercados ou à implementação de novos negócios suportados por SI e TIC), ter conhecido um grande incremento dos últimos anos.

O sucedido com os ataques perpetrados contra o *World Trade Center* em Nova Iorque, ou contra os transportes ferroviários em Madrid, são exemplos claros de actos globais capazes de afectar o normal decorrer das actividades humanas, não só pela alteração das condições de circulação e movimentação das Pessoas e bens, mas também pelos graves impactos na segurança física das Pessoas, nos seus bens materiais e na informação detida pelas organizações afectadas.

Neste mesmo contexto, deve notar-se o surgimento de uma nova categoria de ameaças consubstanciadas nas alterações climáticas actualmente registadas, particularmente pela imprevisibilidade da sua ocorrência e da inexistência de uma percepção clara dos seus reais impactos.

As preocupações com a segurança em SI, ou mais concretamente nos sistemas informáticos, centravam-se nas componentes tecnológicas desses sistemas, nomeadamente através do controlo dos acessos físicos ao sistema, na utilização de mecanismos de criptografia e até no limite do número de utilizadores dos sistemas. Todavia, a evolução tecnológica forçou mudanças substanciais nessa focalização, levando à inclusão das Pessoas e dos diversos procedimentos de utilização nas preocupações de segurança.

Em termos latos os problemas de segurança com que as organizações se deparam actualmente localizam-se essencialmente:

- Na rede de comunicações;
- Nos sistemas informáticos;
- Nas instalações físicas;
- No pessoal técnico;
- Nos diversos tipos de utilizadores.

Esta identificação de tópicos relevantes em termos de segurança não exclui a obrigatoriedade de entender os impactos sobre as suas actividades, que possam decorrer de qualquer das situações mencionadas.

O desafio para a segurança reside actualmente na diversidade de ameaças e vulnerabilidades a que tem de responder, considerando um contexto onde essa diversidade tem vindo a aumentar.

Segundo Mamede [2006], o termo ‘segurança’ está associado aos riscos, à sua prevenção e também à minimização desses riscos, referindo que segurança implica a capacidade para serem tomadas medidas preventivas capazes de evitar ocorrências inesperadas e/ou indesejadas. Segundo o autor, importa proceder a uma identificação dos elementos mais fracos do sistema a utilizar, de modo a serem encontradas soluções adequadas que considerem os riscos e respectivos custos relacionados com a protecção dos sistemas e dos dados.

Todavia, pode dizer-se que, em termos estritos, os problemas de segurança estão intrinsecamente relacionados com a forma como a segurança é encarada no interior das organizações e consequentemente nas sociedades onde estas se inserem. Esta situação pode conduzir à emergência de algumas questões, de entre as quais se refere a necessidade de identificar quem decide a adopção de políticas de segurança.

Esta situação, crucial para todas as actividades relacionadas com a segurança organizacional, requer um comprometimento inequívoco da gestão de topo, não apenas na designação do respectivo responsável, mas também na atribuição dos recursos essenciais ao desenvolvimento das actividades necessárias.

Neste sentido, Mamede [2006] refere que “a segurança de uma organização deve ser analisada num contexto alargado”, onde devem ser consideradas todas as perspectivas de modo a reflectir a multidisciplinaridade da segurança.

Em termos de segurança não existe uma resposta única para todas as questões, referindo-se que a preocupação central é saber quando a função segurança terá a influência e autoridade que necessita para desempenhar o seu papel na organização, considerando que esse papel compreende informar, monitorizar, conduzir e forçar as melhores práticas [Henry 2003].

4.2. Globalização e Segurança

A Sociedade da Informação e o contexto de globalização com que as organizações actualmente se confrontam colocam-lhes novos e exigentes desafios, levando a que aumente a sua dependência das TIC, exigindo uma atenção especial para com a sua escolha, aquisição e utilização, enquadrando-as na estratégia da organização e nos objectivos de negócio definidos, no sentido de suportar os fluxos de informação inter e intra organizacionais.

Sociedade da Informação pode assim ser definida como “uma forma de desenvolvimento social e económico” capaz de conduzir à criação de conhecimento e à satisfação das necessidades dos cidadãos e das organizações, suportando-se na aquisição, avaliação, processamento, armazenamento, distribuição e disseminação da informação, desempenhando estas actividades um “papel fulcral na evolução da humanidade” [Fernandes *et al* 2007].

Pode todavia considerar-se uma definição mais formal, onde a Sociedade da Informação¹⁶ é entendida como uma “etapa no desenvolvimento da civilização moderna” que se caracteriza pelo crescente papel social da informação, assim como pelo aumento da partilha de produtos e serviços de informação e também pelo surgimento de “um espaço global de informação” [APDSI 2005]. Neste âmbito referem-se “a aprendizagem, o conhecimento, o envolvimento, a ligação em rede, a cooperação e a igualdade dos cidadãos”, como os principais objectivos no seu desenvolvimento.

Verifica-se então que, perante a necessidade de competir na actual Sociedade da Informação e nos mercados que esta comporta, onde o ciclo de vida dos produtos é cada vez menor, a informação é necessária a ritmos elevados, colocando-se a obrigatoriedade de a obter de forma rápida, fiável e no formato adequado, e simultaneamente de garantir a sua preservação.

Com os referidos desafios a serem condicionados pela utilização da informação e pelas competências necessárias para responder adequadamente aos requisitos organizacionais, emerge a pertinência de assegurar a segurança da informação pessoal e organizacional, implicando assim a definição e implementação das políticas de segurança adequadas à

¹⁶ Neste glossário [APDSI 2005], é referido o facto de a Sociedade do Conhecimento não ser mais do que uma evolução da Sociedade da Informação.

estratégia da organização, políticas essas que devem considerar quer os aspectos internos quer os aspectos externos, estes não apenas no ambiente envolvente da organização mas também nas relações com os clientes, parceiros de negócio, considerando com especial atenção as implicações legais aplicáveis em função da localização geográfica e do respectivo sector de actividade.

O dia-a-dia das organizações impõe-lhes então, conjuntamente com os novos desafios, adaptações constantes das suas estruturas organizativas e dos seus modelos de negócio, afectando simultaneamente o seu ambiente competitivo e todos os seus parceiros de negócio, quer sejam internos ou externos. Esta situação ganha relevância perante uma sociedade baseada na utilização ampla da informação, confrontando-se com o actual ambiente de negócio possibilitado pela globalização.

Perante este contexto turbulento e contingencial, as Pessoas deverão ser encaradas como um importante activo organizacional, sendo essencial proporcionar-lhes condições de desenvolvimento e motivação para que desenvolvam o seu potencial ao serviço das organizações onde se inserem, procurando garantir simultaneamente que a utilização dos SI e das TIC, contribuem para melhorar perceptivelmente o seu desempenho.

Torna-se então cada vez mais necessário dedicar especial atenção à sua recolha e utilização, devido essencialmente à diversidade e quantidade de informação actualmente disponível, pois se por um lado a velocidade a que se processa a troca de informação, implica que os problemas inerentes a sua gestão façam parte das preocupações dos decisores organizacionais, pelo outro obriga a que se tenha simultaneamente em atenção a sua privacidade e integridade.

O crescimento de relevância da informação conduziu a um tipo de problema que até há pouco tempo não tinha concentrado a generalidade das atenções – a segurança (protecção) da informação – principalmente porque a partilha de informação se registava quase exclusivamente por interacções pessoais, ou seja, através das actividades habituais dos SI informais.

Esta percepção da importância do papel das Pessoas e da informação nas actividades organizacionais é reforçada por Herold [2003] quando refere que o sucesso da protecção e segurança da informação requer a participação, concordância e suporte das Pessoas na

organização, independentemente da sua posição, localização e relações com a organização, em especial quando a implementação de SGSI afecta o seu desempenho.

Verifica-se então que a evolução dos negócios e das organizações ganhou novos ritmos e âmbitos face à crescente globalização a que se tem assistido, afectando indistintamente as Pessoas e as organizações. Neste contexto, o entendimento que os responsáveis organizacionais possuem acerca dos desafios a que devem responder na actualidade e a forma como entendem a relevância das TIC como ferramentas essenciais ao desempenho das suas organizações, pode fazer a diferença relativamente ao seu grau de sucesso.

A situação torna-se tanto mais grave quanto maior é o desconhecimento existente acerca dos fluxos de informação e do controlo dos acessos a essa informação, exigindo novas atitudes e a sua concertação com os recursos organizacionais e com a estratégia da organização. Emerge por isso a necessidade de entender os impactos motivados pela utilização dos SI que suportam esses fluxos e pela criticidade da própria informação.

4.3. Segurança da Informação e dos Sistemas de Informação

Embora no contexto deste trabalho não seja efectuada qualquer diferenciação entre ‘segurança da informação’¹⁷, protecção dos SI contra o acesso ou modificação não autorizados da informação [APDSI 2005], e ‘segurança informática’¹⁸, conjunto de medidas de segurança (físicas, lógicas, administrativas) e de urgência para proteger os bens informáticos de uma organização (*hardware*, *software*, dados) [APDSI 2005], utilizar-se-à preferencialmente o termo ‘segurança da informação’.

Frequentemente assumida como uma necessidade para as actividades organizacionais, deve atender-se ao facto do conceito de ‘informação’ poder ser compreendido de acordo com diferentes perspectivas, dependentes do contexto em que é aplicado. Neste sentido o termo ‘informação’ é utilizado de acordo com o que é apresentado pela BS ISO/IEC 17799 [ISO 2005a], que define informação como um activo que tem valor para uma organização e que requer protecção adequada, independentemente da forma ou meio de armazenamento, processamento e/ou transmissão.

¹⁷ Do termo inglês ‘information security’.

¹⁸ Do termo inglês ‘computer security’. Neste contexto [APDSI 2005], “segurança informática = confidencialidade + integridade + disponibilidade”.

A informação tornou-se um factor crítico de sucesso exigindo por isso uma protecção adequada, principalmente no contexto actual dos mercados onde as TIC assumem papéis fundamentais no desempenho das organizações, na sua assumpção de contingencialidade e turbulência com que os referidos mercados se confrontam.

Perante a necessidade de se proceder a um entendimento da importância da informação, Parker [2002] identifica seis características da informação a ser preservada:

- (1) disponibilidade (usabilidade da informação para um propósito);
- (2) utilidade (interesse da informação para um propósito);
- (3) integridade (perfeição, totalidade e legibilidade da informação e a qualidade de não se modificar de um estado inicial);
- (4) autenticidade (validade, conformidade e genuinidade da informação);
- (5) confidencialidade (observação e revelação limitada do conhecimento);
- (6) posse (deter, controlar e ter a capacidade de usar informação).

Reforça-se deste modo a indispensabilidade de garantir a segurança da informação, assumindo-se a sua caracterização de acordo com a BS ISO/IEC 17799 [ISO 2005a], como a preservação da confidencialidade (assegurar que a informação apenas é acedida por quem está autorizado a fazê-lo), da integridade (garantir a exactidão e a credibilidade da informação) e da disponibilidade (assegurar que as Pessoas autorizadas têm acesso à informação e aos activos associados sempre que necessário) da informação.

Todavia, ainda de acordo com a BS ISO/IEC 17799 [ISO 2005a], deve ter-se em atenção que o propósito da segurança da informação é proteger a informação de uma grande variedade de ameaças, assegurando a continuidade do negócio através da minimização dos danos causados no negócio por incidentes de segurança e da maximização do retorno dos investimentos e das oportunidades de negócio.

Segundo Peltier [2001:4], cada organização possui o seu próprio conjunto de requisitos para a protecção dos activos de informação, que são habitualmente documentados através de uma metodologia de análise e de uma política de classificação da informação. O autor refere ainda que a salvaguarda da informação difere de organização para organização, considerando a sua integridade (a informação mantém-se sem modificações inapropriadas ou corrupção), a sua confidencialidade (a informação é

protegida de disponibilizações não autorizadas ou acidentais), e a sua disponibilidade (os utilizadores autorizados podem aceder aos sistemas e aplicações quando necessário para o desempenho dos seus trabalhos).

Referenciar segurança de computadores significa, na perspectiva de Pfleeger and Pfleeger [2003:10], ponderar três aspectos muito importantes: confidencialidade, integridade e disponibilidade. Confidencialidade¹⁹ tem a ver com assegurar que os activos apenas são acedidos por quem está autorizado, Integridade significa que os activos apenas podem ser modificados por Pessoas autorizadas para tal e na forma autorizada, e Disponibilidade significa que os activos apenas são acedidos por Pessoas autorizadas nos tempos apropriados. Os autores entendem assim que a segurança deve observar estes três objectivos, considerando que o desafio é encontrar o balanceamento correcto entre estes objectivos em constante conflito, perspectiva esta que é apresentada na figura seguinte.

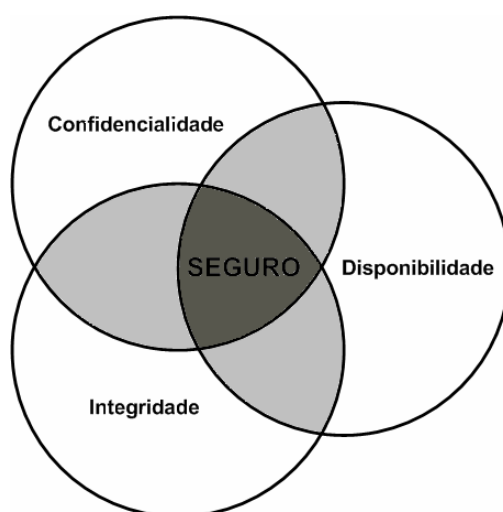


Figura 4.1 – Desafio da segurança da informação
(Adaptado de Pfleeger and Pfleeger [2003])

Numa perspectiva complementar, considerando uma visão holística, segurança da informação é assumida como uma tríade de Pessoas, processos e tecnologias [Fenton and Wolfe 2003], entendendo-a como o grupo de medidas que basicamente comprometem as políticas de segurança, objectivando a protecção da informação relativa aos negócios e aos clientes, tentando simultaneamente controlar o risco de acessos não autorizados.

¹⁹ Entendida muitas vezes como ‘segredo’ ou ‘privacidade’ [Pfleeger and Pfleeger 2003].

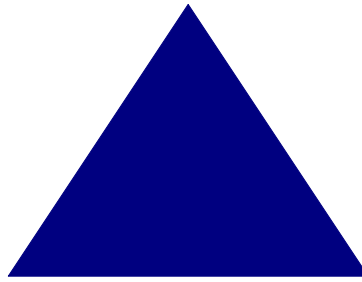


Figura 4.2 – Envoltantes da segurança da informação
(Adaptado de Fenton and Wolfe [2003])

Considerando então esta envolvente, onde as tecnologias e as Pessoas são fundamentais para a segurança da informação, afectando a sua utilização e rentabilização ao serviço da organização, emerge a necessidade de entender as suas interacções e a forma como é afectada a segurança da informação.

Segurança da informação corresponde a algo mais do que implementar controlos tecnológicos variados e complexos, pois de acordo com Berti and Rogers [2002] compreende também lidar com os comportamentos das pessoas que utilizam as tecnologias implementadas.

TECNOLOGIAS

Neste âmbito, Hansche [2002] refere que as Pessoas utilizam os SI sem estarem alertadas para os problemas da segurança, essencialmente quando os utilizam como ferramenta para desempenhar as actividades pelas quais são responsáveis da melhor forma possível para os seus intentos, onde a segurança é vista apenas como um entrave e não uma necessidade.

Muitos dos problemas de segurança da Informação e dos SI com que as organizações se deparam actualmente derivam em grande parte da utilização da Internet, problemas estes motivados geralmente pelo facto de esta se basear num conjunto de protocolos com mais de 30 anos, “abertos e de livre acesso” segundo Castells [2004], que na sua essência foram concebidos para assegurar e facilitar a conectividade e não para proporcionarem segurança das comunicações.

Neste mesmo sentido, Veiga [2002] considera que a Internet comporta um conjunto de desafios, proporcionando acessos alternativos e alargados aos SI, mencionando no entanto que essas vantagens apresentam como aspecto negativo o aumento das oportunidades de ataques aos SI.

Deve no entanto referir-se que a relevância assumida pela Internet permite uma ampla difusão da informação e o acesso a esta por um número crescente de utilizadores, mesmo considerando as falhas de segurança que aquela apresenta com o alargamento da sua base de utilização suportada no desenvolvimento actual das TIC, emergindo por isso a necessidade de se ponderar a sua utilização de forma cuidada e com os mecanismos de segurança adequados.

Contrariamente ao que sucedia com os requisitos de segurança tradicionais (essencialmente físicos, e como tal tangíveis), cujo centro das preocupações eram as Pessoas e os acessos físicos aos equipamentos, os actuais requisitos de segurança dependem também de parâmetros intangíveis, cuja integridade, confidencialidade e disponibilidade se revelam difíceis de controlar e de auditar, particularmente com a evolução tecnológica que se tem vindo a registar e que tem possibilitado um acesso fácil e rápido às TIC e consequentemente aos SI organizacionais.

Pode então considerar-se que a crescente utilização das novas TIC tem contribuído para o agravamento dos problemas de segurança, constatação simples se atendermos ao facto de ferramentas e técnicas estarem disponíveis e acessíveis aos potenciais interessados, facilitando muitas vezes acessos não autorizados, e como tal ilegítimos, aos SI organizacionais.

Não existe assim, em termos de segurança, uma resposta única para a generalidade das questões, residindo frequentemente a preocupação central na especificação da influência e autoridade que a função segurança exige para desempenhar o seu papel na organização, considerando que esse papel compreende informar, monitorizar, conduzir e forçar as melhores práticas [Henry 2003].

Em questões de segurança o que parece poder fazer a diferença são as Pessoas e a sua capacidade de, com recurso às TIC e ao conhecimento que detêm acerca da sua utilização, suportarem as necessidades da organização. Esta situação é reforçada pelo entendimento expresso por Carneiro [2002] acerca da dependência do conhecimento e cooperação dos utilizadores para uma correcta implementação da política de segurança, referenciando ainda a necessidade de um conhecimento geral sobre:

- adopção de comportamentos adequados perante ameaças ao SI;
- a quem recorrer no caso de surgirem perguntas ou suspeitas;

- o que fazer para minimizar os riscos de segurança;
- saber que as políticas e medidas de segurança são estabelecidas para benefício dos SI e do desempenho dos utilizadores.

Se os SI existem para suportar a partilha de informação através da organização e entre esta e os seus parceiros de negócio, então existe a obrigatoriedade de, simultaneamente com a segurança da informação, assegurar a segurança do SI e das TIC que o suportam.

Planear e desenvolver SI seguros corresponde a planear e desenvolver os respectivos sistemas de segurança. Corresponde também a planear e desenvolver, com segurança, os suportes tecnológicos que são intrínsecos aos SI, tal como as redes de comunicação, o *software* e o *hardware* que suportam o sistema.

Emerge assim a necessidade de identificar o que deve ser protegido, nomeadamente os recursos de TIC (*hardware* e *software*), de informação (documentos, processos de negócio, registos e procedimentos), considerando as disponibilidades em termos de recursos humanos e o seu envolvimento na operação e utilização do SI, assim como na manipulação de dados e de outros documentos [Barman 2002].

No entanto, quando está em causa a segurança da informação suportada pelo SI das organizações, aspectos como controlo de acessos, confidencialidade, integridade e disponibilidade da informação são cruciais, reforçando a necessidade de proceder a uma gestão adequada da segurança da informação, que atenda simultaneamente às necessidades organizacionais e dos utilizadores dos SI.

A segurança constitui então um dos aspectos de maior importância, se não mesmo o mais importante, no que respeita aos SI e às TIC. Importa às Pessoas, uma vez que são fornecidos dados pessoais e financeiros relevantes, e importa também à organização que disponibiliza o acesso ao sistema porque lhe compete garantir a credibilidade dos fluxos de informação assim como garantir a confidencialidade das informações relativas aos seus clientes e parceiros de negócio.

Todavia, o sucesso das medidas de segurança depende essencialmente do comprometimento dos decisores organizacionais, confrontando-se estes com uma Sociedade da Informação onde as organizações dependem dos seus SI e onde as TIC estão a originar uma revolução baseada na Informação, levando a que a segurança seja

encarada em termos físicos (colaboradores, instalações) e em termos lógicos (acessos, controlo de operações, protecção dos dados) [Reis 2000].

O entendimento da importância das TIC no desenvolvimento e desempenho organizacional depende, na sua essência, da percepção dos gestores organizacionais acerca da pertinência dessas TIC e da sua articulação com a cultura organizacional.

Neste âmbito, a decisão sobre a escolha de entre a panóplia de TIC ao dispor das organizações poderá fazer a diferença em termos de desempenho, porquanto a criação de valor dependerá mais da utilização das TIC do que das próprias TIC, tornando-se assim fundamental que as políticas de segurança a adoptar tenham em conta essa realidade.

Por outro lado, a diversidade de situações passíveis de constituir uma ameaça para a informação ou para o SI organizacional, ou uma vulnerabilidade do SI a ser prevenida, requer que se proceda a uma identificação clara das potenciais ameaças e das vulnerabilidades que possam ser alvo dessas ameaças.

Constatar-se-á então que segurança e privacidade correspondem a uma área complexa com a qual os gestores dos SI têm de lidar. Os conceitos de pertença e acesso à informação são cruciais quando se pretende segurança, levando a que sejam tomadas medidas preventivas sempre que exista o risco de ocorrência de qualquer acção criminosa capaz de afectar a normal utilização dos activos organizacionais [Edwards *et al* 1995].

A implementação de políticas de segurança pode por isso transformar-se numa forte condicionante da utilização dos SI, em especial quando as actividades correntes das Pessoas são afectadas de forma profunda, envolvendo novas fases de aprendizagem e implicando atrasos e condicionantes nos acessos aos SI.

4.4. Políticas de Segurança

Segundo Zúquete [2006], as políticas de segurança definem o foco da segurança e o que deve ser garantido com a sua utilização, enquanto que os mecanismos de segurança correspondem às tecnologias utilizadas para colocar em prática essas mesmas políticas.

As políticas de segurança da informação, de acordo com Barman [2002], são planos de alto nível que descrevem os fins e procedimentos, ou seja, as políticas não são directrizes ou *standards*, nem procedimentos ou controlos, as políticas descrevem a segurança em termos genéricos, não específicos.

Uma outra perspectiva apresenta as políticas de segurança como um conjunto de práticas que definem como a organização gere, protege e atribui recursos de modo a atingir os seus objectivos de segurança [Hare 2002]

A segurança da informação pode assim ser entendida como o conjunto de medidas que constituem basicamente a política de segurança, pretendendo a protecção das informações relativas aos clientes e aos negócios, procurando simultaneamente controlar o risco de acessos não autorizados.

A protecção da informação comporta oito aspectos ou actividades fundamentais [Peltier 2001]:

- (1) suporte dos objectivos da organização;
- (2) componente fundamental das obrigações;
- (3) ser necessária;
- (4) responsabilidades e custos devem estar explícitos;
- (5) responsabilidades no exterior da organização;
- (6) aproximação compreensiva e integrada;
- (7) reavaliação periódica;
- (8) condicionada pela cultura da organização.

Sobressai assim a necessidade de definição de políticas de segurança da informação, que segundo a norma BS ISO/IEC 17799 [ISO 2005a], têm como principal objectivo proporcionar directivas de gestão e suporte para a segurança da informação, constituindo a primeira do conjunto de 11 directrizes estabelecidas pela referida norma. A política de segurança da informação deve assim providenciar o comprometimento da gestão e o adequado suporte às actividades essenciais à segurança da informação.

Entender o incremento dos riscos e da sua dimensão, implica a consciencialização por parte das organizações da necessidade de um maior rigor e seriedade na definição das políticas de segurança para o SI, aumentando o seu nível e rigor particularmente face à actual dependência das organizações perante os seus SI [Reis e Amaral 2002].

Neste sentido, segundo Barman [2002], verifica-se que as responsabilidades da gestão relativas à segurança da informação devem ser parte integrante do processo, indo além do simples apoio básico, tornando-se parte integrante do processo e demonstrando liderança de forma idêntica ao que sucede relativamente a outros aspectos na organização.

No mesmo contexto, Carneiro [2002] refere a importância de um adequado conhecimento e entendimento das relações entre segurança, risco e informação, por parte dos responsáveis organizacionais e dos utilizadores, considerando o seu potencial impacto no funcionamento da própria organização.

A referida política de segurança da informação deve ser suportada por um documento que deve ser do conhecimento de todos os colaboradores da organização, constando dele o comprometimento da gestão, a definição do que se entende por segurança da informação, a descrição das políticas, a definição das responsabilidades pela segurança da informação e ainda as referências a documentação de suporte, procurando obter-se a colaboração do maior número possível de Pessoas.

Associados às questões de segurança da informação e dos SI, existem riscos que afectam a actividade das organizações e que devem atender às ameaças, às vulnerabilidades e ao valor dos activos a proteger [Henry 2002], onde é essencial que a definição da política de segurança da informação na organização proceda à sua caracterização, permitindo responder adequadamente às ameaças e reduzindo simultaneamente as vulnerabilidades identificadas.

Vulnerabilidade pode ser entendida como uma fraqueza ou falha num sistema ou mecanismo de protecção que expõe activos de informação a ataques ou danos [Pfleeger and Pfleeger 2003, Whitman and Mattord 2005], como uma fraqueza num sistema, aplicação ou infra-estrutura, que pode ser explorada para violar a integridade do sistema [Peltier 2001], ou ainda como uma fraqueza de um activo ou grupo de activos que podem ser explorados por uma ou mais ameaças [ISO 2004].

Uma outra definição, apresentada por Herrmann [2002] entende vulnerabilidade como uma fraqueza num sistema, que pode ser utilizada para violar o comportamento pretendido desse sistema relativamente à sua segurança, confiança, disponibilidade e integridade.

Ameaça é qualquer capacidade, intenção e método de ataque de adversários para explorar ou causar dano à informação ou a um sistema [King *et al* 2001], com as ameaças a serem definidas pelos autores como passivas (monitorizando mas não alterando a informação) ou como activas (alterando deliberadamente a informação).

Numa perspectiva complementar, ameaça pode ser definida como as capacidades, intenções e métodos de ataque de adversários, ou qualquer circunstância ou evento, seja de origem externa ou interna, com potencial para causar danos à informação, programa ou sistema, ou mesmo originar que estes causem danos a outros [ISO 2002].

Outra definição considerando o contexto da segurança da informação é proporcionada por Whitman and Mattord [2005], que entendem ameaça como um objecto, Pessoa ou outra entidade que representa um perigo constante para um activo, ou ser também entendida como um evento com potencial para causar acessos não autorizados, modificações ou destruição dos recursos de informação, de aplicações ou de sistemas [Peltier 2001].

Como ameaças mais comuns com que a informação organizacional e o SI que a suporta se confronta, identificam-se segundo Whitman and Mattord [2005]:

- ⇒ Acidentes ocasionados pelos utilizadores ou técnicos;
- ⇒ Violação da propriedade intelectual;
- ⇒ Actos deliberados de sabotagem ou vandalismo;
- ⇒ Actos deliberados de espionagem ou extorsão de informação;
- ⇒ Roubo;
- ⇒ Variações na qualidade de serviço;
- ⇒ Desastres naturais;
- ⇒ Falhas ou erros de *software* ou *hardware*;
- ⇒ Ataques deliberados de *software* (vírus informático e outro *software* malicioso).

Outra perspectiva em termos de ameaças, ou de actividades ilícitas ou não autorizadas, na acepção de Zúquete [2006], considera cinco tipos base:

- (1) Acesso a informação;
- (2) Alteração de informação;

- (3) Utilização exagerada ou abusiva de recursos computacionais;
- (4) Impedimento de prestação de serviço (*denial of service* – DoS);
- (5) Vandalismo.

Nesta envolvente, a segurança da informação pode também ser entendida como o conjunto de medidas que constituem basicamente a política de segurança, referenciada por Zúquete [2006] como um plano de alto nível, que descreve os objectivos dos procedimentos, definindo estes por sua vez os detalhes de implementação das políticas, ou seja, proporcionando uma descrição de segurança em termos gerais.

Contudo, segundo Barman [2002], antes de serem escritas as políticas de segurança torna-se necessário determinar quais os objectivos gerais, nomeadamente que actividades de negócio devem ser protegidas, se essa protecção deve atender apenas a fluxos de dados ou aos SI, referindo ainda que o primeiro passo é determinar o que deve ser protegido e porquê.

Por outro lado, a crescente utilização das TIC tem contribuído para o agravamento dos problemas de segurança nas organizações, constatação simples se atendermos ao facto de ferramentas e técnicas estarem disponíveis e acessíveis a todos os potenciais interessados. Todavia, em questões de segurança o que parece fazer a diferença são as Pessoas, situação esta que deve considerar a relevância de medidas tendentes a incentivar as Pessoas a prestar maior atenção e mesmo envolvimento, quer na definição dessas políticas, quer na sua implementação.

A segurança, em particular a de SIBC, encontra-se associada a confidencialidade (garantir que a informação não é acedida por Pessoas não autorizadas) e integridade (garantir que a informação se mantém exacta) da informação [Bishop 2002, Ross 1999]. Neste âmbito deve ter-se também em conta que a disponibilidade da informação deve ser garantida, atendendo às políticas de segurança da informação definidas.

Neste contexto, Reis e Amaral [2002] entendem que a implementação das medidas de segurança implica a sua gestão de acordo com o planeado, considerando os objectivos da segurança, a avaliação do risco, o estabelecimento de medidas de segurança, a atribuição de responsabilidades, o teste da segurança do sistema e ainda a avaliação dos níveis de segurança implementados.

4.5. Sistemas de Gestão da Segurança da Informação

A opção das organizações por SI e TIC traduziu-se em mudanças nos procedimentos organizacionais, afectando claramente as suas actividades de negócio e de suporte, situação esta que comportou custos adicionais para as organizações, quer em termos dos investimentos necessários para suportar as actividades de negócio, quer em termos de necessidades de formação para a utilização dos SI e das TIC implementadas.

A questão dos investimentos em SI e TIC costuma aliás revelar-se crítica para as organizações cujo *core-business* não são os SI e as TIC, essencialmente porque a sua maioria encara estes investimentos como um custo que a organização tem de suportar, não vislumbrando, por conseguinte, qualquer vantagem, financeira ou organizacional na sua concretização.

A aquisição de SI e de TIC por parte das organizações acaba por se dar na sequência de imposições dos mercados, por decisão dos seus principais responsáveis, ou mesmo por imposição do sector de actividade onde se inserem. Todavia, qualquer que seja o motivo inicial, o que sucede frequentemente não tem a ver directamente com decisões estratégicas ou políticas, mas sim com questões meramente pontuais, sucedendo muitas vezes que os SI e as TIC apenas se adquirem porque os concorrentes ou os parceiros de negócio também o fazem.

As aquisições por imposição dos mercados cingem-se habitualmente ao estritamente necessário para o cumprimento de um conjunto restrito de funções, que acabam por não responder cabalmente às necessidades das organizações, pois focam-se apenas nas respostas obrigatórias aos requisitos de negócio.

Já as aquisições que ocorrem só porque os concorrentes ou os parceiros também possuem, revelam-se quase sempre completamente desajustadas para a realidade e para as necessidades das organizações, essencialmente pela especificidade inerente a cada organização e às Pessoas que a integram, mesmo que a actividade de negócio seja a mesma.

Com as aquisições feitas por iniciativa dos principais responsáveis das organizações, verifica-se que se adequam às estratégias organizacionais e respondem às suas principais necessidades, geralmente porque permitem a resolução de alguns problemas

identificados por esses mesmos responsáveis, mesmo quando a sua abrangência não se estende à totalidade das necessidades organizacionais.

Denota-se então uma necessidade de proceder à adequação das estratégias dos SI e das TIC com as estratégias organizacionais, o que corresponde actualmente à situação vigente em muitas organizações.

Para a generalidade das organizações verifica-se que os custos de aquisição de SI e TIC não se restringem exclusivamente a SI e TIC, englobando também as respectivas envolventes como sejam os serviços de consultoria e análise e a formação dos utilizadores, comportando simultaneamente mudanças organizacionais.

Implementar políticas de segurança implica que a organização disponibilize recursos humanos e financeiros, o que, perante os valores habitualmente envolvidos, conduz à imposição de restrições e condicionamentos diversos à utilização dos SI, com estes aspectos a serem frequentemente incompreendidos por parte da estrutura organizacional [Veiga 2002].

Desta forma, a necessidade de suportar estes investimentos em SI e TIC leva a que as organizações procedam a controlos apertados nos montantes investidos, deixando de fora os aspectos encarados como não essenciais, tais como os que se relacionam com a facilidade de utilização dos SI (usabilidade) e com a sua segurança, ficando também de fora a satisfação dos utilizadores e a segurança da informação de negócio, genericamente porque estes aspectos não são entendidos e assumidos como fundamentais para o desempenho da organização.

Assim, face aos desafios actuais que se colocam às organizações, em particular às que apostaram nos SI e nas TIC para suportar os requisitos que os novos mercados lhes colocam, a segurança entendida como um componente global deve ser parte integrante do projecto inicial dos SI.

Neste sentido, considera-se que a estratégia dos SGSI directamente relacionada com a estratégia organizacional, deve ser tida em atenção no estabelecimento da estratégia dos SI, pelo que se procede à alteração do modelo de adequação estratégica definido por Edwards *et al* [1995], interligando-o com a estratégia dos SGSI.

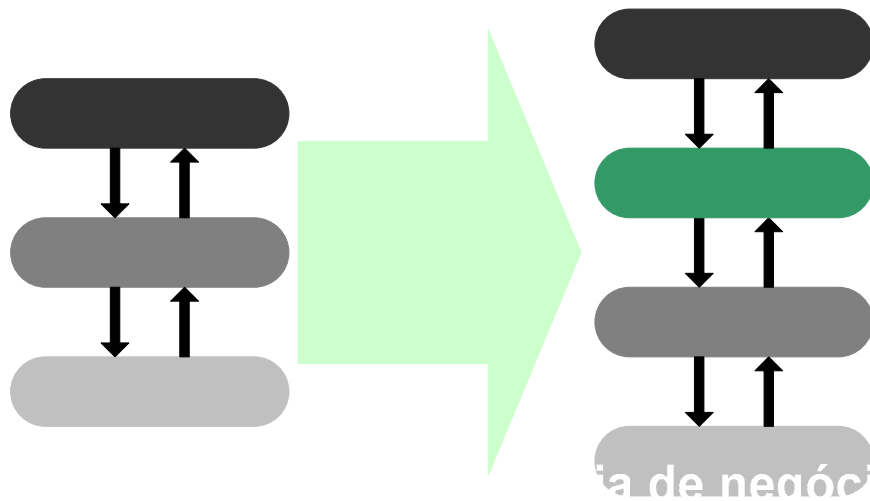


Figura 4.3 – Integração da estratégia dos SGSI na estratégia da organização

A implementação de políticas e sistemas de segurança envolve recursos financeiros e humanos, mas comporta essencialmente mudanças nas estruturas organizacionais que não são cabal e adequadamente entendidas no interior das organizações, particularmente pela escassez de informação disponibilizada. A implementação dos potenciais impactos nas actividades organizacionais.

A necessidade de dispor de equipamentos adequados às actividades da organização e de mais formação para técnicos e utilizadores, conduzem frequentemente à implementação de formação contínua e à mudança dos equipamentos que suportam a actividade de negócio, factos que contribuem para aumentar os custos associados aos SI e para diminuir a sua usabilidade.

Todavia, no estabelecimento de políticas de segurança, torna-se importante atender à relação custo-benefício de modo a que os custos habitualmente associados às violações do SI ou mesmo às medidas tomadas para as evitar, não sejam superiores aos eventuais benefícios obtidos com a utilização do SI.

Neste sentido, a identificação das melhores políticas (soluções) de segurança para uma organização devem atender a factores como os recursos humanos, os recursos técnicos e os recursos financeiros que a organização pode disponibilizar, procurando responder às necessidades de negócio ao garantir a segurança da sua informação, assim como dos SI e das TIC que os suportam.

4.6. Conclusões

Os aspectos associados à segurança sempre estiveram presentes na evolução da humanidade, indo desde a satisfação das necessidades mais básicas nos seus primórdios até aos problemas com os impactos das tecnologias nas actividades das Pessoas e os receios de perda de estabilidade financeira e social, realçando por isso a necessidade de garantir a segurança da informação pessoal e organizacional.

Com a emergência da Sociedade da Informação, potenciada pela crescente globalização social e económica e pelo surgimento de novas TIC, as Pessoas têm visto crescer a sua importância para as actividades organizacionais e sociais, não só pelas suas capacidades e competências na utilização das TIC, mas também pelo papel que podem desempenhar na aquisição de vantagens competitivas, ao ser possibilitado um maior envolvimento nas actividades organizacionais.

A globalização e os seus impactos nas Pessoas, nas organizações e nas sociedades, forçou mudanças de atitudes e alterações nas estruturas e actividades organizacionais, motivadas essencialmente pelos novos mercados, por clientes mais exigentes e pela crescente dependência dos SI e das TIC e das Pessoas que as utilizam, para melhorar a competitividade e o desempenho das organizações, mesmo num ambiente onde a segurança, da informação, dos SI, das TIC e mesmo das Pessoas, é fundamental para um adequado desempenho neste contexto.

Por outro lado, verifica-se genericamente, que a segurança da informação parece não fazer parte integrante das principais preocupações dos decisores organizacionais, conduzindo inevitavelmente a uma menorização do seu papel nas actividades organizacionais. Constatava-se todavia que esta atitude apenas se altera quando ocorre algum problema com a informação de negócio, surgindo a necessidade de modificação das atitudes face a esta problemática.

Nesse sentido, identificar que activos organizacionais necessitam de protecção, estabelecer e implementar políticas adequadas, não apenas a proteger esses activos mas também a respeitarem a missão e os objectivos organizacionais, requer a participação de todos os envolvidos nas actividades de negócio

Além disso, a utilização do normativo adequado a suportar a definição e implementação de políticas de segurança ou dos mais abrangentes SGSI, apresenta-se como uma opção viável para responder a muitos dos problemas em termos de segurança com que as organizações actualmente se deparam.

Conclui-se assim da necessidade de um claro comprometimento da gestão de topo com as actividades associadas às políticas de segurança e aos SGSI, proporcionando também os recursos necessários e adequados às tarefas identificadas.

Pode assim concluir-se que a segurança da informação e dos SI é uma necessidade das organizações, considerando essencialmente o facto de estes serem assumidos como importantes activos organizacionais, procurando entender os benefícios que possam decorrer da sua implementação.

Todavia, conclui-se ser igualmente importante que os SI e as TIC que os suportam sejam fáceis de aprender e utilizar, evitando-se desde logo eventuais oposições por parte das Pessoas ao assegurar a sua participação nos processos de alteração ou mudanças, possibilitando a inclusão nesses SI dos requisitos funcionais identificados pelos utilizadores em resposta às suas expectativas e necessidades.

Constatando-se habitualmente que a implementação de políticas de segurança nas organizações afecta a forma como as Pessoas utilizam os SI e as TIC, importa identificar e implementar os mecanismos necessários a minimizar ou até mesmo evitar os impactos daí derivados, particularmente quando as Pessoas constituem, a par da informação, um dos mais importantes activos organizacionais.

Referências bibliográficas

APDSI, *Glossário da Sociedade da Informação*, José Palma Fernandes (Coordenador), Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI), Outubro de 2005.

Barman, S., *Writing Information Security Policies*, New Riders Publishing, 2002.

Berti, J. and Rogers, M., “Social Engineering: The Forgotten Risk”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 3, 4th Edition, Auerbach Publications, 2002, p.51-63.

Bishop, M., *Computer Security: Art and Science*, Adisson-Wesley Professional, 2002.

- Carneiro, A., *Introdução à Segurança dos Sistemas de Informação*, FCA, 2002.
- Castells, M., *A Galáxia Internet: Reflexões sobre Internet, Negócios e Sociedade*, Fundação Calouste Gulbenkian, 2004.
- Cerveira, A.G., “Informática e Mecanografia”, *Associação Internacional de Estudos sobre Mecanografia*, IV Encontro Internacional de Mecanografia e Informática, Outubro de 1967, p.45-50.
- Edwards, C., Ward, J. and Bytheway, A., *The Essence of Information Systems*, 2nd Edition, Prentice Hall, 1995.
- Fenton, J.H. and Wolfe, J.M., “Organizing for Success: Some Human Resources Issues in Information Security”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 4, 4th Edition, Auerbach Publications, 2003, p.313-324.
- Fernandes, J.P., Correia, M. e Antunes, M., “A Terminologia e a Sociedade da Informação”, in José Dias Coelho (Coordenador), *Sociedade da Informação – O percurso Português*, Edições Sílabo, 2007, p.457-472.
- Hansche, S.D., “Making Security Awareness Happen”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 3, 4th Edition, Auerbach Publications, 2002, p.317-335.
- Hare, C., “Policy Development”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 3, 4th Edition, Auerbach Publications, 2002, p.353-383.
- Henry, K., “Risk Management and Analysis”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 3, 4th Edition, Auerbach Publications, 2002, p.407-418.
- Henry, K., “The Human Side of Information Security”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 4, 4th Edition, Auerbach Publications, 2003, p.239-261.
- Herrmann, D.S., *A Practical Guide to Security Engineering and Information Assurance*, CRC Press, 2002.
- Herold, R., “Information Protection: Organization, Roles, and Separation of Duties”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 4, 4th Edition, Auerbach Publications, 2003, p.415-439.

- ISO, *ISO/IEC 21827 – Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM)*, International Standard Organization, 2002.
- ISO, *ISO/IEC FDIS 13335-1 – Information technology - Guidelines for the management of IT security - Concepts and models for information and communications technology security*, International Standard Organization, 2004.
- ISO, *BS ISO/IEC 17799 (BS 7799-1:2005) – Information Technology - Code of practice for information security management*, British Standard Institution, 2005.
- King, C.M., Dalton, C.E. and Osmanoglu, T.E., *Security Architecture: Design, Deployment & Operations*, Osborne/McGraw-Hill, 2001.
- Mamede, H.S., *Segurança Informática nas Organizações*, FCA, 2006.
- Parker, D., “Toward a new Framework for Information Security”, in S. Bosworth and M.E. Kabay, (Editors), *Computer Security Handbook*, 4th Edition, John Wiley & Sons, 2002.
- Peltier, T.R., *Information Security Risk Analysis*, Auerbach Publications, 2001.
- Pfleeger, C.P. and Pfleeger S.L., *Security in Computing*, 3rd edition, Prentice Hall, 2003.
- Reis, L., *Planeamento de Sistemas de Informação e da Contingência e da Recuperação*, Tese de Doutoramento, Universidade do Minho, 2000.
- Reis, L. e Amaral, L., “Gestão de Riscos num contexto de Planeamento da Contingência e Recuperação”, Actas (formato digital) da 3^a Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.
- Ross, S., “Computer Security: A practical definition”, 1999, <http://www.albion.com/security> (31-10-2003).
- Veiga, P., “Prefácio”, in Alberto Carneiro, *Introdução à Segurança dos Sistemas de Informação*, FCA, 2002.
- Whitman, M.E. and Mattord, H.J., *Principles of Information Security*, 2nd Edition, Thomson Course Technology, 2005.
- Zúquete, A., *Segurança em Redes Informáticas*, FCA, 2006.

5

As Pessoas

Mesmo o facto de serem frequentemente identificadas como o elo mais fraco no contexto da segurança da informação, a presença das Pessoas e a sua importância para as actividades organizacionais impõe que se tenha em atenção as suas necessidades e anseios. Os aspectos motivadores e a sua envolvimento nos processos directamente relacionados com as suas actividades organizacionais podem e devem servir como impulsionadores do desempenho das Pessoas e consequentemente das organizações em que se inserem.

Qualquer abordagem à segurança da informação, e consequentemente também dos SI e das TIC que a suportam, deverá ter em atenção os impactos originados pelas Pessoas que manipulam essa informação, independentemente do grau de utilização motivado pelas suas necessidades específicas, tornando-se assim fundamental a obtenção de uma perspectiva alargada dos seus anseios, com esta perspectiva a ser condicionada pela sua cultura assim como pelos seus objectivos pessoais e sociais.

5.1. O Capital Humano das Organizações

Habitualmente considerada como um importante activo organizacional, a informação, e consequentemente os SI e as TIC que a suportam, encontra-se condicionada pela utilização que as Pessoas fazem dela, particularmente quando se torna necessário assegurar a manutenção da sua confidencialidade, integridade e disponibilidade.

Neste âmbito, uma das muitas questões que se colocam é saber como recolher e seleccionar informação de entre a sua grande disponibilidade, considerando que isso é um processo humano que requer um alto grau de experiência acumulada em organizações, ou seja, de capital humano [Reponen 1998].

O capital humano, de acordo com Garcia [2005], compreende as aptidões e competências das Pessoas e a sua utilização para melhorar o desempenho das organizações que integram, recorrendo às capacidades, experiências, princípios e

valores que possuem. Este capital, segundo o mesmo autor, pode ser aumentado pela valorização e retenção das competências pessoais por parte da organização, desenvolvendo-se em consonância com as políticas de gestão de recursos humanos.

O capital humano é um dos activos intangíveis²⁰ que faz parte integrante do Capital Intelectual, com capital humano a ser entendido como “as capacidades, conhecimentos, experiência e facilidade de resolução de problemas que reside nos indivíduos de uma organização” [Pinto *et al* 2005].

Todavia, o grau de exigência das TIC nas organizações tem também implicações ao nível das Pessoas, levando, segundo Serra [1998], à “desvalorização das qualificações tradicionais e à exigência de novas qualificações”. Torna-se assim importante que as opções tomadas no respeitante à adopção dessas tecnologias, atendam simultaneamente à emergência dos novos papéis que as Pessoas tendem a desempenhar nas organizações. Constata-se então a indispensabilidade de a aprendizagem (actualização de conhecimentos, desenvolvimento de novas competências, promoção de novos perfis profissionais) se concretizar de forma contínua para proporcionar novas mobilidades [Kovács 1998, Lindley 2000].

Neste âmbito, Hansche [2002] entende que ao considerar as Pessoas como o mais importante activo organizacional, lhes deve ser propiciada formação adequada a suportar eficazmente o funcionamento e a protecção do SI.

Considerando que informação, conhecimento e aprendizagem são conceitos “associados às pessoas, às organizações e à sociedade”, Anunciação e Zorrinho [2006] assumem que a memória individual e colectiva, inerentes às Pessoas, e às organizações e sociedades respectivamente, constituem “a base de conhecimento que possibilita a troca ou a partilha de informações e a consequente aprendizagem”.

Estes aspectos têm a sua importância definida e condicionada pela utilização e propósitos que a organização encontra para a informação de negócio, comportando especificidades de aquisição, tratamento e partilha com os parceiros organizacionais, necessitando por isso mesmo das Pessoas adequadas à prossecução das suas actividades.

²⁰ Sendo os outros o capital estrutural e o capital relacional.

Neste contexto, Barman [2002] refere que, de entre todos os recursos, o mais importante e dispendioso de todos eles são os humanos, que utilizam e mantêm a lista dos activos organizacionais, ou seja, a lista dos documentos, programas, *hardware*, sistemas, processos e documentação acerca dos processos de negócio. A inventariação, segundo o autor, das Pessoas envolvidas na utilização dos sistemas, dados e recursos de computadores, pode proporcionar uma visão dos aspectos para os quais são necessárias as políticas.

Perante a relevância das Pessoas nas organizações, é essencial que exista segurança nos respectivos empregos para que as Pessoas possam investir tempo e energia no seu desenvolvimento pessoal, procurando simultaneamente suprir as necessidades das organizações a que pertencem [Ulrich 1998].

O factor humano emerge então como um dos principais elementos a considerar quando se assume a indispensabilidade da colaboração das Pessoas (particularmente utilizadores e técnicos) para manutenção da segurança do SI, independentemente da sofisticação e preço dos meios e dispositivos disponibilizados [Carneiro 2002].

As Pessoas, as suas ligações com a organização e o modo como estas entendem a informação organizacional e pessoal emergem como factores fundamentais aos quais deve ser dedicada especial atenção, essencialmente quando se considera a sua utilização nas actividades organizacionais e a necessidade de garantir a sua privacidade,.

Considerando o contexto de mudança decorrente quer da globalização dos mercados, quer da utilização das TIC, Dinis [2005] considera que os colaboradores da organização podem tolerar melhor as mudanças, caso encarem essas mesmas mudanças como relevantes e entendam a sua importância num ambiente de imparcialidade e transparência.

Neste sentido, perante o impacto das Pessoas na utilização das TIC, importa não descurar a necessidade de se proceder à escolha criteriosa dos utilizadores, tendo em vista a redução da hipótese de acesso por parte de intrusos [Silberschatz *et al* 2003]. Importa assim considerar a adequação dos processos de recrutamento às necessidades concretas e objectivas da própria organização, em função da maior ou menor criticidade da informação e dos SI e TIC com que é presumível as Pessoas venham a trabalhar.

Constando a relevância da informação para as organizações, e simultaneamente a forma como as Pessoas actuam perante a informação, Neves [2001] referencia uma perspectiva apresentada por Lindsay and Norman²¹ que enquadra as fases de percepção das Pessoas acerca da informação com os fenómenos implicados nessa percepção. A figura seguinte apresenta esse mesmo enquadramento.

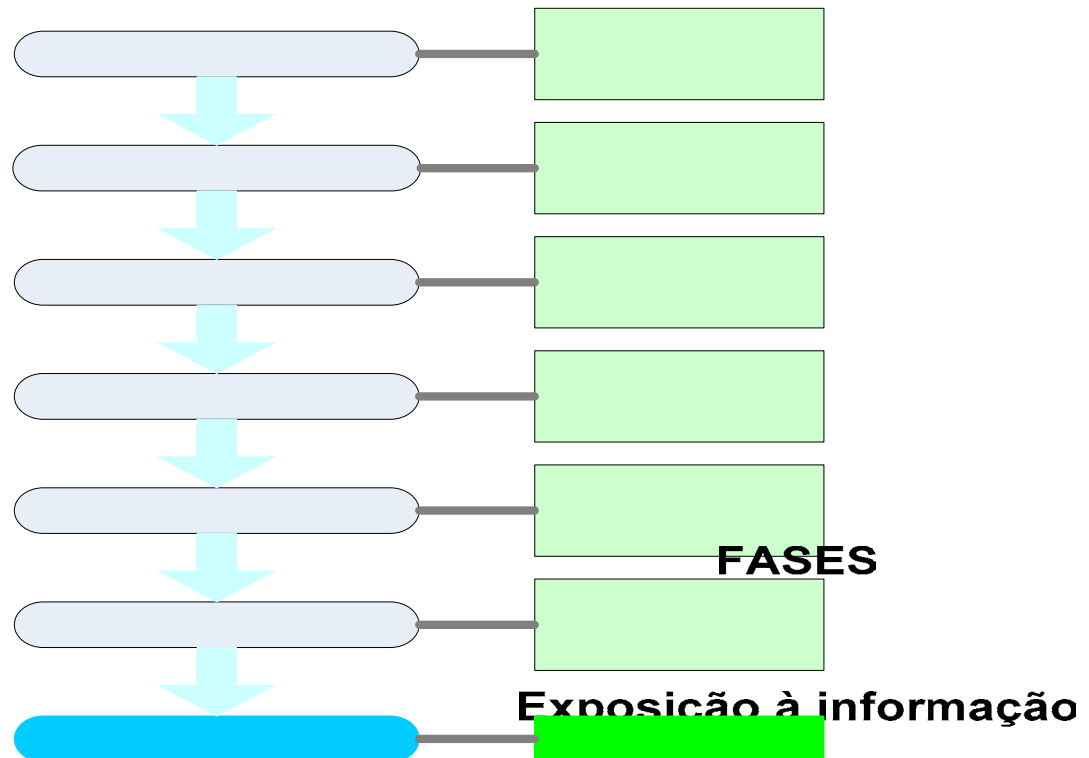


Figura 5.1 – O indivíduo como um sistema processador de informação
(Adaptado de Lindsay and Norman [1972], citado por Neves [2001])

Esta perspectiva enquadra a importância das Pessoas nas actividades relacionadas com a **Perceber a informação** informação organizacional, num contexto onde podem desenvolver as suas competências e potenciar o desempenho da organização, considerando os diversos fenómenos envolvidos na actuação das Pessoas sobre a informação.

Deve assim constatar-se que o comportamento das Pessoas, quando colocadas perante desafios que lhes exigem, mais formação e empenho, resultará do seu envolvimento na **Compreender a informação** organização e da forma como percebem esses desafios, actuando conseqüentemente em conformidade com a sua perspectiva pessoal.

²¹ Lindsay, P.H. and Norman, D.A., *Human Information Processing: An Introduction to Psychology*, Academic Press, 1972.

Validar a informação

Reter a informação

Pelo que, face às mudanças organizacionais motivadas pela implementação de novas TIC, a formação das Pessoas, uma maior disponibilização de informação, a necessidade de garantia da segurança e da privacidade da informação, são factores cuja relevância implica aceitação das novas TIC por parte dos utilizadores finais, proporcionando a sua integração nos processos de trabalho [Misiólek *et al* 2002].

No respeitante às organizações, considera-se pertinente a perspectiva apresentada por Ferreira *et al* [2001] onde as organizações são entendidas como “um sistema social composto por subsistemas que integram acções individuais e colectivas”, referindo ainda que as organizações só podem ser eficientes e eficazes se existir “uma compreensão profunda e sistemática dos seres humanos que nelas trabalham e vivem”.

Por outro lado, considerando que as organizações são uma obra das Pessoas, constituídas por Pessoas e com o objectivo primordial de servir as necessidades das Pessoas, detecta-se claramente que também existem relações difíceis entre as organizações e as tecnologias, em particular quando as tecnologias em causa são as que permitem uma partilha ampla de informação entre as Pessoas e parceiros de negócio, ou seja, as TIC.

Todavia, essa constatação deve atender ao facto das implicações das interacções entre TIC, SI, Pessoas e segurança serem variadas e nem sempre claramente perceptíveis, tornando-se importante considerar as consequências da utilização da Internet, quer pelas potencialidades que apresenta em termos de facilidade de acessos aos sistemas e à informação, quer pela exposição que envolve por parte das Pessoas e das organizações [Smith and Dinn 1999].

Neste âmbito, a situação assume-se tanto mais crítica quanto as Pessoas forem consideradas como um entrave a uma efectiva segurança dos computadores [Whitten and Tygar 1998], em especial pela utilização de controlos tecnológicos que podem ser facilmente ultrapassados pela intervenção humana [Bishop 2002].

As competências e o comprometimento das Pessoas com as organizações encontram-se relacionadas, segundo Ulrich [1998], com o que cada um pensa acerca do que faz e como faz, considerando também as políticas adoptadas e os sistemas criados pela organização de modo a certificar-se que as tarefas são executadas.

Neste contexto, garantir a adesão das Pessoas às mudanças nos SI e nas TIC, com particular atenção para uma identificação adequada das suas necessidades e expectativas, confronta-se frequentemente com as exigências que emergem por força das estruturas organizacionais e dos seus modelos de negócio, levando a que a obtenção do seu comprometimento seja entendida como essencial.

5.2. As Pessoas e as Tecnologias de Informação e Comunicação

O comportamento das Pessoas no seu contexto de trabalho é, segundo Neves [2001], “influenciado pela forma como as pessoas percebem a realidade que as rodeia”, considerando que essa percepção depende maioritariamente do que é importante e significativo para a pessoa e não da “essência objectiva da realidade percebida”.

Desenvolver competências envolve aprendizagem organizacional, ou seja, aprender como combinar e usar recursos, incorporando também a aprendizagem já envolvida nas rotinas organizacionais utilizadas. As combinações possíveis entre rotinas e recursos disponíveis e os resultados obtidos são assim muito variáveis visto que dependem de condições específicas de cada momento.

A partir do momento em que a aprendizagem toma o seu lugar no contexto organizacional, as capacidades distintivas dependem do caminho escolhido, isto é, têm um alto grau de especificidade, facto este que é crucial para que sejam difíceis de imitar e ainda para que resultem em vantagens sustentáveis e duráveis [Ciborra and Andreu 1998].

Todavia, a velocidade com que as TIC entram no dia a dia das organizações leva a que estas não necessitem apenas de especialistas, mas também que os utilizadores sejam capazes de desempenhar cabalmente as suas tarefas sem recurso a apoio técnico ou com necessidades mínimas de suporte. Esta situação requer que as aplicações e o *hardware* disponibilizado sejam fáceis de aprender e usar, permitindo que o nível de conhecimentos necessários se encontre ao nível do utilizador final.

Os estudos de aceitação das tecnologias, em especial das que suportam a informação nas organizações, têm sido efectuados com recursos a alguns modelos, de entre os quais se destaca o Modelo de Aceitação das Tecnologias (referenciado usualmente como

Technology Acceptance Model – TAM), apresentado por Davis [1989], que se suporta essencialmente na percepção (utilidade e facilidade de uso), nas intenções (de uso) e nos comportamentos (situação de uso actual) dos utilizadores, factores estes que, segundo o autor, são fundamentais para que os utilizadores aceitem e utilizem as tecnologias.

Neste âmbito, Santana e Dias [2005] referem a utilidade percebida como o grau “em que o potencial utilizador acredita que a utilização do sistema irá melhorar o seu desempenho”, enquanto que “a percepção de simplicidade de utilização mede o grau da crença do indivíduo na simplicidade na utilização da tecnologia”, o que leva as autoras a assumir que, no caso da percepção de utilidade ser elevada e a sua utilização ser simples, fica facilitado o processo de adesão e utilização das tecnologias.

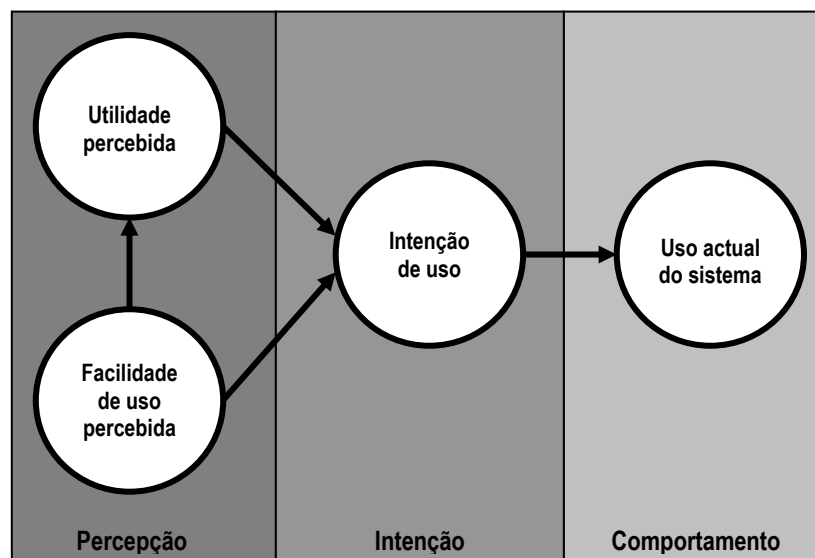


Figura 5.2 – Modelo de Aceitação das Tecnologias
(Adaptado de Davis [1989])

Considerando que as Pessoas, utilizadores actuais e potenciais da informação, dos SI e das TIC que a suportam, desempenham um papel crucial nos SGSI, verifica-se que o modo como aceitam e utilizam as TIC e os SI torna-se um factor fundamental para o sucesso das implementações de segurança efectuadas na generalidade das organizações, mesmo considerando o facto de nem todas as componentes do SGSI se relacionarem com as tecnologias.

Perante a percepção, intenção e comportamento das Pessoas acerca da aceitação das tecnologias (TAM), constata-se que a usabilidade (facilidade de aprendizagem e utilização) pode reflectir o maior ou menor grau em termos de aceitação das

tecnologias, particularmente quando as necessidades básicas das Pessoas estão atingidas, fazendo emergir como cruciais os aspectos de segurança, ou mais propriamente ‘necessidades de segurança’, de acordo com as teorias de Maslow [1954], que enquadram a auto preservação e evitar ameaças, perigos e privação.

Garantir a segurança pode afectar a usabilidade dos SI e das TIC que os suportam, principalmente pelas implicações que impõe na utilização dos SI e das TIC, onde a aceitação das tecnologias e consequentemente das necessidades de segurança da informação poderá ser afectada se essas necessidades não forem entendidas pelas Pessoas como úteis e potenciadoras do seu próprio desempenho.

Segundo o Relatório FRISCO [Falkenberg *et al* 1998], os SI dizem respeito à utilização da informação por Pessoas ou grupos de Pessoas nas organizações, particularmente através de SIBC, com a sua natureza a ser entendida no contexto em que as organizações os utilizam.

Desenvolver competências na área dos SI/TI possibilita a construção interna de sistemas informáticos, além de potenciar o diálogo entre utilizadores, habitualmente não especialistas em SI/TI, e os profissionais dessas áreas relacionados com os fornecedores de serviços e produtos [Caldeira e Romão 2002b]. Estes autores referem ainda que deve ser assegurada a sua formação e o apoio necessário ao desempenho das suas actividades, no sentido de aumentar o nível de eficiência dos utilizadores.

Genericamente é possível constatar que as dificuldades sentidas relativamente às TIC derivam mais do receio que existe relativamente ao desconhecido do que da incapacidade das Pessoas em lidarem com essas tecnologias, assumindo particular relevância quando a sua utilização pode afectar as relações de poder no interior das organizações.

Pode assim constatar-se que a introdução na organização de novas tecnologias e em particular de TIC tende sempre, segundo Zorrinho [1991], a ser um factor de conflito com a rotina e com o poder instalados, interessando demonstrar que dessas inovações e desenvolvimento subsequentes, depende a evolução e sobrevivência global da organização. Zorrinho [1999] referencia também que “o saber, a disponibilidade de infra-estruturas e a capacidade de acesso à Informação”, são fontes crescentes de poder

pela alteração que provocam em seu favor perante as antigas fontes de poder “radicadas no património e na força bruta”.

Caldeira e Romão [2002b] referem a propósito que o facto de ser implementado um sistema informático numa organização afecta as relações de poder no interior dessa organização, essencialmente devido à diversidade de modos com que as Pessoas reagem a essa situação, umas entendendo a sua utilização como um benefício próprio, outras assumindo o facto como um perigo capaz de reduzir a sua influência no interior da organização.

Além disso, a forma como as TIC são compreendidas relaciona-se também com a influência que detêm nas organizações, em especial nos aspectos relacionados com o suporte às actividades organizacionais, onde podem assumir um papel fulcral na aquisição de vantagens competitivas. Acresce ainda que a percepção dos papéis desempenhados pelas TIC depende em grande parte dos decisores organizacionais e no como perspectivam a sua aplicação na prossecução dos objectivos da organização.

A este propósito, Caldeira e Romão [2002b] referem que o envolvimento da gestão de topo na adopção de SI/TI desempenha um papel fundamental para contrariar a resistência à mudança surgida quando são implementados novos sistemas e tecnologias, particularmente as TIC.

Neste sentido deter capacidades adequadas à utilização eficaz e eficiente das TIC emerge como um dos factores capazes de garantir o sucesso das organizações, em particular quando o ambiente competitivo depende em grande escala da utilização dessas TIC para suportar os negócios.

A posse de capacidades adequadas ao trabalho com as TIC, nomeadamente as que podem contribuir para adicionar valor às actividades de negócio, constitui então um importante factor de valorização pessoal capaz de motivar a aquisição de novas competências. O facto de a aquisição de competências ser entendida como um factor potenciador da competitividade das organizações contribui para reforçar o valor das Pessoas para as organizações e para as sociedades onde se inserem.

5.3. Caracterização e Tipificação dos Utilizadores

Face à actual difusão dos SI e das TIC, a existência de receptores puros da informação tem tendência para se reduzir, particularmente se for assumido que cada utilizador da informação deve assumir a responsabilidade pela sua segurança, surgindo esta tarefa como comum e partilhada por todos os utilizadores. Todavia, nas situações em que os clientes não possuem qualquer hipótese de interacção com o SI da organização, poderá considerar-se que estes são receptores puros, assumindo-se no entanto que esta é uma situação cada vez mais rara.

Perante os referidos aspectos, tipificar os utilizadores poderá ser vantajoso no sentido de permitir um enquadramento adequado da informação e da sua utilização, confrontando-se com a diversidade de sectores de actividade e de culturas organizacionais, pelo que deve ser entendida como um quadro de referência, necessariamente ajustável aos requisitos de cada organização de *per si*.

Neste âmbito, Tudor [2001] refere que utilizadores do sistema são os funcionários, os subcontratados, fornecedores, consultores e quaisquer parceiros de negócio que utilizem os recursos do SI para desempenharem as suas actividades, considerando que as suas responsabilidades de segurança incluem os seguintes aspectos:

- Manter a confidencialidade das *passwords*;
- Assegurar a segurança da informação que utilizam como parte do seu trabalho;
- Utilizar os recursos da organização apenas para os propósitos aprovados pela gestão;
- Aceitar todas as políticas, procedimentos e *standards* de segurança da informação;
- Reportar à gestão quaisquer eventos ou incidentes de segurança.

Consideradas como um dos mais importantes activos organizacionais, a par da informação, as Pessoas e a sua capacidade de utilização dos SI e das TIC podem afectar o desempenho das organizações, tornando-se frequentemente necessário proporcionar formação adequada à plena utilização dos SI e das TIC.

Formar os utilizadores deve incluir a utilização apropriada do sistema e as razões para os vários controlos e parâmetros de segurança construídos no sistema, onde, sem

divulgar os detalhes dos controlos, explicar as razões para os controlos pode ajudar os utilizadores a aceitar e a aderir às restrições de segurança construídas no sistema [Henry 2003].

Neste âmbito, Carneiro [2002] refere a importância de ser proporcionada às Pessoas a formação e informação adequadas, abrangendo igualmente os responsáveis organizacionais, considerando assim que a protecção não deve basear-se apenas em meios físicos, mas abarcar os aspectos essenciais para as actividades organizacionais.

Deste modo, considera-se que a abrangência da formação deve permitir a aquisição de um conjunto de capacidades e de competências que potencie uma evolução sustentada das Pessoas no seu progresso social e profissional, possibilitando assim a construção de um ambiente de aprendizagem permanente que suporte as necessidades das organizações onde se inserem.

Perante este contexto, Dark [2006] considera que as organizações necessitam de sensibilização, treino e educação sobre segurança, por entender que as Pessoas são a primeira linha de defesa da organização, constituindo uma parte essencial na prevenção, detecção e resposta a quebras de segurança que podem surgir de negligências, acidentes e até de actividades maliciosas contra os SI.

Emerge pois a necessidade de ter em atenção as competências das Pessoas e a sua inserção na actual Sociedade da Informação, onde a exclusão social e económica ganhou outra vertente, a exclusão tecnológica ou mais concretamente a info-exclusão se considerarmos a existência dessa Sociedade da Informação, condicionada pela utilização massiva da informação e suportada pelos SI e pelas TIC.

No contexto abordado, Castells [2004] refere que o conceito de info-exclusão costuma estar ligado à desigualdade no acesso à Internet, embora considere a info-exclusão num contexto global, condicionada pelas infra-estruturas de TIC e pela forma como as sociedades e as organizações actuam perante os desafios da globalização.

Considerando então o contexto anteriormente mencionado, pode entender-se, em termos genéricos, que a percepção do papel dos utilizadores requer a sua tipificação, sendo habitual a separação em utilizadores primários (ou utilizadores finais), utilizadores

secundários (inclui quem instala e quem mantém o sistema) e *stakeholders*²² (quem influencia ou é afectado pelo sistema que não os utilizadores finais).

Numa outra perspectiva, identificando as Pessoas como um activo organizacional, Whitman and Mattord [2005] apresentam a sua tipificação como funcionários e não funcionários, enquadrando os funcionários em duas categorias: aqueles que desempenham cargos de confiança e que possuem a correspondente autoridade e responsabilidade, e aqueles que não têm qualquer privilégio especial. Os não funcionários por seu lado incluem fornecedores, consultores, parceiros de negócio e público em geral.

Uma outra tipificação possível dos utilizadores pode basear-se no grau de utilização do SI e nas funções desempenhadas, identificando-se quem introduz dados, quem depende dos dados para executar o seu trabalho, quem efectua o tratamento dos dados para produzir informação ou quem utiliza apenas a informação produzida por outros.

Todavia, perante a actual Sociedade da Informação, Drucker [1988] considera que um dos requisitos de uma organização baseada em informação é que qualquer um tem responsabilidades na informação, com a actividade da organização a ser desenvolvida à volta do *feedback* organizado dos seus pares, dos seus clientes e das suas delegações, que compara os resultados com as expectativas de desempenho, de forma que cada membro (especialista ou não) possa exercer auto controlo. Este entendimento releva a pertinência da informação e da responsabilidade que sobre ela possuem todos os directa ou indirectamente relacionados com a actividade da organização.

Neste pressuposto, verifica-se que a tipificação dos utilizadores surge especificada numa grande diversidade, o que dificulta desde logo a obtenção de um consenso nesta tarefa.

Sobressai assim uma situação que contribui para reforçar a necessidade de caracterizar os utilizadores em função do seu grau de conhecimentos ou das taxas de utilização dos SI, o que poderá permitir que a segurança da informação a proporcionar encontre o seu apoio tácito, possibilitando a adequação das políticas de segurança às necessidades pessoais e organizacionais.

²² Pessoa ou grupo que está envolvido ou pode ser afectado por um sistema, projecto ou organização em particular [OxfDic 2005].

Verifica-se então que também as necessidades dos técnicos serão certamente diferentes das que os utilizadores apresentam, tal como serão diferentes as necessidades dos gestores, e de entre estes também existirão diferenças em função do nível organizacional em que se inserem.

Neste sentido, serão também diferentes as necessidades específicas de cada departamento ou unidade de negócio, apresentando por isso características distintas que implicam a adequação das políticas de segurança da informação à sua especificidade, considerando a missão e a estratégia de negócio adoptadas pela organização.

Poderá então ser possível constatar que quanto maior for o grau de utilização do SI tanto maior será o grau de dificuldade sentido pelos utilizadores na utilização do sistema. Esta situação permite conjecturar que os potenciais problemas de usabilidade emergentes da implementação de políticas de segurança se farão sentir com impactos significativos junto destes utilizadores.

Acresce ainda que o facto de ter aumentado o número de utilizadores não especializados tem contribuído para aumentar a dificuldade de estabelecimento de uma tipificação. A tipificação de utilizadores que emerge desta situação engloba dois tipos que se diferenciam apenas pelo grau de utilização do SI e consequente capacidade de aplicação das TIC. Todavia, esta opção pode revelar-se muito restritiva para avaliação da usabilidade resultante da implementação de políticas e normas de segurança, particularmente quando os aspectos associados à segurança e usabilidade dos SI se encontram condicionados às perspectivas pessoais dos diversos intervenientes e interessados na actividade organizacional.

Segundo Daly-Jones *et al* [1999], a qualidade de utilização de um sistema, incluindo a usabilidade e segurança, e a protecção dos utilizadores depende muito do contexto em que o sistema vai ser usado, procurando entender-se: as características dos potenciais utilizadores, as tarefas que esses utilizadores vão desempenhar e ainda o ambiente no qual o sistema vai ser utilizado.

Compete assim às Pessoas, à sua percepção sobre a informação e os sistemas que utilizam, a aplicação dos recursos disponibilizados às actividades pelas quais são responsáveis, considerando a segurança da informação e dos sistemas como um factor

fundamental a ter em conta na concretização eficiente e eficaz dessas mesmas actividades.

Todavia, a diversidade de actividades a desenvolver pelas Pessoas e a complexidade associada aos papéis que devem desempenhar no seu dia-a-dia, torna importante a especificação dos diferentes contextos em função desses mesmos papéis, particularmente quando a generalidade das situações apresentadas são comuns e exigem uma mesma caracterização.

Assim, no contexto deste trabalho, perante a diversidade de termos utilizados presentemente para designar os intervenientes nas actividades organizacionais, assume-se que os recursos humanos associados à utilização das TIC serão referenciados como **Pessoas**, por se entender ser um termo abrangente que inclui os actuais e potenciais utilizadores dos sistemas. Todavia, em situações muito específicas de utilização dos SI, o termo **utilizador** será aplicado indistintamente com o mesmo significado.

Perante a diversidade de possíveis contextos de utilização, considera-se que podem existir mais ‘papéis’ a desempenhar pelos recursos humanos. No entanto, a responsabilidade pela segurança da informação pertence em primeira instância a todos os envolvidos na sua utilização, independentemente do respectivo grau de envolvimento.

O envolvimento das Pessoas, particularmente nos contextos onde as actividades que desempenham são essenciais para as organizações, assume aspectos distintos quando implica a utilização das TIC, exigindo novas e maiores competências e um crescimento desse seu envolvimento, o que nem sempre é assumido de forma clara, quer pelas Pessoas, quer pelos decisores organizacionais.

Constata-se assim que as relações entre as Pessoas e as tecnologias sempre se revelaram difíceis, forçando as Pessoas a uma maior envolvimento nas actividades organizacionais e à necessidade de adquirirem novas competências, verificando-se que estas situações contribuem para as dificuldades de relacionamento na utilização das tecnologias, em particular quando essas tecnologias são encaradas como uma ameaça à estabilidade dos empregos. Todavia, porque a evolução apenas foi possível pelo domínio e utilização das tecnologias, essencialmente com a sua adequação às necessidades humanas, torna-se possível assumir a existência de um paradoxo.

Este paradoxo é tanto mais real quanto maiores são as dificuldades sentidas pelas Pessoas na utilização dessas tecnologias e quanto maior for a necessidade de as utilizar para suportar a evolução das sociedades humanas. As capacidades humanas na utilização das novas TIC são, para Soete [2000], “um activo complementar essencial”, constituindo “dois aspectos (Pessoas e TIC) inseparáveis da acumulação do conhecimento” e como tal indissociáveis de todo o processo de desenvolvimento organizacional.

5.4. As Pessoas e a Segurança da Informação

Se a segurança da informação constituiu uma preocupação pessoal e social, o actual contexto de globalização reforçou esta preocupação, forçando que todos os aspectos respeitantes à garantia da sua confidencialidade, integridade e disponibilidade passassem a fazer parte das atenções dos decisores organizacionais. No entanto, torna-se crucial que as Pessoas sejam amplamente envolvidas em todos os aspectos associados à segurança da informação, assumindo-se como parte activa e responsável pela sua utilização adequada e nos termos definidos pela organização.

Nesta mesma envolvente, Mamede [2006] considera que “a tomada de consciência por parte dos responsáveis da organização relativamente ao processo de segurança constitui a pré-condição essencial para a concretização do mesmo”, considerando que estas actividades não devem ser executadas apenas por um pequeno grupo da organização, passando sim pelo envolvimento de todas as Pessoas, indo do topo para a base. O autor refere ainda que este envolvimento da estrutura organizacional pode fazer a “diferença entre o sucesso e o insucesso de todo o processo”.

Perante este contexto turbulento e contingencial, as Pessoas deverão ser encaradas como um importante activo organizacional, sendo essencial proporcionar-lhes condições de desenvolvimento e motivação para que desenvolvam o seu potencial ao serviço das organizações onde se inserem, procurando garantir simultaneamente que a utilização dos SI e das TIC contribuem para melhorar perceptivelmente o seu desempenho.

Um sistema que não tenha sido desenhado correctamente pode conduzir a uma alta incidência de erros dos utilizadores, elevados custos de formação ou curvas de aprendizagem alargadas, baixos desempenhos e frustração, e suporta-se sobre controlos

restritivos ou medidas de segurança. Situação esta que leva a que, a partir do momento em que os utilizadores detectam estes problemas, existam tentativas frequentes para circundar controlos e outras funcionalidades que consideram desnecessariamente restritivas ou abandonar em conjunto a utilização do sistema [Henry 2003].

Estas situações podem vir a ser agravadas, particularmente quando se considera que as políticas de segurança desafiam os utilizadores a mudar a forma como pensam acerca da sua própria responsabilidade para a protecção da informação da organização, onde a tentativa de imposição que quaisquer políticas a Pessoas não dispostas a isso resulta em resistências porque procedimentos de segurança mais rígidos tornam o trabalho mais difícil e porque as Pessoas não gostam que lhes digam o que fazer, em particular quando isso é feito por quem está fora da cadeia de comando [Kabay 2002].

Verifica-se no entanto que muitas das violações à segurança da informação são concretizadas por pessoal de confiança que efectua actividades não autorizadas ou mesmo actividades que extravasam as suas autorizações [King *et al* 2001].

Este facto reforça a necessidade de ter uma atenção especial para com os aspectos relativos às atitudes das Pessoas, considerando simultaneamente a obrigatoriedade de colocar cláusulas adequadas ao estabelecimento de regras de confidencialidade e privacidade, quando se concretiza a respectiva contratação.

Pelo que, quando se procura enquadrar a problemática da segurança da informação, não deve ser esquecido um aspecto fundamental que se encontra relacionado com a identificação das ameaças, reais e potenciais, que existem relativamente a essa segurança, possibilitando assim uma adequação das medidas a tomar para evitar a concretização dessas ameaças, particularmente quando se verifica que as Pessoas por si só e a sua capacidade de utilização das tecnologias correspondem ao maior número de ameaças possíveis à segurança da informação, verificando-se que o maior número dessas perdas, segundo King *et al* [2001], corresponde a acções não intencionais, ocorridas durante as operações organizacionais.

Neste contexto, Whitman and Mattord [2005] consideram que embora as Pessoas sejam muitas vezes desdenhadas em termos de segurança dos computadores, estas poderão constituir sempre uma ameaça para a segurança da informação.

Esta constatação contribui para relevar a necessidade de, por um lado proporcionar acções de sensibilização e formação acerca da segurança, e pelo outro assegurar um maior envolvimento das Pessoas nas actividades relacionadas com a segurança, procurando que esta seja percebida pelas Pessoas como uma vantagem para o seu próprio desempenho.

Em qualquer programa de segurança da informação organizacional, as Pessoas serão sempre entendidas como o elo mais fraco a não ser que as políticas, a formação, as competências e as tecnologias sejam devidamente utilizadas para evitar que as Pessoas, acidental ou intencionalmente, danifiquem ou percam informação [Whitman and Mattord 2005].

De acordo com Veiga [2002], em termos de SI, os problemas de segurança podem localizar-se nos mais diversos níveis organizacionais (redes, sistemas informáticos, instalações, Pessoas – utilizadores e/ou técnicos, modo como é encarada a segurança), onde é crucial atender ao facto de as falhas ocorrerem habitualmente no elo mais fraco, considerando-se por isso todas as dimensões do problema.

Genericamente registam-se duas situações distintas em termos de SI, que se relacionam com o modo como o SI foi desenvolvido e implementado, afectando a forma como os utilizadores entendem a sua pertinência para as suas actividades e para o desempenho da organização.

Uma dessas situações ocorre quando o SI foi desenvolvido e implementado com o envolvimento e suporte dos utilizadores, que participaram na especificação dos requisitos (independentemente de ter sido um novo sistema ou alterado o sistema existente). Outra situação surge quando o SI foi desenvolvido e implementado sem recurso à participação dos utilizadores.

Enquanto que na primeira situação existe uma maior receptividade à implementação de políticas e normas de segurança, onde os problemas de usabilidade se façam sentir previsivelmente com menor acuidade, na segunda situação afigura-se bastante mais problemática, exigindo usualmente um maior cuidado na definição e implementação de políticas e normas de segurança.

5.5. Usabilidade dos Sistemas de Informação

Neste contexto onde a confiança na informação é essencial e a sua perda ou destruição pode afectar as actividades de negócio, é necessário dispor de SI e TIC fáceis de usar e cuja aprendizagem não envolva grandes recursos, com esta necessidade a ser reforçada pelos autores que sugerem a exigência do desenvolvimento de SI mais ‘utilizáveis’ para ambientes onde não existiam apenas e só especialistas mas utilizadores sem grandes níveis de conhecimentos técnicos [Bias and Mayhew 1994].

Referir SI amigáveis, no sentido da facilidade de utilização, corresponde a um termo (*user-friendly*) surgido no início dos anos 80 e que, face às conotações vagas e subjectivas que vinha a adquirir, encontra substituto no termo ‘usabilidade’, já então entendido como um dos seus sinónimos [Bevan *et al* 1991].

Deverá notar-se que uma parte considerável dos problemas nesta área deriva das diferentes perspectivas em confronto, essencialmente entre quem implementa os sistemas (técnicos, genericamente com conhecimentos suficientes para ultrapassar as potenciais dificuldades) e quem os utiliza (utilizadores, maioritariamente não detentores do conjunto de competências para uma adequada utilização do sistema).

A definição de usabilidade de um produto é proporcionada pela norma ISO 9241 (parte 11), como a extensão até onde um produto pode ser usado por utilizadores especificados para atingir objectivos especificados com eficácia, eficiência e satisfação num contexto de uso especificado.

Esta definição pode ser expandida para os SI, na sua essência um produto como qualquer outro, só que intangível, onde o problema da sua usabilidade após a definição de políticas de segurança, se inicia na formação dos utilizadores para a segurança. Genericamente registam-se duas situações distintas em termos de SI, que se relacionam com o modo como o SI foi desenvolvido e implementado, considerando-se por conseguinte que implementar políticas e sistemas de segurança envolve recursos financeiros e humanos, mas comporta essencialmente mudanças nas estruturas organizacionais, mudanças estas que usualmente não são cabalmente entendidas no interior das organizações.

Torna-se então possível constatar que a usabilidade compreende diversas componentes que por vezes estão em conflito, onde frequentemente nem todos os aspectos da usabilidade tem igual peso num dado projecto de desenho de SI [Nielsen 1993], referindo-se neste contexto a obrigação de atender às necessidades dos utilizadores finais do SI.

Neste sentido, os benefícios de uma aproximação centrada nos utilizadores incluem aumentos de produtividade, melhoria da qualidade do trabalho, redução dos custos de suporte e treino, e melhorias na saúde e protecção dos utilizadores [Daly-Jones *et al* 1999].

Nielsen [2000] refere a propósito que a usabilidade assumiu uma importância maior na economia baseada na Internet do que tinha assumido no passado, reforçando assim a necessidade de ter uma maior atenção para com as actividades onde a usabilidade dos SI é crucial para o desempenho organizacional.

Esta situação é tanto mais importante quanto a importância dos SI e da informação para as organizações, verificando-se que esta tem aumentado continuamente, forçando um contexto onde a confiança na informação é essencial e a sua perda, modificação ou destruição pode afectar seriamente a actividade da organização, condicionando o seu desempenho.

A motivação e apetência para adquirir ou melhorar competências em termos de SI e das TIC, encontrar-se-á relacionada com questões culturais, das Pessoas e das organizações, e com as expectativas que cada um dos intervenientes possui sobre a necessidade ou pertinência, quer de introduzir os SI e as TIC nas organizações, quer de adquirir as competências necessárias à sua adequada utilização.

A utilização das informações fornecidas pelos potenciais utilizadores de um sistema em desenvolvimento para suportar essas actividades pode servir para chegar a um sistema que corresponda às expectativas desses utilizadores, contribuindo assim para a optimização das actividades necessárias, e para uma melhor aceitação desse sistema por parte dos utilizadores.

Considerando que o coração de qualquer sistema de segurança são as Pessoas, aumentar o quadro de confiança, incluindo a segurança da informação e da rede, autenticação, protecção da privacidade e do consumidor, constitui um pré-requisito para o

desenvolvimento da Sociedade da Informação [Bishop 2002], e para a construção da confiança entre as Pessoas que utilizam as TIC [WSIS 2003a]. Como tal, torna-se imprescindível que as preocupações associadas à segurança da informação e do SI que a suporta sejam integrados na estratégia da organização.

Neste contexto, deve atender-se ao facto de a qualidade de utilização do SI envolver não só as Pessoas mas também as TIC e a própria organização. Segundo Daly-Jones *et al* [1999], a qualidade de utilização de um SI, incluindo usabilidade e segurança, e ainda a protecção dos utilizadores, depende muito do contexto em que o sistema vai ser usado, pelo que é necessário entender entre outros aspectos: as características dos potenciais utilizadores, as tarefas que esses utilizadores vão desempenhar e o ambiente no qual o sistema vai ser utilizado.

A segurança da informação, e dos SI e das TIC que a suportam, e a usabilidade desses mesmos SI são habitualmente aspectos antagónicos e cuja relevância tem sido negligenciada ao longo dos tempos, embora nos últimos anos, por força da difusão e utilização das TIC, exista uma maior atenção para a necessidade de garantir a privacidade da informação e que, simultaneamente, a mesma é fácil de utilizar.

Note-se a propósito que a segurança da informação e dos SI, conjuntamente com a usabilidade dos SI, têm sido factores habitualmente menosprezados nos processos relacionados com os SI, em particular quando os custos de desenvolvimento e implementação de SI constituem os principais condicionantes a impor.

Estas opções tem conduzido a que apenas se invista no que é entendido como fulcral, excluindo frequentemente os factores capazes de tornar os SI mais utilizáveis, com estas actividades a serem genericamente feitas por aproximações centradas nos utilizadores, assim como a generalidade dos factores necessários para garantir a segurança da informação.

De acordo com Henry [2003], um sistema que não tenha sido desenhado correctamente pode conduzir a uma alta incidência de erros dos utilizadores, elevados custos de formação ou curvas de aprendizagem alargadas, baixos desempenhos e frustração, e suporta-se sobre controlos restritivos ou medidas de segurança.

A situação relatada leva a que possam existir tentativas frequentes para circundar ou ultrapassar controlos e outras funcionalidades que consideram desnecessariamente

restritivas, ou até mesmo abandonar em conjunto a utilização do sistema, a partir do momento em que estes problemas são detectados pelos utilizadores.

Constata-se assim que, para suportar o desenvolvimento das actividades humanas sobre a informação, os SI devem ser desenhados de modo a tolerar as características individuais de cada um, no sentido de ajudar as Pessoas a vencer as suas limitações de processamento e ainda a complementar e mesmo ultrapassar as suas capacidades naturais [Martin *et al* 2002].

Por outro lado, porque a informação que os SI detêm é actualmente um activo mais significativo do que as TIC, que podem ser facilmente substituídas, torna-se necessário que a atenção da gestão (da informação e/ou do SI) se centre na protecção da informação organizacional.

Esta maior atenção que é necessária sobre a informação baseia-se essencialmente em dois vectores fundamentais:

- (1) A necessidade de assegurar a correcção dos dados detidos pela organização;
- (2) A necessidade de protecção contra perdas e danos da informação da organização ou das TIC que a suportam;

Registe-se todavia que uma quebra de segurança pode ser entendida como a ocorrência de qualquer acto, deliberado ou não, que conduz a acessos não autorizados, a perdas, a alterações ou a danos na informação detida por um SI.

Se a forma habitual de pensar um SI se baseia nas funções que este desempenha ou deve desempenhar, constata-se facilmente que esta visão é contrária a dos utilizadores (actuais e potenciais), visão esta que atende essencialmente ao como os SI são ou podem ser utilizados.

A confluência destas duas visões pode ser encontrada nas interacções entre as Pessoas e os SI e as TIC que os suportam, verificando-se que a usabilidade de um sistema se encontra directamente relacionada com as interacções proporcionadas, nomeadamente no respeitante à facilidade de uso, velocidade de realização das tarefas e mesmo à margem de erro dos utilizadores.

O estudo destas interacções compreende o estudo das Pessoas, das tecnologias e das suas influências mútuas, onde entender as tarefas a desempenhar com a utilização das

tecnologias, em particular quando testar a usabilidade de um sistema pode requer a observação da interacção dos utilizadores com esse mesmo sistema.

Para o desenvolvimento de produtos utilizáveis é necessário conhecer, entender e trabalhar com Pessoas que possam ser consideradas representativas dos actuais ou potenciais utilizadores de um determinado produto [Dumas and Redish 1999], situação esta que é tanto mais relevante quando o produto em causa são os SI e as TIC que suportam os fluxos de informação através da organização.

Mais segurança implica mais tecnologia, que por isso implica mais formação, provocando por sua vez mais dificuldades e por conseguinte mais problemas, logo, maior dificuldade na utilização dos SI e da informação que suportam, factos pelos quais é desejável que os utilizadores sejam envolvidos nos processos que originem mudanças nos SI e nas TIC que utilizam ou que se espera que venham a utilizar.

5.6. Impactos da Segurança na Usabilidade

A segurança é actualmente um dos mais relevantes aspectos desde que os SI se tornaram globais, mais dependentes de redes e consequentemente mais acessíveis por parte das Pessoas, possibilitando assim a inclusão das Pessoas que a ele procuram aceder com más intenções [Edwards *et al* 1995].

A usabilidade de um produto, e consequentemente do SI organizacional, depende da sua facilidade de utilização e aprendizagem num contexto especificado no qual é crucial entender o papel das Pessoas na sua utilização, particularmente quando essa utilização pode ser condicionada pela imposição de regras e restrições tendentes a assegurar a privacidade da informação que o SI suporta.

Neste contexto, pode-se constatar que a actividade das Pessoas fica condicionada pela usabilidade desses sistemas, onde é importante a qualidade da interacção entre as Pessoas que usam o SI para desempenhar as suas actividades actuais e o próprio SI, onde os principais pontos desta interactividade são a eficácia (como vão os utilizadores cumprir os objectivos estabelecidos utilizando o SI), a eficiência (os recursos consumidos para atingirem os seus objectivos) e a satisfação (o sentimento dos utilizadores acerca da sua utilização do SI), na utilização do referido sistema.

Considerando satisfação do utilizador como um “conceito pluridisciplinar, que incorpora várias vertentes: psicológica, organizacional, financeira, etc.”, Serrano e Caldeira [2001] assumem-no como muito importante pois permite avaliar o sucesso de um projecto informático comparativamente com a aceitação e com o nível de satisfação dos utilizadores.

Poderá colocar-se a questão de saber até que ponto uma política de segurança contribui para a diminuição dos custos ou mesmo para o aumento da usabilidade do SI. Considera-se assim que é também indispensável identificar até que ponto a aprovação dos utilizadores condiciona a utilização e a usabilidade do SI. Situações estas que dependerão certamente do grau de envolvimento e cooperação dos utilizadores e da própria cultura organizacional.

Neste sentido, de acordo com Serrano e Caldeira [2001], quando se procura identificar o nível de satisfação dos utilizadores dos SI, deve considerar-se também “que devido às suas diferenças de personalidade e de papel na organização, estes poderão ter interesses e perspectivas significativamente diferentes”.

Parece assim ser relevante garantir que as políticas de segurança a ser implementadas, sejam objecto de um planeamento adequado a permitir que o seu impacto nessas organizações e nas Pessoas que as constituem seja mínimo e fácil de absorver, respondendo deste modo às necessidades das organizações.

Refira-se aliás que uma segurança demasiado formal, que exija por exemplo identificações excessivas, particularmente em sistemas onde a rapidez de funcionamento é uma característica fundamental, pode, segundo Carneiro [2002], ser outro dos factores capazes de levar os utilizadores a ultrapassar os mecanismos implementados.

Neste contexto, torna-se essencial conhecer a percepção que os utilizadores possuem acerca da segurança e que hábitos ou políticas de segurança aplicam nas suas actividades diárias, perspectivando a criação de condições que potenciem o seu envolvimento na definição e implementação das referidas políticas.

Verifica-se assim que a necessidade de proceder sequencial ou continuamente a validações de utilizador para aceder a aplicações específicas, a obrigatoriedade de alterar periodicamente as *passwords*, que implicam frequentemente a construção de códigos difíceis de memorizar, ou ainda o facto de se forçar a deslocação dos

utilizadores a determinados locais para aceder a recursos que são essenciais para a sua normal actividade, são todos eles aspectos que podem contribuir para condicionar o seu próprio desempenho, afectando consequentemente a usabilidade dos SI.

Outras soluções potencialmente facilitadoras dos acessos aos SI, como seja a utilização de sistemas de segurança que respondem à validação biométrica levanta, além de questões éticas, alguns problemas operacionais. Uma das situações mais simples coloca-se, perante a validação pela íris, particularmente quando qualquer utilizador está doente, ou quando, pela validação digital, o dedo respectivo foi objecto de um corte.

Neste âmbito verifica-se que a usabilidade de um sistema pode ser claramente afectada pela validação dos utilizadores recorrendo a este tipo de tecnologia, em especial se não existir uma percepção clara das vantagens que estas tecnologias podem comportar para a organização, relevando a necessidade de existirem mecanismos complementares de controlo de acessos.

As questões associadas à segurança e usabilidade dos SI podem então ser colocadas de diferentes perspectivas, de entre as quais se destacam:

- Quais os custos associados à implementação de um plano de segurança?
- Qual a usabilidade do plano de segurança e do sistema de suporte perante a ocorrência de um desastre?
- Qual o tempo de sistema que implica a efectiva utilização de todos os processos de segurança que estão definidos num plano?
- Que atrasos de sistema implica a segurança lógica da informação (*software*, acessos, protecção de dados)?

Pode pois concluir-se que dispor de SI com elevados níveis de segurança e de usabilidade constitui um factor de sucesso organizacional essencial para garantir que o SI a desenvolver ou a reformular considera as políticas de segurança da informação organizacional, cumprindo simultaneamente os requisitos de usabilidade das Pessoas em geral e da organização em particular.

5.7. Conclusões

As Pessoas, pelas suas capacidades, conhecimentos e competências surgem então como um dos mais importantes activos organizacionais, dependendo do seu adequado desempenho a aquisição de vantagens competitivas por parte das organizações.

Por outro lado, torna-se pertinente assegurar que as Pessoas que utilizam a informação de negócio possuem as competências necessárias para suportar as actividades de negócio, utilizando adequadamente os SI e as TIC de que dispõem em prol dos objectivos organizacionais.

Os desafios actuais em termos da utilização dos SI e das TIC levantam frequentemente receios e oposição das Pessoas às mudanças com que as organizações se confrontam. Este facto, embora cada vez mais os SI sejam concebidos e desenvolvidos para uma utilização mais abrangente, pressupõe desde logo a necessidade de identificar os diversos tipos de utilizadores ou mesmo do modo como os SI são utilizados.

Face ao exposto, é possível concluir que a segurança da informação e dos SI que a suportam, mais do que uma necessidade, é uma obrigatoriedade para as Pessoas e para as organizações onde elas se inserem.

Considera-se assim pertinente desenvolver acções de sensibilização sobre a importância da segurança da informação, que numa primeira fase considerem simultaneamente os impactos que podem existir na imagem interna e externa da organização.

Entende-se também que este tipo de actividade deve envolver todos os actuais ou potenciais utilizadores do SI e das TIC, procurando um claro comprometimento e envolvimento de todos os membros da organização para com as necessidades identificadas em termos de segurança da informação e dos SI que a suportam.

Conclui-se deste modo que proporcionar às Pessoas formação adequada às actividades a desempenhar e sensibilizá-las para a missão, estratégia e objectivos da organização se torna uma obrigação para os decisores organizacionais.

Referências bibliográficas

Anunciação, P. e Zorrinho, C., *Urbanismo Organizacional – Como gerir o choque tecnológico nas empresas*, Edições Sílabo, 2006.

- Barman, S., *Writing Information Security Policies*, New Riders Publishing, 2002.
- Bevan, N., Kirakowski, J. and Maissel, J., “What is usability?”, Proceedings of the 4th International Conference on HCI, September 1991.
- Bias, R.G. and Mayhew, D.J., *Cost-Justifying Usability*, Morgan Kaufmann Publishers, 1994.
- Bishop, M., *Computer Security: Art and Science*, Adisson-Wesley Professional, 2002.
- Caldeira, M. e Romão, M., “Porque falham os sistemas e tecnologias de informação nas PMEs Portuguesas”, Actas (formato digital) da 3ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.
- Carneiro, A., *Introdução à Segurança dos Sistemas de Informação*, FCA, 2002.
- Castells, M., *A Galáxia Internet: Reflexões sobre Internet, Negócios e Sociedade*, Fundação Calouste Gulbenkian, 2004.
- Ciborra, C. and Andreu, R., “Organizational Learning and Core Capabilities Development: The Role of IT”, in Robert D. Galliers and Walter R. J. Baets (Organization), *Information Technology and Organizational Transformation: Innovation for the 21st Century Organization*, London, John Wiley & Sons, 1998, p.87-106.
- Daly-Jones, O., Bevan, N. and Thomas, C., “Handbook of User-Centred Design – INUSE 6.2”, Version 1.2, Serco Usability Services – National Physical Laboratory, 12 February 1999, <http://www.ejeisa.com/nectar/inuse/6.2/index.htm> (15-11-2002).
- Dark, M.J., “Security Education, Training, and Awareness from a Human Performance Technology Point of View”, in Michael E. Whitman and Herbert J. Mattord (Editors), *Readings and Cases in The Management Information Security*, Thomson Course Technology, 2006, p.86-104.
- Davis, F.D., “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology”, *MIS Quarterly*, September 1989, p.319-339.
- Dinis, J.A., *Guerra de Informação – Perspectivas de Segurança e Competitividade*, Edições Sílabo, 2005.
- Drucker, P., “The Coming of the New Organization”, *Harvard Business Review*, Jan.-Feb. 1988, p.45-53.
- Dumas, J.S. and Redish, J.C., *A Practical Guide to Usability Testing*, Intellect, 1999.

- Edwards, C., Ward, J. and Bytheway, A., *The Essence of Information Systems*, 2nd Edition, Prentice Hall, 1995.
- Falkenberg, E., Hesse, W., Lindgreen, P., Nilssen B., Oei, J., Rolland, C., Stamper, R., Van Assche, F., Verrijn-Stuart, A. and Voss, K., *FRISCO: A Framework of Information Systems Concepts*, IFIP WG 8.1 Task Group FRISCO, 1998.
- Ferreira, J.M.C., Neves, J. e Caetano, A., *Manual de Psicossociologia das Organizações*, McGrawHill, 2001.
- Garcia, C., “A Notável Intangibilidade das Organizações: O Capital Intelectual e os Sistemas de Informação”, in Luís Amaral, Rodrigo Magalhães, Carlos Campos Morais, António Serrano e Carlos Zorrinho (Editores), *Sistemas de Informação Organizacionais*, Edições Sílabo, 2005, p.199-222.
- Hansche, S.D., “Making Security Awareness Happen”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 3, 4th Edition, Auerbach Publications, 2002, p.317-335.
- Henry, K., “The Human Side of Information Security”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 4, 4th Edition, Auerbach Publications, 2003, p.239-261.
- Kabay, M.E., “Developing Security Policies”, in S. Bosworth and M.E. Kabay, (Editors), *Computer Security Handbook*, 4th Edition, John Wiley & Sons, 2002.
- King, C.M., Dalton, C.E. and Osmanoglu, T.E., *Security Architecture: Design, Deployment & Operations*, Osborne/McGraw-Hill, 2001.
- Kovács, I., “Trabalho, Qualificações e Aprendizagem ao longo da vida: Ilusões e problemas da sociedade de informação”, in VII Encontro Nacional da APSIOT, *Formação, Trabalho e Tecnologia: Para uma Nova Cultura Organizacional*, Celta Editora, 1998, p.69-84.
- Lindley, R.M., “Economias Baseadas no Conhecimento”, in Maria João Rodrigues (Coordenadora), *Para Uma Europa da Inovação e do Conhecimento*, Celta Editora, 2000, p.33-78.
- Mamede, H.S., *Segurança Informática nas Organizações*, FCA, 2006.
- Martin, E.W., Brown, C.V., DeHayes, D.W., Hoffer, J.A. and Perkins, W.C., *Managing Information Technology*, 4th Edition, Prentice Hall, 2002.
- Maslow, A., *Motivation and Personality*, Harper and Row, 1954.

- Misiolek, N., Zakaria, N. and Zhang, P., “Trust in Organizational Acceptance of Information Technology: A Conceptual Model and Preliminary Evidence”, Proceedings of the Decision Sciences Institute 33rd Annual Meeting, November 2002.
- Neves, J., “Personalidade, Percepção e Aprendizagem”, in J.M. Carvalho Ferreira, José Neves e António Caetano (Editores), *Manual de Psicossociologia das Organizações*, McGrawHill, 2001.
- Nielsen, J., *Usability Engineering*, Morgan Kaufmann – Academic Press, 1993.
- Nielsen, J., *Designing Web Usability*. New Riders Publishing, Indianapolis, USA, 2000.
- Pinto, M.P., Lopes, F.C. e Moraes, M.P., “Integração da Medição do Capital nos Sistemas de Gestão do Conhecimento: Uma Proposta de Modelo”, Actas (formato digital) da 6^a Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade do Minho e pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança, Bragança, 26-28 de Outubro de 2005.
- Reponen, T., “The Role of Learning in Information Systems Planning and Implementation”, in R.D. Galliers and R.J. Baets (Editors), *Information Technology and Organizational Transformation: Innovation for the 21st Century Organization*, John Wiley & Sons, 1998, p.133-149.
- Santana, S. e Dias, A., “Condicionantes da introdução de TIC em instituições prestadoras de cuidados”, Actas (formato digital) da 6^a Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade do Minho e pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança, Bragança, 26-28 de Outubro de 2005.
- Serra, H., “Tecnologias da Informação, Emprego e Organização do Trabalho: A Sociedade da Informação como problemática teórica”, in VII Encontro Nacional da APSIOT, *Formação, Trabalho e Tecnologia: Para uma Nova Cultura Organizacional*, Celta Editora, 1998, p.39-50.
- Serrano, A. e Caldeira, M., “Gestão de Investimentos em Sistemas e Tecnologias de Informação – uma revisão crítica”, *Revista da Associação Portuguesa de Sistemas de Informação*, 15, 2001, p.99-107.
- Silberschatz, A., Galvin, P. and Gagne, G., *Operating Systems Concepts*, 6th edition, John Wiley & Sons, 2003.

- Smith, C. and Dinn, A., “User Centered Design: The Key to a ‘User-Friendly’ Information Society”, *European Journal of Engineering for Information Society Applications*, 2 (1) September, 1999.
- Soete, L., “A Economia Baseada no Conhecimento num Mundo Globalizado: Desafios e Potencial”, in Maria João Rodrigues (Coordenadora), *Para Uma Europa da Inovação e do Conhecimento*, Celta Editora, 2000, p.3-31.
- Tudor, J.K., *Information Security Architecture: An Integrated Approach to Security in the Organization*, Auerbach Publications, 2001.
- Ulrich, D., “Intellectual Capital = Competence x Commitment”, *Sloan Management Review*, Winter, 1998, p.15-26.
- Veiga, P., “Prefácio”, in Alberto Carneiro, *Introdução à Segurança dos Sistemas de Informação*, FCA, 2002.
- Whitman, M.E. and Mattord, H.J., *Principles of Information Security*, 2nd Edition, Thomson Course Technology, 2005.
- Whitten, A. and Tygar, J.D., “Usability of Security: A Case Study”, 18 December 1998.
- World Summit on the Information Society, “Declaration of Principles”, WSIS-03/Geneva/Doc/4-e, 12 December, 2003.
- Zorrinho, C., *Gestão da Informação*, Editorial Presença, 1991.
- Zorrinho, C., “O Mundo Virtual”, *Cadernos de Gestão de Sistemas e Tecnologias da Informação Henrique Marcelino*, Instituto de Informática, 1999, p.27-35.

6

Métricas de Segurança

Genericamente, qualquer projecto de SI necessita da definição do conjunto de características directamente relacionadas com o sistema, nomeadamente o que é o sistema, quais as funções a desempenhar, quem o vai utilizar e onde, como vai ser instalado e mantido, entre muitas e diversas questões possíveis [Maguire 1998].

Este facto pode contribuir para proporcionar um enquadramento das questões a colocar, ao permitir a percepção do que pretendia ser o sistema que está em uso após a implementação do sistema de segurança.

Torna-se assim possível constatar que, quando se procura identificar o conjunto de parâmetros que permitam medir a segurança e a usabilidade de um sistema, se torna importante identificar e compreender o contexto em que o sistema foi desenvolvido e implementado, considerando como factor fundamental o grau de envolvimento dos utilizadores finais.

Neste sentido, torna-se também relevante perceber o negócio, procurando-se um entendimento de que quais são os objectivos que o SI deve atingir em consonância com a missão e a estratégia organizacional, de modo a que o âmbito dos parâmetros a analisar englobe todo o sistema.

6.1. Conceito de Métrica

As preocupações inerentes à segurança da informação, as políticas de segurança implementadas e os impactos de ambos os aspectos na actividade organizacional impõem a pertinência de se proceder à avaliação da segurança na organização e na respectiva envolvente.

Considera-se então que, neste contexto, se torna importante definir pontos de referência (parâmetros) que permitam proceder à avaliação de todos os aspectos associados à

utilização da política de segurança adoptada pela organização, considerando expressamente os objectivos estabelecidos para organização.

Os impactos da segurança nas actividades das Pessoas e das organizações devem ser considerados em moldes adequados que permitam assegurar que as actividades associadas ao planeamento, à implementação e ao teste da segurança, são abrangidas por um conjunto de métricas que possibilitem a sua posterior avaliação.

Por conseguinte, a maior ou menor subjectividade do que se pretende medir surge frequentemente como um problema ou obstáculo a ultrapassar, genericamente por dizer respeito à necessidade de existência de processos definidos (repetíveis e verificáveis) para efectivação da medição necessária.

Constata-se então que a avaliação das políticas de segurança implementadas torna necessária a realização de medições acerca das suas diversas vertentes, que dependem integralmente do ou dos *standards* que são utilizados para suportar essas políticas, assim como das opções assumidas em termos dos objectivos de segurança que são estabelecidos para a organização.

Torna-se também obrigatória a definição concreta e objectiva do que se vai medir, quando e como se vai medir, com base em que referências vai ser concretizado. Esta situação pode ser solucionada pelo recurso a padrões definidos com esse objectivo, entre os quais se encontram as métricas de segurança, que surgem como o instrumento base para essas actividades.

Assumindo então as métricas de segurança como uma das opções adequadas para aferir a segurança na organização, torna-se essencial especificar o que se entende por métrica, referindo-se que a alusão a métricas não se encontra relacionada com o sistema métrico mas sim com o conjunto de medições efectuadas por comparação com um padrão.

O termo ‘métrica’ descreve uma categoria alargada de ferramentas utilizadas pelos decisores para avaliação de dados de diversas áreas da organização. Na sua forma mais simples uma métrica é uma medição que é comparada com uma escala ou ponto de referência para produzir resultados expressivos [Stoddard *et al* 2005].

Já Swanson *et al* [2003] entendem métricas como ferramentas desenhadas para facilitar a tomada de decisão e melhorar o desempenho e responsabilidade através da recolha,

análise e reporte dos dados relevantes relacionados com desempenho, mencionando ainda que as métricas de segurança devem ser baseadas nas metas e objectivos de desempenho da segurança dos SI e das TIC que estabelecem os resultados desejados para o programa de implementação da segurança.

Por outro lado, segundo Payne [2006], outro entendimento acerca do que é uma métrica pode ser feito pela especificação da distinção entre métricas (derivadas da comparação de duas ou mais medições tomadas ao longo do tempo com uma base de referência pré determinada) e medições (que proporcionam pontos de vista temporais de factores discretos e específicos). A mesma autora refere ainda que as medições são geradas por contagem e as métricas são geradas por análise, ou seja, as medições são dados objectivos em bruto e as métricas são interpretações humanas, objectivas e subjectivas, desses mesmos dados.

O *IEEE Standard Glossary of Software Engineering Terminology* [IEEE 1990] define métrica como a medida quantitativa do grau que um sistema, processo ou componente possui relativamente a um dado atributo, enquanto que medição corresponde à avaliação de um processo ou um produto por comparação com um *standard*.

Outra definição, obtida através do *Oxford Business English Dictionary* [OxfDic 2005], especifica métrica como um sistema para medir algo, especialmente o desempenho de um negócio, definindo medição como o acto ou processo de encontrar o tamanho, quantidade ou grau de algo.

Métricas são ferramentas destinadas a melhorar o desempenho e a responsabilidade, recolhendo, analisando e reportando dados relacionados com o desempenho, com o cumprimento de metas e dos objectivos a serem acompanhados pelas métricas de segurança da informação, quer através da quantificação dos níveis de implementação dos controlos de segurança, quer da eficácia e eficiência desses mesmos controlos, analisando a adequação das actividades de segurança e procurando identificar possíveis acções de melhoria [Bowen *et al* 2006].

6.2. Tipificação de Medições e Métricas de Segurança

Quando se pretende proceder à definição de métricas, torna-se importante considerar as possíveis alternativas que permitam uma adequada definição dessas métricas, dedicando

uma atenção especial às métricas que se encontram directamente relacionadas com as Pessoas.

Os tipos de métricas que realisticamente podem ser obtidos e simultaneamente ser úteis para melhorar o desempenho da organização, dependem da maturidade do programa de segurança da própria organização e da implementação do controlo de segurança do sistema.

Considera-se assim que, embora diferentes tipos de métricas possam ser usados simultaneamente, o foco primário das métricas de segurança dos SI e das TIC muda com a maturidade da implementação dos controlos de segurança, procedendo-se por isso ao ajuste desses mesmos controlos sempre que tal se revele necessário.

Um modelo de métricas de segurança compreende três componentes [Henning 2001, Katzke 2001]:

- (1) O objecto a ser medido (produto, sistema, eficácia do programa de segurança, competência profissional organizacional e pessoal);
- (2) Os objectivos de segurança, ou seja, o padrão contra o qual o objecto está a ser medido;
- (3) O método de medição.

Segundo Swanson *et al* [2003], o processo de especificação de métricas assegura que as métricas são desenvolvidas com o propósito de identificar causas de fraco desempenho e, por conseguinte, aponta para as acções correctivas consideradas apropriadas à resolução do problema. Neste âmbito, as organizações podem desenvolver e recolher métricas de três tipos:

- (1) Implementação de métricas para avaliar a implementação de políticas de segurança;
- (2) Eficácia/eficiência das métricas para medir resultados das entregas dos serviços de segurança;
- (3) Métricas de impacto para medir o impacto de eventos de segurança no negócio ou na missão.

Neste contexto, para facilitar o entendimento e aceitação a todos os níveis do novo programa de métricas de segurança, Payne [2006] considera ser pertinente suportar o

programa em *frameworks* de melhoria dos processos que já sejam familiares na organização, referenciando no entanto que, na ausência de qualquer *framework* pré existente, pode ser usada uma aproximação *top-down* ou *bottom-up* para determinar que métricas podem ser desejáveis.

A aproximação *top-down* inicia-se com os objectivos do programa de segurança, funcionando para trás de modo a identificar métricas específicas que podem ajudar a determinar se aqueles objectivos são atingidos, e as últimas medidas necessárias para gerar aquelas métricas. Esta aproximação compreende:

- ⇒ Definir/Listar os objectivos de todo o programa de segurança;
- ⇒ Identificar métricas que possam indicar progressos para cada objectivo;
- ⇒ Determinar as medições necessárias para cada métrica.

A aproximação *bottom-up* vincula em primeiro lugar a definição de que processos de segurança, produtos e serviços estão prontos para ser medidos ou já foram medidos, considerando-se então as métricas significativas que podem ser derivadas dessas medições e finalmente procede-se à valorização adequada dessas métricas relativamente aos objectivos de todo o programa de segurança. Esta aproximação compreende os seguintes aspectos:

- ⇒ Identificar medições que são ou podem ser recolhidas por este processo;
- ⇒ Determinar métricas que possam ser geradas por essas medições;
- ⇒ Determinar a associação entre as métricas derivadas e os objectivos estabelecidos para o programa de segurança.

A ser considerada a visão apresentada por Payne [2006], relativamente à utilização de *frameworks* de melhorias de processos, deve atender-se ao facto de a aproximação *top-down* permitir identificar mais rapidamente as métricas a utilizar, ao ter em atenção os objectivos do programa de segurança, enquanto que a aproximação *bottom-up* produz as métricas que são mais fáceis de obter.

Ambas as aproximações referenciadas assumem que os objectivos do programa de segurança já tinham sido estabelecidos. Se isto não tiver acontecido, a definição desses objectivos de alto nível é obviamente importante e constitui um pré requisito, pelo que é fundamental que se proceda à validação das métricas definidas e implementadas.

Se aquilo que se pretende é adequar as métricas à avaliação dos processos de segurança, onde o que está em causa é o entendimento da percepção das Pessoas e do seu empenho no desenvolvimento e implementação de políticas de segurança, então deve diligenciar-se a minimização de eventuais impactos negativos derivados do seu eventual desconhecimento dessas mesmas políticas.

Neste âmbito, o processo de aferir as políticas relacionadas com sensibilização e formação em segurança, deve ter o suporte de métricas adequadas à obtenção de resultados, com a maior fidelidade possível utilizando os conhecimentos adquiridos nestas acções e a sua aplicação nas actividades organizacionais, considerando inclusive os impactos na melhoria do desempenho organizacional.

Por outro lado, o facto de estar em causa a percepção das Pessoas acerca de um conjunto diversificado de aspectos relativos à segurança da informação, as métricas devem ser estabelecidas considerando a subjectividade intrínseca à apreciação dos fenómenos segundo este tipo de perspectiva.

Perante este contexto, deve também ser considerado o enquadramento ambiental onde a organização se insere e os recursos utilizados pelas Pessoas nas suas actividades, particularmente os recursos de informação, SI e TIC, considerando quer os aspectos associados à segurança e aos SGSI, quer a reacção às mudanças efectuadas e ao como aceitam as TIC e a respectiva segurança.

Deste modo, as métricas a adoptar, sejam qualitativas ou quantitativas, deverão ter em conta os contributos do caso de estudo e a sua aplicabilidade na resposta às questões de partida.

A generalidade das métricas apresentadas define como fundamental que os factores sobre os quais se vão efectuar as medições sejam de natureza quantitativa, o que levanta desde logo algumas questões, particularmente se for considerado que muitos dos aspectos de segurança da informação respeitantes a este trabalho estão relacionados com fenómenos de origem qualitativa, ou seja, aspectos que dependem em grande parte da percepção das Pessoas e do investigador acerca dos factos em observação.

6.3. Métricas

No actual contexto de actuação das organizações, Sociedade da Informação, globalização, novos mercados, clientes mais exigentes, maior competitividade, identificaram-se as Pessoas como um factor fundamental para o sucesso das organizações, particularmente quando estas detêm as capacidades e competências adequadas a permitir que as organizações adquiram vantagens competitivas que as diferenciem dos seus principais concorrentes.

Neste sentido, a informação, os SI e as TIC utilizadas pelas Pessoas nas suas actividades, necessitam de uma protecção adequada, relevando a importância da existência e utilização de políticas de segurança apropriadas aos objectivos e estratégias definidas pela organização.

Considerando então a especificidade do objecto de estudo, as Pessoas e a sua percepção acerca da segurança da informação e dos SI e TIC organizacionais, as métricas a especificar devem considerar essencialmente aspectos de natureza qualitativa, não estando todavia condicionadas a esses mesmos aspectos.

Esta focalização nas Pessoas necessita que as métricas a aplicar considerem a sua percepção acerca da segurança da informação e dos SI e TIC que suportam os seus fluxos, considerando factores como a sua satisfação, competências e envolvimento nas actividades relacionadas com a problemática da segurança.

6.3.1. Princípios Orientadores

Assumindo que o sucesso das métricas depende da sua aplicação directa na organização, emerge como necessária a sua integração no ciclo de gestão da organização. Existem então dois aspectos essenciais para a sua concretização: por um lado através da utilização dos dados já disponíveis nos SGSI e por outro lado por as métricas poderem suportar o processo de decisão e por conseguinte ser possível a sua utilização no SGSI [Weiß *et al* 2005].

Os objectivos de desempenho da segurança dos SI e das TIC permitem o cumprimento de metas pela identificação das práticas definidas pelas políticas de segurança e procedimentos consistentes com a implementação dos controlos de segurança na organização. As métricas de segurança monitorizam o cumprimento das metas e

objectivos pela quantificação do nível de implementação dos controlos de segurança e da sua eficácia e eficiência, analisando a adequação das actividades de segurança e identificando possíveis acções de melhoria [Swanson *et al* 2003].

Em termos genéricos, consideram-se os instrumentos de medida como de carácter quantitativo ou qualitativo, em função dos aspectos que se pretendem aferir e dos objectivos subjacentes à actividade a avaliar.

Perante a necessidade de medir a segurança, Weiß *et al* [2005] consideram que, após se proceder à identificação dos principais requisitos para a segurança de toda a organização e da descrição das métricas de segurança, devem ter-se em atenção três aspectos fundamentais:

- (1) Diagnóstico compreensivo de toda a organização (efectuar o diagnóstico de todos os aspectos de segurança da organização, desde os mais simples aos mais complexos);
- (2) Objectividade (o diagnóstico de segurança não deve reflectir apenas a opinião de uma única pessoa, devendo sim ser o resultado de uma audiência alargada);
- (3) Comparabilidade (medir e observar as melhorias de segurança podendo os resultados ser comparados com resultados de outras organizações, assumindo a possibilidade de estabelecer controlos adicionais).

Os métodos de medição, em termos de segurança incluem, segundo Katzke [2001]:

- ⇒ Teste directo (funcional, penetração);
- ⇒ Avaliação;
- ⇒ Diagnóstico (risco/vulnerabilidade);
- ⇒ Acreditação;
- ⇒ Treino/educação/nível de competência;
- ⇒ Observação do desempenho do sistema (detecção de intrusões).

Numa perspectiva complementar, Weiß *et al* [2005] referem que o acesso à segurança da informação na globalidade da organização é difícil, relacionando-se o principal problema com a falta de indicadores de base apropriados que permitam a expressão de segurança de toda a organização, assumindo que um bom ponto de partida para estes

indicadores de base parece residir no estabelecimento de um entendimento intuitivo da segurança.

Entende-se assim como relevante considerar como referencial três dos nove princípios estabelecidos pela OECD, *Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security* [OECD 2002]. Estes três princípios são:

(i) Sensibilização – todos os participantes devem estar cientes da necessidade da segurança dos SI e das redes, e do papel que podem desempenhar na sua melhoria; Este princípio focaliza-se na sensibilização para o risco e disponibilidade de salvaguardas como a primeira linha de defesa para a segurança dos SI e das redes, podendo estes ser afectados por riscos externos e/ou internos.

(ii) Responsabilidade – todos os participantes são responsáveis pela segurança dos SI e das redes;

Considerando a sua dependência da proximidade da interligação local e global dos SI e das redes, os participantes devem entender as suas responsabilidades para a segurança desses SI e redes, responsabilizando-se de forma adequada relativamente aos seus papéis individuais.

(iii) Resposta – os participantes devem agir atempadamente e cooperar entre si, no sentido de prever, detectar e responder a incidentes de segurança;

A inter conectividade dos SI e das redes, e o potencial para difusão rápida de danos, implica uma actuação atempada e cooperativa para endereçar os incidentes de segurança e partilhar informação acerca de ameaças e vulnerabilidades, como for apropriado, implementando ainda procedimentos para uma rápida e eficaz cooperação para prevenir, detectar e responder a incidentes de segurança.

Considera-se assim que a utilização de normativos adequados às necessidades organizacionais e capazes de responder aos princípios enunciados, permitirá a especificação de métricas de acordo com os requisitos identificados para cada caso concreto.

6.3.2. Normas de Referência

O normativo inicialmente analisado permitiu inferir que duas dessas normas procedem à abordagem da definição e especificação de métricas, considerando todavia uma visão

quase exclusivamente tecnológica, onde as Pessoas não constituem o seu principal foco de atenção.

Estas normas são a NIST SP800-55, *Security Metrics Guide for Information Technology Systems*, e a NIST SP800-80, *Guide for Developing Performance Metrics for Information Security*.

A NIST SP800-55 [Swanson *et al* 2003] baseia-se essencialmente nas técnicas e nos controlos de segurança especificados na NIST SP800-26 (*Security Self-Assessment Guide for Information Technology Systems*) [Swanson 2001], que enquadram as medidas de segurança em três tipos de controlos distintos: de Gestão, Técnicos e Operacionais.

- (1) Controlos de Gestão: (i) Gestão do Risco; (ii) Revisão dos Controlos de Segurança; (iii) Ciclo de Vida; (iv) Autorizar Processamento (Certificação e Acreditação); (v) Plano de Segurança do Sistema.
- (2) Controlos Operacionais: (vi) Segurança das Pessoas; (vii) Segurança Física; (viii) Controlos de Produção, Entradas/Saídas; (ix) Planeamento da Contingência; (x) Manutenção dos Sistemas de *Software* e *Hardware*; (xi) Integridade dos Dados; (xii) Documentação; (xiii) Sensibilização, Treino e Educação sobre Segurança; (xiv) Capacidade de Resposta a Incidentes.
- (3) Controlos Técnicos: (xv) Identificação e Autenticação; (xvi) Controlo dos Acessos Lógicos; (xvii) Seguimento das Auditorias.

Considerando a definição anterior, a NIST SP800-55 refere a existência de três tipos de métricas: de implementação (medir a implementação da política de segurança), de eficácia/eficiência (para medir os resultados da entrega de serviços de segurança) e de impacto (para medir o impactos dos eventos de segurança nos negócios ou na missão). Cada uma das métricas referenciadas pode ser utilizada isoladamente ou em conjunto com outras.

A NIST SP800-80 [Chew *et al* 2006] apresenta métricas candidatas (pelo menos uma) por cada uma das 17 famílias de controlos definidas na NIST SP800-53 [Ross *et al* 2005] com estas métricas a poderem ser reduzidas, expandidas ou ainda utilizadas como modelo para suportar o desenvolvimento de outras métricas. Este documento deve ser utilizado em conjunto com a NIST SP800-55.

As famílias de controlos referenciadas nesta norma são: (i) Controlo de Acessos; (ii) Sensibilização e Treino; (iii) Auditoria e Responsabilização; (iv) Certificação, Acreditação e Valorização da Segurança; (v) Gestão da Configuração; (vi) Planeamento da Contingência; (vii) Identificação e Autenticação; (viii) Resposta a Incidentes; (ix) Manutenção; (x) Protecção dos dispositivos de Dados; (xi) Protecção Ambiental e Física; (xii) Planeamento; (xiii) Segurança das Pessoas; (xiv) Valorização do Risco; (xv) Aquisição de Serviços e Sistemas; (xvi) Protecção das Comunicações e Sistemas; (xvii) Integridade da Informação e dos Sistemas.

Uma outra norma, a COBIT, *Control Objectives for Information and related Technology*, focalizando-se no controlo ao invés de se focalizar na execução, proporciona uma orientação de negócios, ligando as metas de negócio às metas de TI, proporcionando desse modo métricas e modelos de maturidade para medir a realização dessas métricas e simultaneamente identificar as responsabilidades associadas aos detentores de negócio dos processos de TI [COBIT 2005].

Mesmo não sendo uma norma, o *Federal Information Security Management Act of 2002* (FISMA), apresenta um conjunto de controlos que podem ser relevantes para a especificação de métricas.

Os controlos definidos no FISMA [2002] englobam: (i) Acreditação e Certificação; (ii) Integração dos Custos dos Controlos de Segurança no Ciclo de Vida dos Sistemas; (iii) Teste dos Controlos de Segurança do Sistema e dos Planos de Contingência; (iv) Sensibilização, Treino e Educação em Segurança; (v) Gestão da Configuração e das Políticas de Tratamento de Incidentes; (vi) Plano de Acção da Agência (Organização) e Processos Relevantes; (vii) Segurança dos Serviços Proporcionados pelos Fornecedores; (viii) Qualidade do Processo de Acreditação e Certificação; (ix) Desenvolvimento e Verificação do Inventário do Sistema.

Os contributos obtidos através dos controlos identificados através das normas anteriormente definidas, serão explicitados no capítulo 7 (Criação do Modelo), aplicando-se no processo de especificação do Modelo.

6.3.3. Especificação de Métricas

Uma alternativa para o estabelecimento de métricas de segurança é apresentada pela NIST SP 800-55 [Swanson *et al* 2003], que apresenta as seguintes características:

- ⇒ Descreve os papéis e responsabilidades do pessoal da agência (organização) que têm interesse directo no programa de segurança das TI;
- ⇒ Proporciona directivas na definição e suporte de métricas de segurança e nos benefícios da implementação;
- ⇒ Apresenta uma abordagem e um processo para o desenvolvimento de métricas de segurança das TI;
- ⇒ Discute os factores que podem afectar a implementação técnica do programa de métricas de segurança.

Outra alternativa é apresentada por Payne [2006] que define um conjunto de sete etapas chave que podem ser utilizadas para conduzir o processo de estabelecimento do programa de métricas de segurança, a saber:

- (1) Definir as metas e objectivos do programa de métricas de segurança;
- (2) Decidir que métricas gerar;
- (3) Desenvolver estratégias para a geração de métricas;
- (4) Estabelecer parâmetros e referências;
- (5) Determinar como devem as métricas ser reportadas;
- (6) Criar um plano de acção e actuar de acordo;
- (7) Estabelecer um programa formal com ciclo de revisão/refinamento.

Segundo Swanson *et al* [2003], o desenvolvimento e implementação do programa de métricas de segurança deve considerar os seguintes aspectos:

- As métricas devem produzir informação quantificável (percentagens, médias e números);
- Os dados de suporte das métricas devem ser obtidos prontamente;
- Apenas os processos repetitivos devem ser considerados para medição;
- As métricas devem ser úteis para seguir o desempenho e direccionar recursos.

As medições de segurança da informação utilizam um conjunto diversificado de técnicas que, de acordo com Herrmann [2002:64], podem ser enquadradas em termos de

confidencialidade, integridade e disponibilidade da informação. A perspectiva apresentada, que congrega os factores considerados como fundamentais no respeitante à segurança da informação, é enquadrada em conformidade com os exemplos de métricas que se apresentam seguidamente:

Medições de confidencialidade:
– Encriptação; – Âmbito da Gestão; – Isolamento seguro dos substitutos; – Controlo de acessos; – Autenticação; – Seguimento da auditoria; – Isolamento de processos; – Etiquetagem de identificação; – Protecção contra acções acidentais e intencionais.
Medições de integridade:
– Algoritmos de detecção/correção de erros; – Provas formais da sua correção; – Compartimentação; – Esconder informação; – Protecção contra acções acidentais e intencionais; – Avaliação dos níveis de conforto.
Medições de disponibilidade:
– Equipamento de comunicação redundante; – Caminhos de comunicação alternativos; – Recuperação confiável.

Tabela 6.1 – Exemplos de medições de confidencialidade, integridade e disponibilidade
(adaptado de Herrmann [2002])

Considerando esta envolvente da segurança da informação, as Pessoas e a maior ou menor facilidade com que trabalham com os sistemas de segurança implementados, tornam fundamental que se proceda à definição de métricas para a usabilidade dos SI após a implementação de segurança, de modo idêntico ao que se pretende para a segurança da informação.

Torna-se assim possível constatar que, quando se procura identificar o conjunto de parâmetros que permitam medir a usabilidade de um sistema, considera-se importante identificar e compreender o contexto em que o próprio sistema foi desenvolvido e

implementado, assumindo como factor fundamental o grau de envolvimento dos utilizadores finais nestas actividades, perspectivando sempre que possível o incremento desse grau de envolvimento.

Neste sentido, torna-se igualmente importante perceber o negócio, procurando um entendimento sobre quais são os objectivos que o SI deve permitir atingir, de modo a que o âmbito dos parâmetros a analisar englobe todo o sistema.

Encontrar parâmetros que possibilitem a aferição da usabilidade de um SI conduz à necessidade de avaliação do desempenho das TIC por um lado e ao entendimento do papel desempenhado pelas Pessoas e pelas componentes organizacionais pelo outro. Kirakowski [1994] sugere aliás duas aproximações, uma para medir a satisfação dos utilizadores e outra para medir a qualidade de utilização do sistema.

Esta focalização nos utilizadores comporta em si quer a avaliação das TIC que suportam o sistema quer as mudanças induzidas na organização, tornando impossível proceder a medições de usabilidade de um sistema sem atender à respectiva envolvente.

Todavia, deve ter-se em atenção que a definição de métricas de segurança da informação quando estão envolvidas Pessoas, nomeadamente a sua percepção acerca dessa segurança, implica incluir no processo aspectos intangíveis que são habitualmente de repetição difícil e usualmente distintos de organização para organização, levando a que seja necessária a definição objectiva das métricas a atingir.

Neste contexto, pode ser arguido que, pela medida do fenómeno conectado com a segurança da informação, as relações cruzadas podem ser melhor entendidas, todavia, o entendimento actual dessas inter relações pode ajudar a entender melhor a verdadeira natureza da segurança da informação [Kajava and Savola 2005].

Assumindo que as métricas dependem dos objectivos da organização e que vão aferir/validar a eficácia da segurança implementada, o espectro sobre o qual vão ser definidas deverá ser suficientemente abrangente para responder às necessidades das organizações.

Neste âmbito, deve considerar-se que estas métricas correspondem apenas a contextos onde as Pessoas estão envolvidas, não significando isso que não possam ser aplicadas a outros contextos quando tal se revele necessário.

Considera-se ainda pertinente, procurando uma focalização nas Pessoas e no como entendem esta problemática, a aplicação de métricas que tenham em atenção a sua percepção pessoal, nomeadamente tópicos a reter da revisão bibliográfica efectuada e que fazem parte das preocupações dos envolvidos na problemática da segurança da informação.

As métricas apresentadas na tabela seguinte devem ser consideradas apenas como exemplos de possíveis métricas obtidas através da revisão bibliográfica, derivando essencialmente da percepção das Pessoas acerca da problemática da segurança da informação e dos SI e das TIC que suportam essa mesma informação. Todavia, deve considerar-se que os exemplos seguintes não esgotam de modo algum as possibilidades de especificação de métricas, considerando-as apenas como meros exemplos.

Satisfação com:
– Mudanças nos SI e nas TIC; – Mudanças das políticas de segurança; – Participação nas mudanças; – Acções de formação; – Documentação de apoio.
Classificação do grau de:
– Participação nas mudanças nos SI e nas TIC; – Participação nas mudanças das políticas de segurança; – Melhorias percebidas; – Satisfação com as mudanças; – Facilidade de utilização após as mudanças; – Facilidade de aprendizagem após as mudanças; – Segurança percebida acerca do SI; – Satisfação com as acções de formação; – Satisfação com a documentação de apoio.
Actividades realizadas:
– Violações do SI detectadas; – Atitudes perante as violações detectadas; – Controlos de segurança violados; – Acções de formação participadas; – Intervenções técnicas solicitadas.
Envolvimento:
– Sugestões de melhoria funcional; – Especificação de requisitos; – Conhecimento das políticas; – Acessos ao SI.

Tabela 6.2 – Exemplos de possíveis métricas

Deve ainda considerar-se que o facto de serem exemplificadas estas métricas, não fica de qualquer forma impedida a definição de outras que, perante situações concretas, sejam entendidas como necessárias para aferir a especificidade de implementações e utilizações do SGSI. Este aspecto é aliás referenciado nas normas como uma hipótese a considerar sempre que tal se revele necessário, cumprindo obviamente os requisitos recomendados para que as medições obtidas possam ser aceites.

Assumindo que, segundo Payne [2006], métricas realmente úteis indicam o grau para o qual os objectivos de segurança são especificados, como por exemplo a confidencialidade dos dados, indicando acções para melhorar o programa de segurança de toda a organização, e que em termos genéricos, para Kajava and Savola [2005], as métricas são muito úteis quando podem ser utilizadas proactivamente, prevendo ou tentando entender situações futuras, torna-se essencial que as métricas a implementar estejam de acordo com os objectivos de segurança previamente estabelecidos.

6.4. Conclusões

Face ao desenvolvimento apresentado, conclui-se que a definição de métricas na área da segurança da informação apresenta condicionalismos derivados da especificidade de cada caso concreto, confrontando-se frequentemente com a escassez de referências de base para validar as medições efectuadas.

Estes aspectos surgem frequentemente afectados pelo tipo de métricas adoptadas, quantitativas ou qualitativas, influenciando desde logo a sua aplicabilidade, particularmente no contexto deste trabalho onde essas métricas devem considerar aspectos directamente associados à percepção das Pessoas acerca da segurança da informação, aspectos estes de natureza claramente subjectiva, e como tal dependentes de quem procede à sua análise.

Verifica-se ainda que, qualquer que seja a métrica definida ou a definir, é obrigatório que seja aplicada a situações e/ou casos passíveis de serem repetidos, levando a que qualquer parâmetro a ser aferido necessite de ser devidamente especificado de forma a assegurar o cumprimento dos requisitos necessários para que qualquer métrica possa ser considerada válida.

Perante as situações identificadas, a definição de métricas encontra condicionamentos motivados quer pela dificuldade da sua aplicação, quer pelas implicações que derivam da utilização de métodos qualitativos que, pela sua natureza intrínseca, envolvem e são afectados pela percepção de quem realiza as medições necessárias.

A utilização de normativo relacionado com métricas de segurança da informação permite proporcionar de uma forma mais fácil um conjunto de métricas capazes de responder aos requisitos das organizações na aferição da eficácia dos controlos relativos às suas políticas de segurança.

Além disto, perspectiva-se a especificação e utilização de métricas adequadas à aferição dos diversos aspectos relacionados com a percepção das Pessoas, seja a sua satisfação relativa à utilização dos sistemas ou tecnologias ou ao como classificam esses mesmos aspectos.

Referências bibliográficas

- Bowen, P., Hash, J. and Wilson, M., *Information Security Handbook: A Guide for Managers*, Special Publication 800-100, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2006.
- Chew, E., Clay, A., Hash, J., Bartol, N. and Brown, A., *Guide for Developing Performance Metrics for Information Security*, Special Publication 800-80 (Initial Public Draft), National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2006.
- COBIT, *Control Objectives for Information and related Technology (Version 4.0)*, IT Governance Institute, 2005.
- FISMA, *Federal Information Security Management Act*, Senate and House of Representatives of the United States of America, 2002.
- Henning, R. (editor), *Workshop on Information Security Scoring and Ranking – Information System Security Attribute Quantification or Ordering* (Commonly but Improperly Known as “Security Metrics”), Applied Computer Security Associates, 2001.
- Herrmann, D.S., *A Practical Guide to Security Engineering and Information Assurance*, CRC Press, 2002.

- IEEE, *Standard Glossary of Software Engineering Terminology*, STD610.12-1990, September 28, 1990.
- Kajava, J. and Savola, R., “Towards Better Information Security Management by Understanding Security Metrics and Measuring Processes”, VTT Technical Research Centre of Finland, 2005.
- Katzke, S., “Security Metrics”, National Security Agency, 2001.
- Kirakowski, J., “The use of Questionnaire methods for usability assessment”, SUMI background reading, <http://www.ucc.ie/hfrg/questionnaires/sumi/sumipapp.html> (25-10-2002).
- Maguire, M.C., “User-Centred Requirements Handbook”, version 3.2, HUSAT Research Institute - Telematics Applications Programme RESPECT project (TE 2010), June 29, 1998, <http://www.ejeisa.com/nectar/respect/5.3/index.htm> (15-11-2002).
- OECD, *Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*, Organisation for Economic Co-operation and Development, 2002.
- Parkinson, D. (Editor), *Oxford Business English Dictionary*, Oxford University Press, 2005.
- Payne, S., “A Guide to Security Metrics”, SANS Institute, Inc., June 19, 2006.
- Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G. and Lee, A., *Recommended Security Controls for Federal Information Systems*, Special Publication 800-53, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2005.
- Stoddard, M., Bodeau, D., Carlson, R., Glantz, C., Haimes, Y., Lian, C., Santos, J. and Shaw, J., “Process Control System Security Metrics – State of Practice”, Research Report, 1, Institute for Information Infrastructure Protection (I3P), Dartmouth College, August 2005.
- Swanson, M., *Security Self-Assessment Guide for Information Technology Systems*, Special Publication 800-26, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2001.
- Swanson, M., Bartol, N., Sabato, J., Hash, J. and Graffo, L., *Security Metrics Guide for Information Technology Systems*, Special Publication 800-55, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2003.

Weiß, S., Weissmann, O. and Dressler, F., “A Comprehensive and Comparative Metric for Information Security”, IFIP International Conference on Telecommunication Systems, Modeling and Analysis 2005 (ICTSM2005), Dallas, TX, USA, November, 18, 2005.

7

Criação do Modelo

Num contexto, complexo e contingencial, onde a informação como activo organizacional, assim como a importância dos SI e das TIC que a suportam, são aspectos claramente condicionados pela necessidade de assegurar a sua segurança e privacidade, realçando a pertinência da criação de modelos, que permitam a simplificação e/ou uma melhor compreensão das implicações das Pessoas nos SGSI.

Um modelo é uma abstracção, ou seja, uma representação de uma parte do mundo real. O benefício de uma abstracção é o desenvolvimento fiável de aplicações complexas, proporcionando uma forma de visualizar que aquilo que o modelo indica são aspectos importantes do sistema, nos seus vários níveis, onde os níveis elevados têm a essência do sistema e os níveis inferiores têm o detalhe, que não compromete essa essência [Avison e Fitzgerald 2003].

Definição similar de modelo é apresentada por Alter [1998], que o entende como a representação útil de uma situação ou coisa específica, considerando que os modelos são úteis para descrever ou simular uma realidade sem ter de se lidar com todos os seus detalhes.

Definições mais formais de modelo apresentam-no como um “esquema teórico em matéria científica, representativo de um comportamento, de um fenómeno ou conjunto de fenómenos” [DicPE 2006], como a “descrição simples de um sistema, usado para especificar como algo funciona ou inferir o que pode acontecer” [OxfDic 2005], ou ainda como “coisa ou pessoa que serve de imagem, forma ou padrão a ser imitado” [DicHouaiss 2003].

A construção do Modelo será ponderada por um conjunto de referenciais²³ provenientes das normas (denominados referenciais alfa – α), da revisão da literatura (denominados referenciais beta – β) e das métricas (denominados referenciais gamma – γ).

²³ O que é utilizado como referência [DicMichaelis 1998].

7.1. Enquadramento Conceptual

Quando se aborda a problemática da segurança da informação, a referência mais comum encontra-se associada à utilização dos computadores, ficando assim esquecidas diversas situações que podem condicionar essa mesma segurança.

De entre essas situações referenciam-se os documentos escritos (frequentemente esquecidos em cima de mesas e secretárias ou até colocados intactos nos caixotes do lixo), telefaxes (deixados por vezes nos respectivos aparelhos), ficheiros abertos em computadores sem qualquer utilizador por perto, *post-its* com *passwords* deixados em local visível por um conjunto de Pessoas, e até conversas de café sobre a organização sem se atender aos potenciais ouvintes.

Considera-se que a generalidade das situações que aqui se colocam derivam de mero descuido (não desejável e sujeito a penalidades) e não de situações propositadas para causar danos. Estas situações decorrem genericamente da inexistência de políticas de segurança da informação ou, no caso de existirem, da sua incorrecta divulgação pelos actores organizacionais.

Um outro aspecto habitualmente descuidado na segurança da informação relaciona-se com o facto de não ser dada atenção às ameaças internas, focalizando-se maioritariamente nos aspectos externos.

Por outro lado, quando a utilização dos SI não se adequa às expectativas dos utilizadores, porque as políticas de segurança implementadas são demasiado restritivas ou complexas, podem aparecer casos onde os utilizadores tendem a encontrar alternativas não previstas para ultrapassar os mecanismos implementados.

7.1.1. Contributos da Literatura

Consederara-se-à aqui a cultura de cada organização, a sua missão e objectivos, como factores que afectam a percepção de segurança que os utilizadores associam à informação que partilham, particularmente se não entenderem essa segurança como crucial para a organização e para o seu próprio desempenho. Também neste âmbito, a cultura de cada utilizador e a sua experiência com os SI e as TIC podem afectar a forma como estes encaram e assumem a pertinência da segurança.

Além disso, a forma como os decisores organizacionais apreendem a relevância da segurança da informação e permitem a envolvimento nesse processo de todos os utilizadores, pode fazer a diferença no sucesso ou fracasso da segurança da informação, afectando em consequência o desempenho da própria organização.

Poderá também considerar-se que a forma como os utilizadores aderem às políticas de segurança da informação depende dessa envolvimento e do sentimento acerca das potenciais ameaças para o seu desempenho na organização, que podem estar associadas a essas mesmas políticas.

Neste contexto, onde a adesão dos utilizadores é crucial, a formação e o consequente envolvimento nas diversas etapas relacionadas com a segurança pode revelar-se fundamental para garantir que o facto de serem implementadas políticas de segurança, não implica que isso constitua uma ameaça para a sua segurança pessoal e para a privacidade da sua informação.

No sentido de manter e reforçar o envolvimento das Pessoas nas mudanças necessárias nas organizações, quer na respostas aos novos objectivos de negócio quer às implicações de utilização de novas TIC e da segurança da informação que suportam, as melhorias a introduzir devem resultar da auscultação das Pessoas em todos os processos, para que quaisquer mudanças a considerar não sejam entendidas como ameaças às suas posições e estabilidade na organização.

Tendo em consideração estes princípios, procedeu-se à identificação dos controlos derivados da revisão da literatura e que foram percebidos como pertinentes para este contexto, particularmente pela sua capacidade de em conjunto suportar a elaboração das respostas às questões de partida, nomeadamente:

- ⇒ Questão 1 (*Qual a percepção dos utilizadores acerca da segurança da informação existente no SI? – Q1*);
- ⇒ Questão 2 (*Que indicadores possibilitam a avaliação da segurança de um SI e a avaliação de um SGSI? – Q2*);
- ⇒ Questão 3 (*Como são aceites pelas pessoas as mudanças tecnológicas e organizacionais motivadas pela implementação do SGSI? – Q3*).

Os controlos mencionados são apresentados nas tabelas seguintes, agrupando-se em referenciais de acordo com a sua afinidade. Nestas tabelas mencionam-se o(s) autor(es) de cada um dos controlos e as questões a cada referencial permite responder.

Aceitação e Desempenho (Q2, Q3)	
Autor(es)	Controlos
Caldeira e Romão 2002b	– Reacção das Pessoas à implementação de um sistema informático
Henry 2003	– Aceitação e adesão dos utilizadores às restrições de segurança
Herold 2003	– Sucesso da segurança da informação requer a participação, concordância e suporte das Pessoas na organização – Sucesso da implementação de SGSI quando esta afecta o desempenho das Pessoas
Kabay 2002	– Responsabilidade das Pessoas na protecção da informação
Lourenço e O'Neill 2002	– Potencialidades das TIC para modificar e/ou renovar as competências
Misiolek <i>et al</i> 2002	– Formação das Pessoas para aceitação das TIC
Reis e Amaral 2002	– Aumentar a eficiência e eficácia do processamento da informação
Rodrigues 2002	– Desempenho dos SI
Serrano e Caldeira 2001	– Aceitação de um projecto informático pelos utilizadores – Nível de satisfação dos utilizadores dos SI

Tabela 7.1 – Controlos para o referencial β 'Aceitação e Desempenho'

Activos Organizacionais (Q1, Q2, Q3)	
Autor(es)	Controlos
Anunciação e Zorrinho 2006	– Os SI e as TIC como activos organizacionais
Barman 2002	– Identificar que activos devem ser protegidos
Dinis 2005	– Informação como activo organizacional, “associado aos processos, às Pessoas e às tecnologias”
Reis 1993	– TIC como veículo de disponibilização da informação
Reis e Amaral 2002	– Aumentar a eficiência e eficácia do processamento da informação
Rodrigues 2002	– Disponibilização de informação
Veiga 2002	– Disponibilização de recursos para implementar políticas de segurança

Tabela 7.2 – Controlos para o referencial β 'Activos Organizacionais'

Ameaças e Violações da Segurança (Q2)	
Autor(es)	Controlos
Carneiro 2002	– Comportamentos adequados perante ameaças ao SI
King <i>et al</i> 2001	– Ameaças à segurança da informação ou do SI – Violações da segurança da informação
Peltier 2001	– Ameaças à informação e aos SI
Whitman and Mattord 2005	– Ameaças aos activos

Tabela 7.3 – Controlos para o referencial β 'Ameaças e Violações de Segurança'

Envolvimento das Pessoas (Q1)	
Autor(es)	Controlos
Barman 2002	– As Pessoas na utilização dos activos
Carneiro 2002	– Colaboração das Pessoas na manutenção da segurança do SI – Cooperação dos utilizadores para a implementação da política de segurança
Kabay 2002	– Responsabilidade das Pessoas na protecção da informação
Llufrú 2005	– Envolver as Pessoas no planeamento e implementação das TIC
Lourenço e O'Neill 2002	– Envolver todas as Pessoas para aproveitamento das potencialidades das TIC
Neves 2001	– Percepção da realidade afecta o comportamento das Pessoas
Whitten and Tygar 1998	– As Pessoas na segurança dos computadores

Tabela 7.4 – Controlos para o referencial β 'Envolvimento das Pessoas'

Estratégia Organizacional e Especificação de Requisitos (Q1)	
Autor(es)	Controlos
Almeida 2007	– Componentes fundamentais da sociedade
Anunciação e Zorrinho 2006	– Enquadramento das organizações
Barman 2002	– Objectivos gerais das políticas de segurança – Identificar que activos devem ser protegidos
Coelho 2005	– Especificação dos SI deve cumprir a estratégia organizacional
Lopes e Amaral 2000	– Alinhamento do SI e das TI com a estratégia organizacional
Mamede 2006	– Perspectivas de segurança de uma organização
Martin <i>et al</i> 2002	– Componentes fundamentais de uma organização
Reis 1993	– TIC como veículo de disponibilização da informação
Reis e Amaral 2002	– Identificar a informação importante e as respectivas fontes
Tavares e Pereira 2000	– Os SI como suporte dos processos de gestão
Veiga 2002	– Segurança contemplada desde o início da concepção dos SI – Segurança como parte integrante das especificações dos SI

Tabela 7.5 – Controlos para o referencial β 'Estratégia Organizacional e Especificação de Requisitos'

Formação (Q3)	
Autor(es)	Controlos
Caldeira e Romão 2002b	– Desenvolver competências na área dos SI/TI para construir sistemas – Desenvolver competências na área dos SI/TI potencia o diálogo entre utilizadores e técnicos
Carneiro 2002	– Proporcionar formação adequada às Pessoas e aos responsáveis organizacionais
Henry 2003	– Formar os utilizadores sobre o SI e a Segurança
Kovács 1998	– Aprendizagem contínua para actualizar conhecimentos
Lindley 2000	– Aprendizagem contínua para desenvolver novas competências
Misiolek <i>et al</i> 2002	– Formação das Pessoas para aceitação das TIC

Tabela 7.6 – Controlos para o referencial β 'Formação'

Mudanças nos SI e/ou nas TIC (Q3)	
Autor(es)	Controlos
Caldeira e Romão 2002b	– Reacção das Pessoas à implementação de um sistema informático – Resistência à mudança quando são implementados sistemas e TIC
Carneiro 2002	– Cooperação dos utilizadores para a implementação da política de segurança
Dinis 2005	– Considerar as mudanças como relevantes permite que as Pessoas as tolerem
Henry 2003	– Aceitação e adesão dos utilizadores às restrições de segurança
Misiolek <i>et al</i> 2002	– Implementação de TIC provoca mudanças organizacionais

Tabela 7.7 – Controlos para o referencial β ‘Mudanças nos SI e/ou nas TIC’

Política de Segurança da Informação (Q1, Q2, Q3)	
Autor(es)	Controlos
Barman 2001	– Políticas de segurança da informação
Barman 2002	– Responsabilidades da gestão na segurança da informação – Objectivos gerais das políticas de segurança
Caldeira e Romão 2002b	– Envolvimento da gestão de topo na adopção de SI/TI
Carneiro 2002	– Políticas e medidas de segurança estabelecidas para benefício dos SI e do desempenho dos utilizadores
Fenton and Wolfe 2003	– Segurança da informação
Henry 2003	– Papel da segurança na organização
Herrmann 2003	– Segurança da informação e do SI
Mamede 2006	– Envolvimento dos responsáveis da organização no processo de segurança
Peltier 2001	– Segurança da informação
Pfleeger and Pfleeger 2003	– Segurança da informação
Reis 2000	– Comprometimento dos decisores organizacionais afecta o sucesso das medidas de segurança
Ross 1999	– Segurança da informação
Zúquete 2006	– Políticas de segurança – Mecanismos de segurança

Tabela 7.8 – Controlos para o referencial β ‘Política de Segurança da Informação’

Usabilidade dos SI e das TIC (Q3)	
Autor(es)	Controlos
Bias and Mayhew 1994	– SI e TIC fáceis de usar e aprender – Desenvolver SI mais ‘utilizáveis’ para qualquer tipo de utilizador
Daly-Jones <i>et al</i> 1999	– Usabilidade e segurança dependem do contexto em que o SI vai ser usado – Usabilidade e segurança dependem das características dos potenciais utilizadores
Santana e Dias 2005	– Percepção da utilidade e simplicidade de utilização do SI
Serrano e Caldeira 2001	– Nível de satisfação dos utilizadores dos SI

Tabela 7.9 – Controlos para o referencial β ‘Usabilidade dos SI e das TIC’

Os referenciais especificados foram posteriormente agrupados, mencionando os autores envolvidos na sua determinação, para enquadrar a resposta à principal questão colocada no trabalho, *Qual o impacto na actividade das pessoas quando se implementa um SGSI?*. Os resultados obtidos constam da tabela seguinte.

Questão: Qual o impacto na actividade das pessoas quando se implementa um SGSI?	
Referenciais Beta (β)	Autor(es)
$\beta 1$ – Aceitação e Desempenho	Caldeira e Romão 2002b, Henry 2003, Herold 2003, Kabay 2002, Lourenço e O'Neill 2002, Misiolek <i>et al</i> 2002, Reis e Amaral 2002, Rodrigues 2002, Serrano e Caldeira 2001
$\beta 2$ – Activos Organizacionais	Anunciação e Zorrinho 2006, Barman 2002, Dinis 2005, Reis 1993, Reis e Amaral 2002, Rodrigues 2002, Veiga 2002
$\beta 3$ – Ameaças e Violações da Segurança	Carneiro 2002, King <i>et al</i> 2001, Peltier 2001, Whitman and Mattord 2005
$\beta 4$ – Envolvimento das Pessoas	Barman 2002, Carneiro 2002, Kabay 2002, Llufríu 2005, Lourenço e O'Neill 2002, Neves 2001, Whitten and Tygar 1998
$\beta 5$ – Estratégia Organizacional e Especificação de Requisitos	Almeida 2007, Anunciação e Zorrinho 2006, Barman 2002, Coelho 2005, Lopes e Amaral 2000, Mamede 2006, Martin <i>et al</i> 2002, Reis 1993, Reis e Amaral 2002, Tavares e Pereira 2000, Veiga 2002
$\beta 6$ – Formação	Caldeira e Romão 2002b, Carneiro 2002, Henry 2003, Kovács 1998, Lindley 2000, Misiolek <i>et al</i> 2002
$\beta 7$ – Mudanças nos SI e/ou nas TIC	Caldeira e Romão 2002b, Carneiro 2002, Dinis 2005, Henry 2003, Misiolek <i>et al</i> 2002
$\beta 8$ – Política de Segurança da Informação	Barman 2001, Barman 2002, Caldeira e Romão 2002b, Carneiro 2002, Fenton and Wolfe 2003, Henry 2003, Herrmann 2003, Mamede 2006, Peltier 2001, Pfleeger and Pfleeger 2003, Reis 2000, Ross 1999, Zúquete 2006
$\beta 9$ – Usabilidade dos SI e das TIC	Bias and Mayhew 1994, Daly-Jones <i>et al</i> 1999, Santana e Dias 2005, Serrano e Caldeira 2001

Tabela 7.10 – Referenciais β para resposta à principal questão do trabalho

Os referenciais constantes da tabela anterior, mencionados como Referenciais Beta (β) vão ser utilizados para o desenvolvimento do Modelo.

7.1.2. Contributos das Métricas

Neste contexto, vão apenas ser utilizadas métricas obtidas de documentos estudados e de normas não constantes do que se referenciou como núcleo central do normativo estudado. De entre os controlos referenciados, entendem-se como relevantes para aplicação no contexto deste trabalho os que vão ser enquadrados em termos de referenciais, na resposta às questões de partida, nomeadamente:

- ⇒ Questão 1 (*Qual a percepção dos utilizadores acerca da segurança da informação existente no SI? – Q1*);
- ⇒ Questão 2 (*Que indicadores possibilitam a avaliação da segurança de um SI e a avaliação de um SGSI? – Q2*);
- ⇒ Questão 3 (*Como são aceites pelas pessoas as mudanças tecnológicas e organizacionais motivadas pela implementação do SGSI? – Q3*).

Estes controlos são apresentados nas tabelas seguintes agrupados em referenciais de acordo com a sua afinidade, mencionando-se os documentos ou as normas de onde cada um dos controlos foi obtido e as questões a que cada referencial permite responder.

Neste âmbito foram utilizadas as seguintes normas: FISMA [FISMA 2002]; NIST SP800-26 [Swanson 2001]; NIST SP800-55 [Swanson *et al* 2003]; NIST SP800-80 [Chew *et al* 2006].

Ameaças e Violações da Segurança (Q2)	
Norma	Controlos
<i>NIST SP800-55 e NIST SP800-26</i>	– Capacidade de Resposta a Incidentes – Integridade dos Dados
<i>NIST SP800-80</i>	– Resposta a Incidentes – Protecção dos dispositivos de Dados – Protecção das Comunicações e Sistemas – Integridade da Informação e dos Sistemas

Tabela 7.11 – Controlos para o referencial γ ‘Ameaças e Violações da Segurança’

Avaliação e Auditorias (Q2)	
Norma	Controlos
<i>FISMA</i>	– Teste dos Controlos de Segurança do Sistema
<i>NIST SP800-55 e NIST SP800-26</i>	– Seguimento das Auditorias – Revisão dos Controlos de Segurança
<i>NIST SP800-80</i>	– Auditoria e Responsabilização – Certificação, Acreditação e Valorização da Segurança

Tabela 7.12 – Controlos para o referencial γ ‘Avaliação e Auditorias’

Gestão de Acessos (Q1)	
Norma	Controlos
<i>NIST SP800-55 e NIST SP800-26</i>	– Controlo dos Acessos Lógicos
<i>NIST SP800-80</i>	– Controlo de Acessos

Tabela 7.13 – Controlos para o referencial γ ‘Gestão de Acessos’

Gestão dos Activos (Q1, Q2, Q3)	
Norma	Controlos
<i>FISMA</i>	– Segurança dos Serviços Proporcionados pelos Fornecedores – Desenvolvimento e Verificação do Inventário do Sistema
<i>NIST SP800-55 e NIST SP800-26</i>	– Manutenção dos Sistemas de Software e Hardware
<i>NIST SP800-80</i>	– Manutenção – Aquisição de Serviços e Sistemas

Tabela 7.14 – Controlos para o referencial γ ‘Gestão dos Activos’

Política de Segurança da Informação (Q1, Q2, Q3)	
Norma	Controlos
<i>FISMA</i>	– Gestão da Configuração e das Políticas de Tratamento de Incidentes – Plano de Acção da Agência (Organização) e Processos Relevantes
<i>NIST SP800-55 e NIST SP800-26</i>	– Documentação – Plano de Segurança do Sistema – Segurança Física – Segurança das Pessoas
<i>NIST SP800-80</i>	– Gestão da Configuração – Planeamento – Protecção Ambiental e Física – Segurança das Pessoas

Tabela 7.15 – Controlos para o referencial γ ‘Política de Segurança da Informação’

Sensibilização, Treino e Educação (Q3)	
Norma	Controlos
<i>FISMA</i>	– Sensibilização, Treino e Educação em Segurança
<i>NIST SP800-55 e NIST SP800-26</i>	– Sensibilização, Treino e Educação sobre Segurança
<i>NIST SP800-80</i>	– Sensibilização e Treino

Tabela 7.16 – Controlos para o referencial γ ‘Sensibilização, Treino e Educação’

Utilização dos Activos (Q1, Q3)	
Norma	Controlos
<i>FISMA</i>	– Acreditação e Certificação – Qualidade do Processo de Acreditação e Certificação
<i>NIST SP800-55 e NIST SP800-26</i>	– Autorizar Processamento (Certificação e Acreditação) – Controlos de Produção, Entradas/Saídas – Identificação e Autenticação
<i>NIST SP800-80</i>	– Certificação, Acreditação e Valorização da Segurança – Identificação e Autenticação

Tabela 7.17 – Controlos para o referencial γ ‘Utilização dos Activos’

Os referenciais especificados foram posteriormente agrupados, mencionando as normas a que correspondem, para enquadrar a resposta à principal questão colocada no trabalho, *Qual o impacto na actividade das pessoas quando se implementa um SGSI?*. Estes resultados constam da tabela seguinte.

Questão: Qual o impacto na actividade das pessoas quando se implementa um SGSI?	
Referenciais Gamma(γ)	Normas
$\gamma 1$ – Ameaças e Violações da Segurança	NIST SP800-55 e NIST SP800-26, NIST SP800-80
$\gamma 2$ – Avaliação e Auditorias	FISMA, NIST SP800-55 e NIST SP800-26, NIST SP800-80
$\gamma 3$ – Gestão de Acessos	NIST SP800-55 e NIST SP800-26, NIST SP800-80
$\gamma 4$ – Gestão dos Activos	FISMA, NIST SP800-55 e NIST SP800-26, NIST SP800-80
$\gamma 5$ – Política de Segurança da Informação	FISMA, NIST SP800-55 e NIST SP800-26, NIST SP800-80
$\gamma 6$ – Sensibilização, Treino e Educação	FISMA, NIST SP800-55 e NIST SP800-26, NIST SP800-80
$\gamma 7$ – Utilização dos Activos	FISMA, NIST SP800-55 e NIST SP800-26, NIST SP800-80

Tabela 7.18 – Referenciais γ para resposta à principal questão do trabalho

Os referenciais constantes da tabela anterior, mencionados como Referenciais Gamma (γ) vão ser utilizados para o desenvolvimento do Modelo.

7.1.3. Modelo SDLC

O *Systems Development Life Cycle* (SDLC), ou Ciclo de Vida de Desenvolvimento de Sistemas, é utilizado para desenvolvimento, manutenção e substituição de SI [Hoffer *et al* 2001], que pretende proporcionar uma visão global dos aspectos associados à construção e utilização de SI, permitindo desse modo uma perspectiva integrada acerca do desenvolvimento de SI.

De acordo com os mesmos autores, este modelo organiza-se em seis fases, com a estrutura que se apresenta na figura 7.1:

- (1) Identificação e Selecção do Projecto;
- (2) Iniciação e Planeamento do Projecto;
- (3) Análise;
- (4) Desenho;
- (5) Implementação;
- (6) Manutenção.

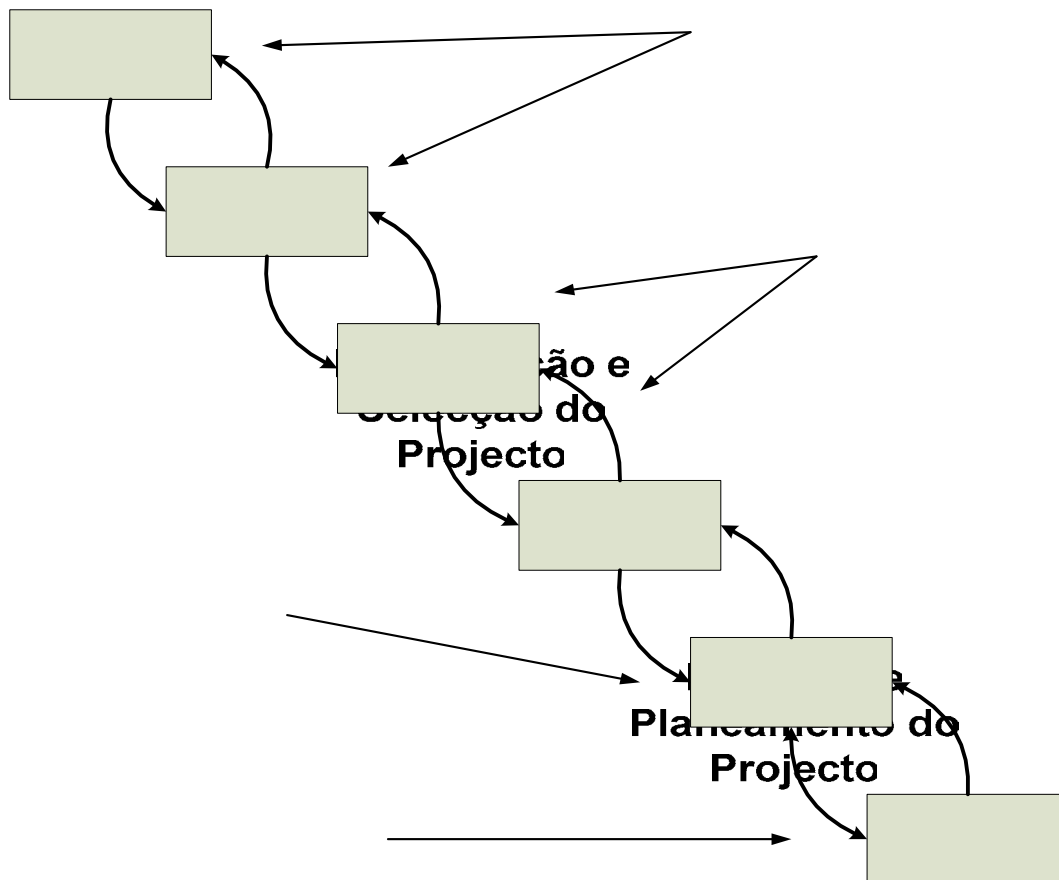


Figura 7.1 – Ciclo de Vida de Desenvolvimento de Sistemas
(adaptado de Hoffer et al [2001])

A utilização do modelo SDLC na segurança é objecto de uma abordagem alargada por parte da norma NIST SP800-64, que no entanto se foca quase essencialmente nos aspectos tecnológicos, sem especial atenção para com o papel das Pessoas no contexto, o que condiciona desde logo a sua plena utilização como base para suporte do Modelo [Grance et al 2003].

O modelo utilizado pela norma organiza-se em quadro fases, com a estrutura que se apresenta na figura 7.2:

- Análise**
- Esta fase considera a implementação e o teste do sistema, onde os utilizadores devem desempenhar um papel fundamental na respectiva validação
- (1) Iniciação;
 - (2) Desenvolvimento;
 - (3) Implementação;
 - (4) Operação e Manutenção

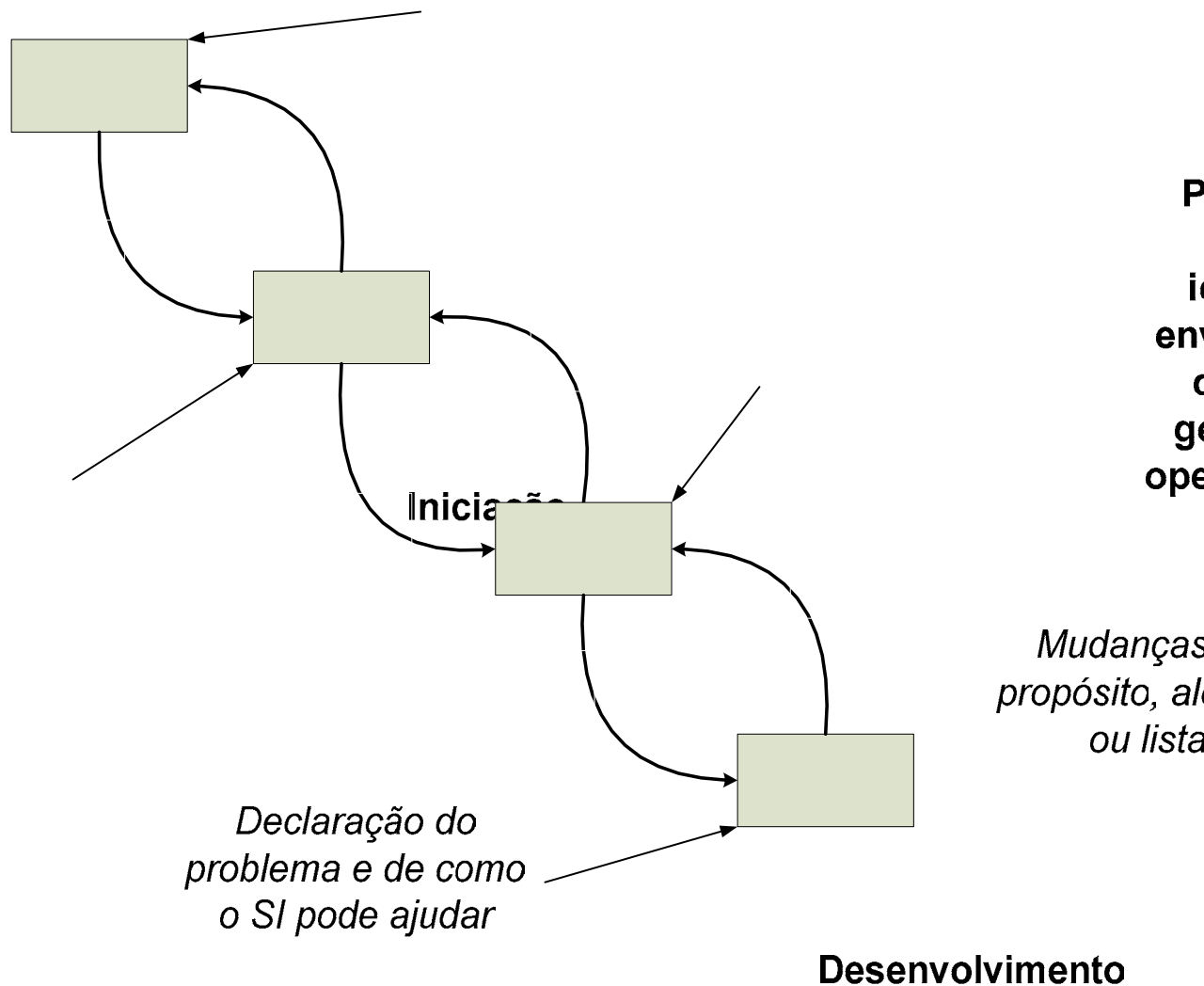


Figura 7.2 – Ciclo de Vida de Desenvolvimento de Sistemas (modelo reduzido)
(adaptado de Alter [1998])

Perante a importância da problemática da segurança, Veiga [2002] considera que esta deve ser contemplada desde o início do processo de concepção de todos os SI, referindo a necessidade das preocupações com a segurança serem parte integrante das especificações dos SI.

Considerando que a segurança da informação e dos sistemas deve ser um aspecto a ter em conta no planeamento, desenvolvimento e implementação de SI, interessa envolver desde logo no processo de desenvolvimento do SI e do SGSI os utilizadores, quer sejam novos ou potenciais, mesmo que não sejam utilizadores directos dos sistemas.

Processo de construir ou adquirir e configurar hardware e software, e outros recursos necessários para desempenhar as funções requeridas, relacionadas com as TI e as funções requeridas não relacionadas com as TI.

Programas executados num computador, mais a documentação dos utilizadores e procedimentos

As necessidades de envolvimento dos utilizadores anteriormente mencionadas podem ser supridas pela aplicação do contexto da segurança da informação ao modelo SDLC, constituindo-se deste modo como uma das bases de desenvolvimento do Modelo.

7.2. Normativo Aplicável

A elaboração do modelo de interacção entre as diversas normas analisadas atendeu aos aspectos relevantes, decorrentes das questões de partida do trabalho, a que cada uma das normas responde ou aborda.

Neste sentido, em função das normas estudadas, procedeu-se ao seu agrupamento de acordo com as respostas que as mesmas poderiam dar às questões de partida do trabalho, ou seja, Questão 1, Questão 2 e Questão 3.

O estudo do diverso normativo directa ou indirectamente aplicável à problemática da segurança da informação e dos SGSI, permitiu encontrar um grupo de normas adequadas a responder às questões de partida deste trabalho, considerando essencialmente a percepção das Pessoas no respeitante à segurança da informação e à sua aceitação na organização, mesmo quando a utilização dos SI, e das TIC que os suportam é afectada por essas alterações.

7.2.1. Normas

Neste contexto, considera-se que a utilização de normas adequadas a possibilitar elevados níveis de participação pode constituir-se como um dos factores de sucesso deste tipo de processos, correspondendo os outros factores a um claro e inequívoco envolvimento da gestão de topo, não só no apoio formal mas também na disponibilização atempada dos recursos necessários, e também à facilidade de utilização e aprendizagem dos SI e dos SGSI em uso na organização.

Refira-se aliás que nem sempre o impacto da implementação de SGSI conduz ou conduzirá a níveis de utilização e de aprendizagem mais baixos, particularmente quando as Pessoas, no seu papel de utilizadores actuais ou potenciais dos SI, são envolvidas nas actividades relacionadas com a sua concepção, desenvolvimento, implementação, e operação e manutenção.

Considera-se ainda pertinente mencionar que a realização de acções de sensibilização para uma utilização adequada dos SI e das TIC, conjuntamente com a problemática da segurança da informação, e o facto de se propiciar a formação necessária para aquisição de competências, podem contribuir para facilitar todo o processo, potenciando o desempenho das Pessoas na aquisição de vantagens competitivas para a organização.

Com esse objectivo em mente foi construído o modelo (derivado do normativo estudado no capítulo 2) que se apresenta na figura seguinte, considerando os aspectos directa ou indirectamente relacionados com as Pessoas, aspectos estes que fazem parte das normas abordadas, e que têm em atenção as políticas de segurança da informação, os SGSI, a utilização dos SI e das TIC e ainda a usabilidade (facilidade de utilização e de aprendizagem) enquadradas por essas mesmas normas.

Após a concretização destas actividades, procedeu-se em cada uma das normas à identificação dos aspectos referenciados que poderiam suportar as respostas necessárias para as questões de partida, independentemente da forma como são apresentados, enquadrados e classificados em qualquer caso concreto.

Esta identificação permitiu a elaboração de um ‘modelo’ de enquadramento das normas com as questões a que cada uma delas poderia responder de por si própria, após o que foi possível obter uma percepção sobre que normas respondiam em simultâneo às questões colocadas. O ‘modelo’ referenciado é apresentado na figura seguinte e vai ser aplicado no enquadramento do Modelo a desenvolver.

O facto de se ter identificado um conjunto restrito de normas (as que respondem em simultâneo a todas as questões), não significa que as que ficaram fora do denominado núcleo central não sejam relevantes para o contexto da segurança da informação.

Refira-se a propósito que o objectivo primordial desta ‘escolha’ foi apenas e só para evitar a dispersão da análise por um conjunto alargado, uma vez que era possível identificar apenas as que poderiam ser aplicadas para otimizar o desenvolvimento do trabalho, assumindo como critério único a existência de controlos adequados a enquadrar as respostas às questões de partida.

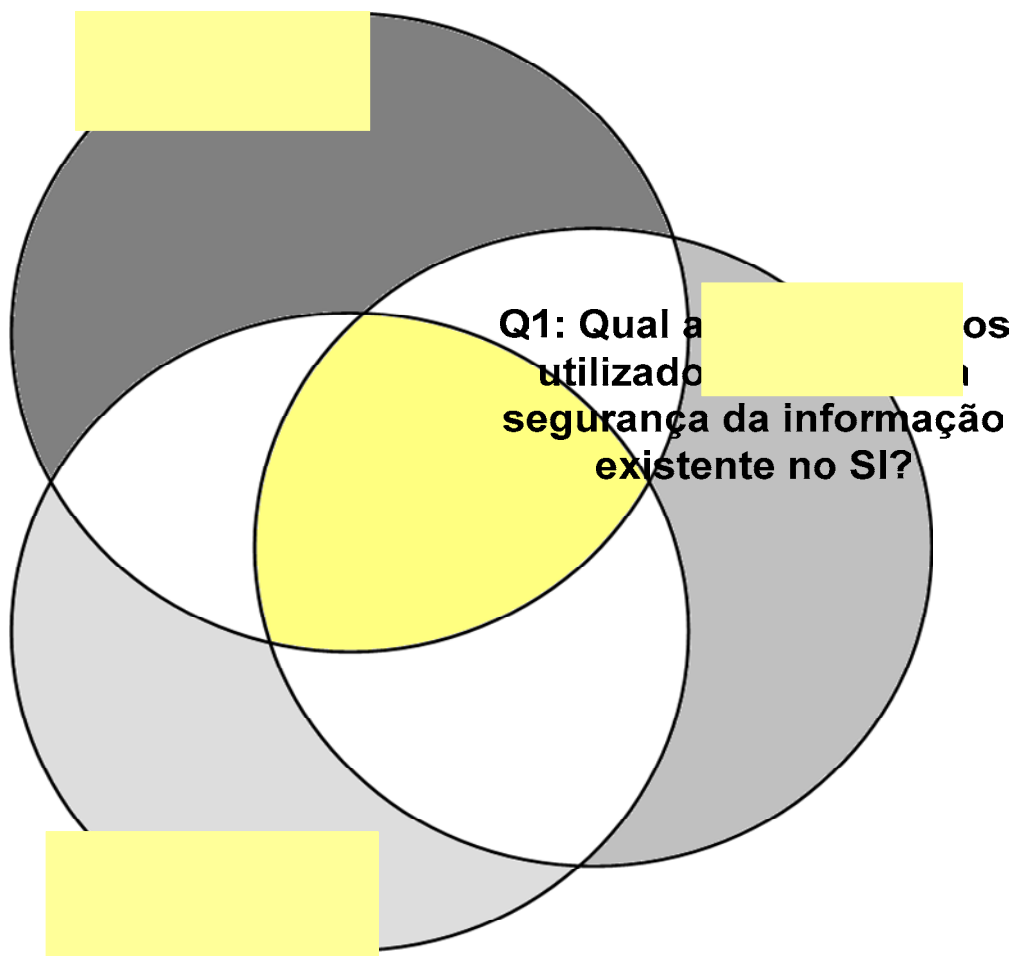


Figura 7.3 – Modelo de interação das normas

Refira-se todavia a necessidade de proceder à sua optimização, considerando a repetição de aspectos fundamentais nas normas que constituem o núcleo central deste modelo, que é basicamente constituído pelas seguintes normas:

- ⇒ BS ISO/IEC 17799:2005 – Information Technology - Security Techniques - Code of Practice for Information Security Management;
- ⇒ BS ISO/IEC 27001:2005 – Information Technology - Security Techniques - Information Security Management Systems – Requirements;
- ⇒ ISO/IEC 21827:2002 – Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM);
- ⇒ NIST SP800-12 – An Introduction to Computer Security: The NIST Handbook;
- ⇒ NIST SP800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems;

BS ISO/IEC 17799-3
BS ISO/IEC 27001-1
ISO/IEC 21827-1
NIST SP800-12
NIST SP800-14
NIST SP800-15
the Standard
COBIT,
GAISP,
ISSAF,
OECD

BS ISO/IEC 20000-1,
NIST SP800-16,
ITIL,
IT Baseline,
RFC 2196

BS IS
NIS
NIS

- ⇒ NIST SP800-18 – Guide for Developing Security Plans for Information Technology Systems;
- ⇒ The Standard of Good Practice for Information Security (the Standard);
- ⇒ OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security;
- ⇒ Control Objectives for Information and related Technology (COBIT);
- ⇒ Generally Accepted Information Security Principles (GAISP);
- ⇒ Information Systems Security Assessment Framework (ISSAF).

A identificação de um grupo de normas que respondam a todas as questões colocadas, foi realizada através do estabelecimento de uma tabela para cada uma das questões de partida, mencionando os itens de cada norma que permitem responder às referidas questões, quer sejam utilizados isolada ou conjuntamente.

As tabelas seguidamente apresentadas contêm apenas as normas do que se entende como o seu núcleo central, ou seja, aquelas que contêm itens relacionados com respostas a todas as questões. A divisão das tabelas de cada uma das questões deveu-se apenas à necessidade de manter a agregação dos itens de cada norma com a respectiva referência.

Nas tabelas seguintes, para os controlos associados a cada uma das normas acima mencionadas, que constituem o que se definiu como sendo o núcleo central do normativo estudado, são associadas as questões de partida do trabalho, referindo-se a que questão cada controlo pode suportar a totalidade ou parte da resposta.

Nesse sentido, com o objectivo de simplificar a apresentação das referidas relações em cada uma das tabelas, a Questão 1 (Qual a percepção dos utilizadores acerca da segurança da informação existente no SI?) é referenciada como Q1, a Questão 2 (Que indicadores possibilitam a avaliação da segurança de um SI e a avaliação de um SGSI) como Q2, e a Questão 3 (Como são aceites pelas pessoas as mudanças tecnológicas e organizacionais motivadas pela implementação do SGSI?) como Q3.

BS ISO/IEC 17799:2005 Code of practice for information security management	
Controlo [ISO 2005a]	Questão
5.1) Política de Segurança da Informação	Q1, Q2
5.1.1) Documento da Política de Segurança da Informação	Q1, Q3
5.1.2) Revisão da Política de Segurança da Informação	Q2
6.1.1) Compromisso da Gestão com a Segurança da Informação	Q1
6.1.2) Coordenação da Segurança da Informação	Q1
6.1.3) Alocação das Responsabilidades da Segurança da Informação	Q1
6.1.4) Processo de Autorização das Facilidades de Processamento da Informação	Q1
6.1.5) Compromisso de Confidencialidade	Q1, Q3
7.1.1) Inventário dos Activos	Q1, Q2, Q3
7.1.2) Posse dos Activos	Q1, Q2, Q3
7.1.3) Utilização Aceitável dos Activos	Q1
7.2) Classificação da Informação	Q2, Q3
7.2.1) Directrizes de Classificação da Informação	Q1, Q2, Q3
7.2.2) Identificação e Manipulação da Informação	Q1, Q3
8.1) Antes do Contracto	Q1
8.1.1) Papéis e Obrigações	Q1
8.2) Durante o Contracto	Q1
8.2.2) Treino, Educação e Sensibilização sobre Segurança da Informação	Q3
8.3) Depois do Contracto	Q1
10.1.1) Documentação dos Procedimentos Operativos	Q3
10.1.2) Gestão das Alterações	Q3
10.1.3) Separação dos Deveres	Q1
10.2.2) Monitorização e Revisão de Serviços de Terceiros	Q2
10.3.1) Gestão das Capacidades	Q1
10.3.2) Aceitação do Sistema	Q3
10.10.1) Registos de Auditoria	Q2
10.10.2) Monitorização da Utilização do Sistema	Q2
10.10.3) Protecção da Informação dos Registos	Q2
10.10.4) Registos do Administrador e do Operador	Q2
10.10.5) Registo de Falhas	Q2
10.10.6) Sincronização do Relógio	Q2
11.1.1) Política de Controlo de Acessos	Q1
11.2.1) Registo dos Utilizadores	Q1
11.2.2) Gestão dos Privilégios	Q1
11.2.3) Gestão das <i>Passwords</i> dos Utilizadores	Q1
11.2.4) Revisão dos Direitos de Acessos dos Utilizadores	Q1
11.3.1) Uso das <i>Passwords</i>	Q1
11.3.2) Utilizadores de Equipamentos sem Vigilância	Q1
11.3.3) Políticas de Limpeza das Secretárias e dos Ecrãs	Q1
12.1.1) Análise e Especificação dos Requisitos de Segurança	Q3
12.5.1) Procedimentos de Controlo das Alterações	Q3
12.5.2) Revisão Técnica das Aplicações após Mudanças do Sistema Operativo	Q3
12.5.3) Restrições nas Mudanças aos Pacotes de <i>Software</i>	Q3
15.1.1) Identificação da Legislação Aplicável	Q3
15.3) Considerações de Auditoria de SI	Q2

Tabela 7.19 – Controlos da norma BS ISO/IEC 17799 *versus* Questões de partida

BS ISO/IEC 27001:2005 – Information Security Management Systems – Requirements	
Controlo [ISO 2005b]	Questão
4.2.1) Estabelecer o SGSI	Q1
4.2.2) Implementar e Operar o SGSI	Q1, Q2
4.2.3) Monitorizar e Rever o SGSI	Q2
4.3) Requisitos de Documentação	Q1, Q3
4.3.3) Controlo dos Registos	Q2
5.1) Comprometimento da Gestão	Q1, Q2
5.2.1) Provisão de Recursos	Q2
5.2.2) Treino, Sensibilização e Competência	Q3
6) Auditorias Internas ao SGSI	Q2
7.2) <i>Inputs</i> para o Processo de Revisão	Q2
8.1) Melhoramentos Continuados	Q2, Q3

Tabela 7.20 – Controlos da norma BS ISO/IEC 27001 *versus* Questões de partida

NIST SP800-12 – An Introduction to Computer Security: The NIST Handbook	
Controlo [NIST 1998]	Questão
2) Elementos da Segurança de Computadores	Q1
3.6) Utilizadores	Q1
5.1.1) Componentes Básicos da Política do Programa	Q3
5.3.2) Regras de Segurança Operacional	Q1
8.4.2.1) Determinação dos Requisitos de Segurança	Q3
9.3.1) Teste e Certificação	Q2
9.4.1) Ferramentas e Métodos de Auditoria	Q2
9.4.2) Ferramentas e Métodos de Monitorização	Q2
10) Problemas de Pessoal/Utilizadores	Q1
10.1) Colocação do Pessoal	Q1
10.1.4) Sensibilização e Treino dos Funcionários	Q3
10.2) Gestão de Utilizadores	Q1
13.1) Comportamento	Q3
13.2) Responsabilização	Q3
13.3) Sensibilização	Q3
13.4) Treino	Q3
13.5) Educação	Q3
14.1) Suporte aos Utilizadores	Q1
14.6) Documentação	Q3
16) Identificação e Autenticação	Q1
17.1) Critérios de Acesso	Q1
17.3.1) Controlos de Acessos Internos	Q1
17.3.2) Controlos de Acesso Externos	Q1
17.4) Gestão dos Controlos de Acessos	Q1

Tabela 7.21 – Controlos da norma NIST SP800-12 *versus* Questões de partida

ISO/IEC 21827:2002 – Systems Security Engineering - Capability Maturity Model (SSE-CMM)	
Controlo [ISO 2002]	Questão
7.1.2) BP.01.01 - Estabelecer Obrigações de Segurança	Q1
7.1.4) BP.01.03 - Gerir os Programas de Sensibilização, Treino e Educação de Segurança	Q3
7.2.3) BP.02.02 - Identificar os Activos do Sistema	Q2
7.2.4) BP.02.03 - Seleccionar Métrica(s) de Impacto	Q2
7.2.5) BP.02.04 - Identificar Relacionamentos entre Métricas	Q2
7.8.2) BP.08.01 - Analisar os Registos dos Eventos	Q2
7.8.3) BP.08.02 - Monitorizar Alterações	Q2
7.8.5) BP.08.04 - Monitorizar Salvaguardas de Segurança	Q2
7.8.6) BP.08.05 - Revisão da Postura de Segurança	Q2, Q3
7.10.3) BP.10.02 - Identificar Leis, Políticas e Constrangimentos Aplicáveis	Q3
7.10.4) BP.10.03 - Identificar o Contexto de Segurança do Sistema	Q3
7.11) PA.11 - Verificar e Validar a Segurança	Q2

Tabela 7.22 – Controlos da norma ISO/IEC 21827 *versus* Questões de partida

SP800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems	
Controlo [Swanson and Guttman 1996]	Questão
3.1) Política	Q1
3.5) Problemas de Pessoal/Utilizadores	Q1
3.5.1) Pessoal	Q1
3.5.2) Administração dos Utilizadores	Q1
3.8) Sensibilização e Treino	Q3
3.9) Considerações de Segurança nas Operações e Suporte de Computadores	Q3
3.11.1) Identificação	Q1
3.11.2) Autenticação	Q1
3.11.3) <i>Passwords</i>	Q1
3.11.4) Autenticação Avançada	Q1
3.12.1) Critério de Acesso	Q1
3.12.2) Mecanismos de Controlo de Acessos	Q1
3.13.1) Conteúdos dos Registos de Seguimento das Auditorias	Q2
3.13.2) Segurança do Seguimento das Auditorias	Q2
3.13.3) Revisão do Seguimento das Auditorias	Q2
3.13.4) Monitorização do Uso do Teclado	Q2

Tabela 7.23 – Controlos da norma NIST SP800-14 *versus* Questões de partida

SP800-18 – Guide for Developing Security Plans for Information Technology Systems	
Controlo [Swanson 1998]	Questão
3.2.4) Atribuição das Obrigações de Segurança	Q1
3.7.1) Leis, Regulamentos e Políticas que Afectam o Sistema	Q3
4.2) Revisão dos Controlos de Segurança	Q2
5.MA.1) Segurança do Pessoal	Q1
5.MA.7) Documentação	Q1, Q3
5.MA.8) Sensibilização e Treino de Segurança	Q3
6.MA.1) Identificação e Autenticação	Q1
6.MA.4) Seguimento de Auditorias	Q2
5.GSS.1) Controlos do Pessoal	Q1
5.GSS.7) Documentação	Q1, Q3
5.GSS.8) Sensibilização e Treino de Segurança	Q3
6.GSS.1) Identificação e Autenticação	Q1
6.GSS.3) Seguimento de Auditorias	Q2

Tabela 7.24 – Controlos da norma NIST SP800-18 *versus* Questões de partida

Control Objectives for Information and related Technology (COBIT)	
Controlo [COBIT 2005]	Questão
PO4.6) Papéis e Responsabilidades	Q1
PO4.11) Segregação de Deveres	Q1
PO7.2) Competências do Pessoal	Q1
PO7.3) Atribuição dos Papéis	Q1
PO7.4) Treino Personalizado	Q3
AI6) Gerir as Alterações	Q3
AI6.5) Documentação e Finalização das Alterações	Q3
DS3.5) Monitorização e Reporte	Q2
DS5.3) Gestão de Identidades	Q3
DS7.1) Identificação das Necessidades de Educação e Treino	Q3
DS7.2) Entrega da Educação e Treino	Q3
DS7.3) Avaliação do Treino Recebido	Q3
DS9.3) Revisão da Integridade da Configuração	Q2
ME1.1) Abordagem da Monitorização	Q2
ME1.2) Definição e Recolha dos Dados da Monitorização	Q2
ME1.3) Método de Monitorização	Q2
ME1.4) Valorização do Desempenho	Q2
ME3) Assegurar a Conformidade Regulamentar	Q3
ME3.3) Avaliação da Conformidade com os Requisitos Regulamentares	Q2
ME4.6) Medição do Desempenho	Q2

Tabela 7.25 – Controlos da norma COBIT *versus* Questões de partida

Generally Accepted Information Security Principles (GAISP)	
Controlo [GAISP 2003]	Questão
2.1) Princípio da Responsabilidade	Q1
2.2) Princípio da Sensibilização	Q3
2.3) Princípio da Ética	Q1
2.4) Princípio da Multidisciplinaridade	Q3
2.8) Princípio da Valorização	Q2
3.1) Política de Segurança da Informação	Q1, Q3
3.2) Educação e Sensibilização	Q3
3.3) Responsabilização	Q1
3.5) Qualificações do Pessoal	Q1
3.6) Qualificações do Pessoal	Q3
3.9) Controlo de Acessos	Q1
3.13) Requisitos Legais, Regulamentares e Contratuais da Segurança da informação	Q3
3.14) Práticas Éticas	Q1

Tabela 7.26 – Controlos da norma GAISP *versus* Questões de partida

OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security	
Controlo [OECD 2002]	Questão
1) Sensibilização	Q3
2) Responsabilidade	Q1, Q3
4) Ética	Q1
9) Reavaliação	Q2

Tabela 7.27 – Controlos da norma OECD *versus* Questões de partida

Information Systems Security Assessment Framework (ISSAF)	
Controlo [ISSAF 2005]	Questão
3.2.2) Valorização dos Controlos	Q2
7) Política de Segurança da Informação Organizacional	Q1
7.5.6) Para os Utilizadores Finais	Q1
7.5.9) Para a Segurança da Informação	Q3
8.5.2) Segregação de Deveres	Q1
9.1) Segurança do Pessoal	Q1
10.2.5) Treino dos Funcionários	Q3
12.1.3) Benefícios da Gestão da Mudança	Q3
12.1.5) Definição do sucesso	Q3
12.1.7) Pré-requisitos	Q3
12.1.9) A <i>Framework</i>	Q3
12.1.11) Psicologia da Mudança	Q3
12.2.1.7) Definir Papéis e Responsabilidades	Q1
12.2.2) Fase 2 – Gerir a Mudança	Q3
12.2.3) Fase 3 – Reforçar a Gestão das Mudanças	Q3
12.2.4) Métricas e Relatórios	Q2
13.1) Metodologia para o Programa de Sensibilização de Segurança	Q3
13.2) Serviços de Sensibilização e Ferramentas de Aviso	Q3

Tabela 7.28 – Controlos da norma ISSAF *versus* Questões de partida

The Standard of Good Practice for Information Security	
Controlo [ISF 2005]	Questão
SM.1.1) Compromisso da Gestão	Q1
SM.1.2) Política de Segurança	Q1
SM.1.3) Acordos de Segurança	Q1
SM.2.4) Sensibilização de Segurança	Q3
SM.2.5) Educação de Segurança	Q3
SM.3.1) Classificação da Segurança	Q3
SM.3.2) Posse (<i>Ownership</i>)	Q1
SM.4.3) Gestão de Activos	Q2
SM.7.1) Auditoria/Revisão de Segurança	Q2
SM.7.2) Monitorização da Segurança	Q2
CB.2.1) Papéis e Responsabilidades	Q1
CB.2.2) Controlo das Aplicações	Q3
CB.2.3) Gestão de Alterações	Q3
CB.3.2) Processo de <i>Sign-on</i>	Q2
CB.3.4) Sensibilização para a Segurança	Q3
CB.5.4) Auditoria/Revisão da Segurança	Q2
CI.1.1) Papéis e Responsabilidades	Q1
CI.1.3) Gestão de Activos	Q2
CI.1.4) Monitorização do Sistema	Q2
CI.3.3) Gestão de Alterações	Q3
CI.4.1) Disposições de Controlo de Acessos	Q1
CI.4.2) Autorização de Utilizadores	Q1
CI.4.3) Privilégios de Acesso	Q1
CI.4.4) Processo de <i>Sign-on</i>	Q1
CI.4.5) Autenticação de Utilizadores	Q1
CI.5.2) Sensibilização de Segurança	Q3
CI.5.5) Auditoria/Revisão de Segurança	Q2
NW.1.1) Papéis e Responsabilidades	Q1
NW.3.2) Gestão de Alterações	Q3
NW.4.2) Sensibilização de Segurança	Q3
NW.4.3) Classificação da Segurança	Q3
NW.4.5) Auditoria/Revisão de Segurança	Q2
SD.1.1) Papéis e Responsabilidades	Q1
SD.2.2) Sensibilização de Segurança	Q3
SD.2.3) Auditoria/Revisão de Segurança	Q2
SD.3.1) Especificação de Requisitos	Q3
SD.5) Teste	Q2
SD.5.2) Testar a Aceitação	Q3
SD.6.3) Revisão Após-implementação	Q2

Tabela 7.29 – Controlos da norma the Standard *versus* Questões de partida

Pela análise directa das tabelas anteriores, é possível referenciar de imediato um conjunto mais restrito, com o qual continua a ser possível obter os controlos capazes de proporcionar as respostas necessárias, pelo que, neste contexto, considerando apenas este núcleo central, é possível proceder a uma especificação mais estreita das normas fundamentais que respondem a todas as questões colocadas.

7.2.2. Contributos das Normas

Neste contexto, vão apenas ser utilizados controlos obtidos do que se referenciou como núcleo central do normativo estudado. Tendo em consideração estes princípios, procedeu-se à identificação dos controlos derivados das normas e que foram percebidos como pertinentes para este contexto, particularmente pela sua capacidade de em conjunto suportar a elaboração das respostas às questões de partida, nomeadamente:

- ⇒ Questão 1 (*Qual a percepção dos utilizadores acerca da segurança da informação existente no SI? – Q1*);
- ⇒ Questão 2 (*Que indicadores possibilitam a avaliação da segurança de um SI e a avaliação de um SGSI? – Q2*);
- ⇒ Questão 3 (*Como são aceites pelas pessoas as mudanças tecnológicas e organizacionais motivadas pela implementação do SGSI? – Q3*).

Os controlos mencionados são apresentados nas tabelas seguintes, agrupando-se em referenciais de acordo com a sua afinidade. Nestas tabelas mencionam-se as normas de onde cada um dos controlos foi obtido e as questões a cada referencial permite responder.

Aceitação do SI e/ou do SGSI (Q3)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	10.3.2) Aceitação do Sistema
<i>NIST SP800-12</i>	13.1) Comportamento 13.2) Responsabilização
<i>the Standard</i>	SD.5.2) Testar a Aceitação
<i>OECD</i>	2) Responsabilidade
<i>COBIT</i>	AI.7.7) Teste de Aceitação Final

Tabela 7.30 – Controlos para o referencial α ‘Aceitação do SI e/ou do SGSI’

Documentos das Políticas de Segurança (Q1, Q3)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	5.1.1) Documento da Política de Segurança da Informação 10.1.1) Documentação dos Procedimentos Operativos
<i>BS ISO/IEC 27001:2005</i>	4.3) Requisitos de Documentação
<i>NIST SP800-12</i>	14.6) Documentação
<i>NIST SP800-14</i>	3.1) Política
<i>NIST SP800-18</i>	5.MA.7) Documentação 5.GSS.7) Documentação
<i>the Standard</i>	SM.1.2) Política de Segurança
<i>COBIT</i>	AI6.5) Documentação e Finalização das Alterações
<i>ISSAF</i>	7) Política de Segurança da Informação Organizacional

Tabela 7.31 – Controlos para o referencial α ‘Documentos das Políticas de Segurança’

Avaliação e Auditorias (Q2)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	10.10.1) Registos de Auditoria 10.10.3) Protecção da Informação dos Registos 10.10.4) Registos do Administrador e do Operador 10.10.5) Registo de Falhas 10.10.6) Sincronização do Relógio 15.3) Considerações de Auditoria de Sistemas de Informação
<i>BS ISO/IEC 27001:2005</i>	4.3.3) Controlo dos Registos 6) Auditorias Internas ao SGSI 8.1) Melhoramentos Contínuos
<i>ISO/IEC 21827:2002</i>	7.8.2) BP.08.01 - Analisar os Registos dos Eventos 7.11) PA.11 - Verificar e Validar a Segurança
<i>NIST SP800-12</i>	9.4.1) Ferramentas e Métodos de Auditoria
<i>NIST SP800-14</i>	3.13.1) Conteúdos dos Registos de Seguimento das Auditorias 3.13.2) Segurança do Seguimento das Auditorias 3.13.3) Revisão do Seguimento das Auditorias
<i>NIST SP800-18</i>	6.MA.4) Seguimento de Auditorias 6.GSS.3) Seguimento de Auditorias
<i>the Standard</i>	SM.7.1) Auditoria/Revisão de Segurança CB.5.4) Auditoria/Revisão da Segurança CI.5.5) Auditoria/Revisão de Segurança NW.4.5) Auditoria/Revisão de Segurança SD.2.3) Auditoria/Revisão de Segurança
<i>COBIT</i>	ME.3.3) Avaliação da Conformidade com os Requisitos Regulamentares

Tabela 7.32 – Controlos para o referencial α ‘Avaliação e Auditorias’

Gestão de Acessos (Q1)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	11.1.1) Política de Controlo de Acessos 11.2.1) Registo dos Utilizadores 11.2.2) Gestão dos Privilégios 11.2.3) Gestão das <i>Passwords</i> dos Utilizadores 11.2.4) Revisão dos Direitos de Acessos dos Utilizadores
<i>NIST SP800-12</i>	10.2) Gestão de Utilizadores 17.1) Critérios de Acesso 17.3.1) Controlos de Acessos Internos 17.3.2) Controlos de Acesso Externos 17.4) Gestão dos Controlos de Acessos
<i>NIST SP800-14</i>	3.5.2) Administração dos Utilizadores 3.12.1) Critério de Acesso 3.12.2) Mecanismos de Controlo de Acessos
<i>the Standard</i>	CI.4.1) Disposições de Controlo de Acessos CI.4.2) Autorização de Utilizadores CI.4.3) Privilégios de Acesso
<i>GAISP</i>	3.9) Controlo de Acessos

Tabela 7.33 – Controlos para o referencial α ‘Gestão de Acessos’

Gestão dos Activos (Q1, Q2, Q3)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	6.1.4) Processo de Autorização das Facilidades de Processamento da Informação 7.1.1) Inventário dos Activos 7.1.2) Posse dos Activos 7.1.3) Utilização Aceitável dos Activos 7.2.1) Directrizes de Classificação da Informação 7.2.2) Identificação e Manipulação da Informação 11.3.1) Uso das <i>passwords</i> 11.3.2) Utilizadores de Equipamentos sem Vigilância 11.3.3) Políticas de Limpeza das Secretárias e dos Ecrãs 11.5.5) Limites do Tempo da Sessão 11.5.6) Limitação do Tempo de Ligação
<i>BS ISO/IEC 27001:2005</i>	4.2.2) Implementar e Operar o SGSI
<i>ISO/IEC 21827:2002</i>	7.2.3) BP.02.02 - Identificar os Activos do Sistema
<i>NIST SP800-12</i>	16) Identificação e Autenticação
<i>NIST SP800-14</i>	3.11.1) Identificação 3.11.2) Autenticação 3.11.3) <i>Passwords</i> 3.11.4) Autenticação Avançada
<i>NIST SP800-18</i>	6.MA.1) Identificação e Autenticação 6.GSS.1) Identificação e Autenticação
<i>the Standard</i>	SM.4.3) Gestão de Activos CB.2.2) Controlo das Aplicações CB.3.2) Processo de <i>Sign-on</i> das Aplicações CI.1.3) Gestão de Activos CI.4.4) Processo de <i>Sign-on</i> CI.4.5) Autenticação de Utilizadores
<i>COBIT</i>	DS.5.3) Gestão de Identidades

Tabela 7.34 – Controlos para o referencial α ‘Gestão dos Activos’

Leis, Regulamentos e Políticas (Q3)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	15.1.1) Identificação da Legislação Aplicável
<i>ISO/IEC 21827:2002</i>	7.10.3) BP.10.02 - Identificar Leis, Políticas e Constrangimentos Aplicáveis
<i>NIST SP800-18</i>	3.7.1) Leis, Regulamentos e Políticas que Afectam o Sistema
<i>COBIT</i>	ME.3) Assegurar a Conformidade Regulamentar
<i>GAISP</i>	3.13) Requisitos Legais, Regulamentares e Contratuais da Segurança da Informação

Tabela 7.35 – Controlos para o referencial α ‘Leis, Regulamentos e Políticas’

Métricas e Testes (Q2)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	5.1) Política de Segurança da Informação 7.2) Classificação da Informação 10.10.6) Sincronização do Relógio
<i>BS ISO/IEC 27001:2005</i>	4.2.2) Implementar e Operar o SGSI 4.2.3) Monitorizar e Rever o SGSI
<i>ISO/IEC 21827:2002</i>	7.2.4) BP.02.03 - Selecionar Métrica(s) de Impacto 7.2.5) BP.02.04 - Identificar Relacionamentos entre Métricas
<i>NIST SP800-12</i>	9.3.1) Teste e Certificação
<i>the Standard</i>	SD.5) Teste
<i>COBIT</i>	ME.1.4) Valorização do Desempenho ME.4.6) Medição do Desempenho
<i>GAISP</i>	2.8) Princípio da Valorização
<i>ISSAF</i>	3.2.2) Valorização dos Controlos 12.2.4) Métricas e Relatórios

Tabela 7.36 – Controlos para o referencial α ‘Métricas e Testes’

Monitorização e Revisão da Segurança da Informação e/ou do SGSI (Q2)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	5.1.2) Revisão da Política de Segurança da Informação 10.2.2) Monitorização e Revisão de Serviços de Terceiros 10.10.2) Monitorização da Utilização do Sistema
<i>BS ISO/IEC 27001:2005</i>	4.2.3) Monitorizar e Rever o SGSI 5.1) Comprometimento da Gestão 5.2.1) Disponibilização de Recursos 7.2) <i>Inputs</i> para o processo de revisão
<i>ISO/IEC 21827:2002</i>	7.8.3) BP.08.02 - Monitorizar Alterações 7.8.5) BP.08.04 - Monitorizar Salvaguardas de Segurança 7.8.6) BP.08.05 - Revisão da Postura de Segurança
<i>NIST SP800-12</i>	9.4.2) Ferramentas e Métodos de Monitorização
<i>NIST SP800-14</i>	3.13.4) Monitorização do Uso do Teclado
<i>NIST SP800-18</i>	4.2) Revisão dos Controlos de Segurança
<i>the Standard</i>	SM.7.1) Auditoria/Revisão de Segurança SM.7.2) Monitorização da Segurança CB.5.4) Auditoria/Revisão da Segurança CI.1.4) Monitorização do Sistema CI.5.5) Auditoria/Revisão de Segurança NW.4.5) Auditoria/Revisão de Segurança SD.2.3) Auditoria/Revisão de Segurança SD.6.3) Revisão Após-implementação
<i>OECD</i>	9) Reavaliação
<i>COBIT</i>	ME.1.1) Abordagem da Monitorização ME.1.2) Definição e Recolha dos Dados da Monitorização ME.1.3) Método de Monitorização DS.3.5) Monitorização e Reporte DS.9.3) Revisão da Integridade da Configuração

Tabela 7.37 – Controlos para o referencial α ‘Monitorização e Revisão da Segurança da Informação e/ou do SGSI’

Mudanças no SI e/ou no SGSI (Q3)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	10.1.2) Gestão das Alterações 12.5.1) Procedimentos de Controlo das Alterações 12.5.2) Revisão Técnica das Aplicações após Mudanças do Sistema Operativo 12.5.3) Restrições nas Mudanças aos Pacotes de <i>Software</i>
<i>BS ISO/IEC 27001:2005</i>	8.1) Melhoramentos Continuados
<i>ISO/IEC 21827:2002</i>	7.8.6) BP.08.05 - Postura da Política de Segurança
<i>the Standard</i>	CB.2.3) Gestão de Alterações CI.3.3) Gestão de Alterações NW.3.2) Gestão de Alterações
<i>COBIT</i>	AI6) Gerir as Alterações
<i>ISSAF</i>	12.1.3) Benefícios da Gestão da Mudança 12.1.5) Definição do Sucesso 12.1.7) Pré-requisitos 12.1.9) A <i>Framework</i> 12.1.11) Psicologia da Mudança 12.2.2) Fase 2 - Gerir a Mudança 12.2.3) Fase 3 - Reforçar a Gestão das Mudanças

Tabela 7.38 – Controlos para o referencial α ‘Mudanças no SI e/ou no SGSI’

Política de Segurança da Informação (Q1, Q2, Q3)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	5.1) Política de Segurança da Informação 5.1.1) Documento da Política de Segurança da Informação 6.1.1) Compromisso da Gestão com a Segurança da Informação 6.1.2) Coordenação da Segurança da Informação 6.1.5) Compromisso de Confidencialidade 7.2) Classificação da Informação 12.1.1) Análise e Especificação dos Requisitos de Segurança
<i>BS ISO/IEC 27001:2005</i>	4.2.1) Estabelecer o SGSI 5.1) Compromisso por Parte da Gestão 7.8.6) BP.08.05 – Revisão da Postura de Segurança 7.10.4) BP.10.03 - Identificar o Contexto de Segurança do Sistema
<i>NIST SP800-12</i>	2) Elementos da Segurança de Computadores 5.1.1) Componentes Básicos da Política do Programa 8.4.2.1) Determinação dos Requisitos de Segurança
<i>NIST SP800-14</i>	3.1) Política 3.9) Considerações de Segurança nas Operações e Suporte de Computadores
<i>the Standard</i>	SM.1.1) Compromisso da Gestão SM.1.2) Política de Segurança SM.3.1) Classificação da Segurança NW.4.3) Classificação da Segurança SD3.1) Especificação de Requisitos
<i>GAISP</i>	2.4) Princípio da Multidisciplinaridade 3.1) Política de Segurança da Informação
<i>ISSAF</i>	7) Política de Segurança da Informação Organizacional 7.5.9) Para a Segurança da Informação

Tabela 7.39 – Controlos para o referencial α ‘Política de Segurança da Informação’

Responsabilidades, Papéis e Obrigações do Pessoal (Q1)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	6.1.3) Alocação das Responsabilidades da Segurança da Informação 6.1.5) Compromisso de Confidencialidade 8.1) Antes do Contracto 8.1.1) Papéis e Obrigações 8.2) Durante o Contracto 8.3) Finalização ou Alteração do Contracto 10.1.3) Separação dos Deveres 10.3.1) Gestão das Capacidades 11.2.1) Registo dos Utilizadores 11.3.2) Utilizadores de Equipamentos sem Vigilância
<i>BS ISO/IEC 27001:2005</i>	5.1) Compromisso por Parte da Gestão
<i>ISO/IEC 21827:2002</i>	7.1.2) BP.01.01 - Estabelecer Obrigações de Segurança
<i>NIST SP800-12</i>	3.6) Utilizadores 5.3.2) Regras de Segurança Operacional 10) Problemas de Pessoal/Utilizadores 10.1) Colocação do Pessoal 14.1) Suporte aos Utilizadores
<i>NIST SP800-14</i>	3.5) Problemas de Pessoal/Utilizadores 3.5.1) Pessoal
<i>NIST SP800-18</i>	3.2.4) Atribuição das Obrigações de Segurança 5.MA.1) Segurança do Pessoal 5.GSS.1) Controlo do Pessoal
<i>the Standard</i>	SM.1.3) Acordos de Pessoal SM.3.2) Posse (<i>Ownership</i>) CB.2.1) Papéis e Responsabilidades CI.1.1) Papéis e Responsabilidades NW.1.1) Papéis e Responsabilidades SD.1.1) Papéis e Responsabilidades
<i>OECD</i>	2) Responsabilidade 4) Ética
<i>COBIT</i>	PO4.6) Papéis e Responsabilidades PO4.11) Segregação de Deveres PO7.2) Competências do Pessoal PO7.3) Atribuição dos Papéis
<i>GAISP</i>	2.1) Princípio da Responsabilidade 2.3) Princípio da Ética 3.5) Qualificações do Pessoal 3.14) Práticas Éticas
<i>ISSAF</i>	7.5.6) Para os Utilizadores Finais 8.5.2) Segregação de Deveres 9.1) Segurança do Pessoal 12.2.1.7) Definir Papéis e Responsabilidades

Tabela 7.40 – Controlos para o referencial α ‘Responsabilidades, Papéis e Obrigações do Pessoal’

Sensibilização, Treino e Educação (Q3)	
Norma	Controlos
<i>BS ISO/IEC 17799:2005</i>	8.2.2) Treino, Educação e Sensibilização sobre Segurança da Informação
<i>BS ISO/IEC 27001:2005</i>	5.2.2) Treino, Sensibilização e Competência
<i>ISO/IEC 21827:2002</i>	7.1.4) BP.01.03 - Gerir os Programas de Sensibilização, Treino e Educação de Segurança
<i>NIST SP800-12</i>	10.1.4) Sensibilização e Treino dos Funcionários 13.3) Sensibilização 13.4) Treino 13.5) Educação
<i>NIST SP800-14</i>	3.8) Sensibilização e Treino
<i>NIST SP800-18</i>	5.MA.8) Sensibilização e Treino de Segurança 5.GSS.8) Sensibilização e Treino de Segurança
<i>the Standard</i>	SM.2.4) Sensibilização de Segurança SM.2.5) Educação de Segurança CB.3.4) Sensibilização para a Segurança CI.5.2) Sensibilização de Segurança NW.4.2) Sensibilização de Segurança SD.2.2) Sensibilização de Segurança
<i>OECD</i>	1) Sensibilização
<i>COBIT</i>	PO7.4) Treino Personalizado DS7.1) Identificação das Necessidades de Educação e Treino DS7.2) Entrega da Educação e Treino DS7.3) Avaliação do Treino Recebido
<i>GAISP</i>	2.2) Princípio da Sensibilização 3.2) Educação e Sensibilização 3.6) Qualificações do Pessoal
<i>ISSAF</i>	10.2.5) Treino dos Funcionários 13.1) Metodologia para o Programa de Sensibilização de Segurança 13.2) Serviços de Sensibilização e Ferramentas de Aviso

Tabela 7.41 – Controlos para o referencial α ‘Sensibilização, Treino e Educação’

Os referenciais especificados foram posteriormente agrupados, mencionando as normas a que correspondem, para enquadrar a resposta à principal questão colocada no trabalho, *Qual o impacto na actividade das pessoas quando se implementa um SGSI?*. Estes resultados constam da tabela seguinte.

Os referenciais constantes da tabela seguinte, mencionados como Referenciais Alfa (α) vão ser utilizados para o desenvolvimento do Modelo.

Questão: Qual o impacto na actividade das pessoas quando se implementa um SGSI?	
Referenciais Alfa (α)	Normas
<i>$\alpha 1$ – Aceitação do SI e/ou do SGSI</i>	BS ISO/IEC 17799:2005, NIST SP800-12, the Standard, OECD, COBIT
<i>$\alpha 2$ – Avaliação e Auditorias</i>	BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, ISO/IEC 21827:2002, NIST SP800-12, NIST SP800-14, NIST SP800-18, the Standard, COBIT
<i>$\alpha 3$ – Documentos das Políticas de Segurança da Informação</i>	BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, NIST SP800-12, NIST SP800-14, NIST SP800-18, the Standard, COBIT, ISSAF
<i>$\alpha 4$ – Gestão de Acessos</i>	BS ISO/IEC 17799:2005, NIST SP800-12, NIST SP800-14, the Standard, GAISP
<i>$\alpha 5$ – Gestão dos Activos</i>	BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, ISO/IEC 21827:2002, NIST SP800-12, NIST SP800-14, NIST SP800-18, the Standard, COBIT
<i>$\alpha 6$ – Leis, Regulamentos e Políticas</i>	BS ISO/IEC 17799:2005, ISO/IEC 21827:2002, NIST SP800-18, COBIT, GAISP
<i>$\alpha 7$ – Métricas e Testes</i>	BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, ISO/IEC 21827:2002, NIST SP800-12, the Standard, COBIT, GAISP, ISSAF
<i>$\alpha 8$ – Monitorização e Revisão da Segurança da Informação e/ou do SGSI</i>	BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, ISO/IEC 21827:2002, NIST SP800-12, NIST SP800-14, NIST SP800-18, the Standard, OECD, COBIT
<i>$\alpha 9$ – Mudanças no SI e/ou no SGSI</i>	BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, ISO/IEC 21827:2002, the Standard, COBIT, ISSAF
<i>$\alpha 10$ – Política de Segurança da Informação</i>	BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, NIST SP800-12, NIST SP800-14, the Standard, GAISP, ISSAF
<i>$\alpha 11$ – Responsabilidades, Papéis e Obrigações do Pessoal</i>	BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, ISO/IEC 21827:2002, NIST SP800-12, NIST SP800-14, NIST SP800-18, the Standard, OECD, COBIT, GAISP, ISSAF
<i>$\alpha 12$ – Sensibilização, Treino e Educação</i>	BS ISO/IEC 17799:2005, BS ISO/IEC 27001:2005, ISO/IEC 21827:2002, NIST SP800-12, NIST SP800-14, NIST SP800-18, the Standard, OECD, COBIT, GAISP, ISSAF

Tabela 7.42 – Referenciais α para resposta à principal questão do trabalho

7.2.3. Modelo PDCA

Conjuntamente com o modelo SDLC deve ser aplicado o modelo PDCA, que é utilizado nas normas ISO/IEC 17799 [ISO 2005a] e ISO/IEC 27001 [ISO 2005b], modelo este que foi desenvolvido no âmbito dos processos de qualidade, até porque as normas referidas impõem que se tenha em consideração, na sua implementação, outro normativo implementado na organização, como por exemplo o ISO 9001 ou o ISO 14001.

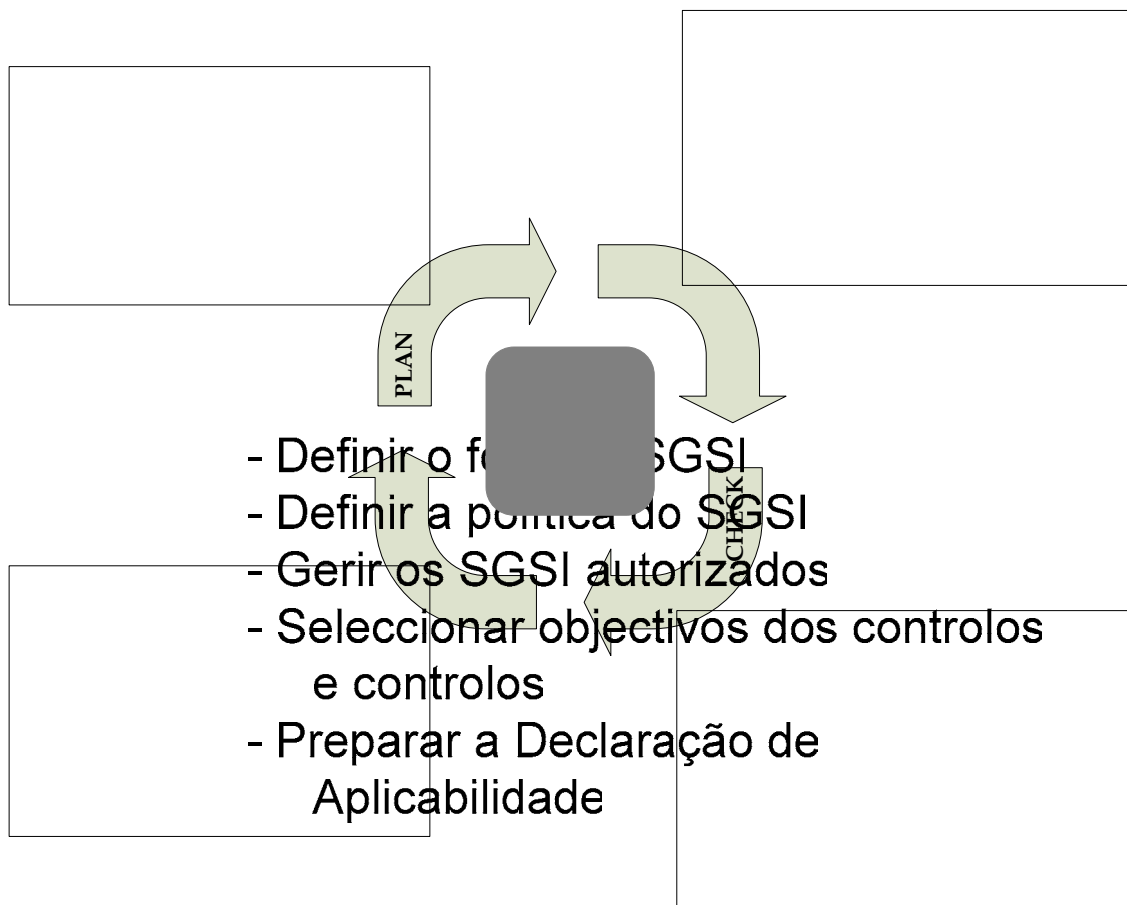


Figura 7.4 – Modelo PDCA
(adaptado de ISO [2005b])

7.3. Modelo

Nesta contextualização, as Pessoas devem conhecer o ambiente e a cultura local e organizacional com que interagem, respeitando as leis e regulamentos aplicáveis, assim como o normativo específico aplicável a alguns sectores de actividade. Acresce aqui que a divulgação dos documentos relevantes por todos os envolvidos na utilização do SI e das TIC onde foram implementados os SGSI, deve ser assumida como uma obrigatoriedade.

- Implementar as melhorias

ACT

7.3.1. Base de Desenvolvimento

No sentido de suportar a concepção da base de desenvolvimento do Modelo, estabelecem-se tabelas comparativas entre os principais aspectos abrangidos pelo PDCA e pelo SDLC, enquadrando as respectivas fases de desenvolvimento em função dos tópicos interrelacionados entre cada uma das fases desses modelos.

- Tomar as acções correctivas/preventivas

- Comunicar os resultados a todas as partes interessadas

- Assegurar que os objectivos de melhoria são atingidos

Utilizando estas tabelas como referência, procede-se ao estabelecimento da base de desenvolvimento do Modelo, considerando também os tópicos identificados como relevantes, tópicos estes que resultam dos contributos proporcionados pela análise dos resultados do questionário.

PDCA [ISO 2005b]		SDLC [Grance <i>et al</i> 2003]	
Plan	– Definir o foco do SGSI – Definir a política do SGSI – Gerir os SGSI autorizados – Seleccionar objectivos dos controlos e controlos – Preparar a Declaração de Aplicabilidade	– Categorização da segurança	Iniciação

Tabela 7.43 – PDCA-Plan *versus* SDLC-Iniciação

PDCA [ISO 2005b]		SDLC [Grance <i>et al</i> 2003]	
Do	– Implementar controlos – Implementar programas de sensibilização e treino – Gerir as operações – Gerir os recursos – Implementar procedimentos para detectar/responder a incidentes de segurança	– Análise dos Requisitos do Nível de Conforto da Segurança – Planeamento da Segurança – Desenvolvimento dos Controlos de Segurança – Avaliação dos Testes de Segurança Desenvolvidos – Outros Componentes do Planeamento	Desenvolvimento

Tabela 7.44 – PDCA-Do *versus* SDLC-Desenvolvimento

PDCA [ISO 2005b]		SDLC [Grance <i>et al</i> 2003]	
Check	– Executar os procedimentos de monitorização – Assumir revisões regulares da eficácia do SGSI – Medir a eficácia dos controlos – Conduzir auditorias internas ao SGSI – Revisão regular pela Gestão – Actualizar planos de segurança – Registar acções e eventos	– Inspeção e Aceitação – Integração dos Controlos de Segurança – Certificação de Segurança – Acreditação da Segurança	Implementação

Tabela 7.45 – PDCA-Check *versus* SDLC-Implementação

PDCA [ISO 2005b]		SDLC [Grance <i>et al</i> 2003]	
Act	– Implementar as melhorias identificadas – Tomar as acções correctivas/preventivas – Comunicar os resultados a todas as partes interessadas – Assegurar que os objectivos de melhoria são atingidos	– Gestão da Configuração e Controlo – Monitorização	Operação e Manutenção

Tabela 7.46 – PDCA-Act *versus* SDLC-Operação e Manutenção

7.3.2. Características do Modelo

A elaboração dos fundamentos de suporte ao desenvolvimento do Modelo de requisitos para a implementação do SGSI foi efectuada tomando em consideração um conjunto de duas etapas prévias, cuja explanação se apresenta seguidamente.

A primeira etapa consistiu no desenvolvimento de um modelo de interacção das normas estudadas, visando a identificação de um conjunto mais reduzido e apropriado de normas de modo a cumprir os seus objectivos.

A segunda etapa proporcionou a identificação de referenciais, utilizando a revisão bibliográfica, o estudo das normas e de métricas, que permitindo a resposta às questões de partida, possibilitam a especificação dos impactos dos SGSI nas Pessoas.

Após a concretização das etapas referidas serão utilizados os modelos SDLC e PDCA, para possibilitar a definição de uma base de desenvolvimento do Modelo.

Atendendo à pertinência, anteriormente justificada, de assegurar que as políticas de segurança e os SGSI sejam incluídas nas actividades de planeamento, desenvolvimento e implementação dos SI, a utilização conjugada dos modelos SDLC e PDCA pode constituir uma vantagem a não descurar, em especial se considerarmos a sua adequação à problemática da segurança.

Na sequência do que foi especificado anteriormente, e após a elaboração da base de desenvolvimento do Modelo, incluindo os principais tópicos a considerar na sua especificação, procede-se à construção do próprio Modelo, utilizando os contributos proporcionados pelas etapas anteriores.

Deste modo, entende-se o Modelo como uma estrutura envolvendo quatro grandes áreas que se relacionam simultaneamente com os SI e com os SGSI. As referidas áreas são as seguintes:

- (1) Iniciação e Planeamento;
- (2) Concepção e Desenvolvimento;
- (3) Implementação e Teste;
- (4) Operação, Manutenção e Optimização.



Figura 7.5 – Base do MIDImOS

Neste contexto, o Modelo designar-se-à como Modelo de Iniciação, Desenvolvimento, Implementação e Optimização da Segurança (MIDIImOS), cuja base se apresenta na figura anterior.

7.3.3. Modelo Conceptual

De acordo com o já mencionado, a concepção do Modelo suportar-se-à nos referenciais anteriormente especificadas, no modelo PDCA e no modelo SDLC, e na interacção de duas tríades que permitem o enquadramento da segurança da informação.

Estas visões da segurança da informação associadas às referidas tríades são especificadas no capítulo 4 (Segurança da Informação), com os seus esquemas apresentados nas figuras 4.1 (Desafio da segurança da informação) e 4.2 (Envolventes da segurança da informação).

A primeira destas visões é apresentada por Pfleeger and Pfleeger [2003] que referem a necessidade de encontrar um balanceamento correcto entre confidencialidade, integridade e disponibilidade, pois apenas assim consideram que é possível atingir a segurança da informação. A outra visão acerca da segurança da informação, com os mesmos objectivos mas baseada em pressupostos bem diferentes, é apresentada por Fenton and Wolfe [2003] como o resultado da interacção entre Pessoas, TIC e processos.

Do enquadramento teórico propiciado neste trabalho, quando se procede à definição do que se entende por segurança da informação, os aspectos que surgem referenciados com maior frequência, constituindo aliás uma recorrência no âmbito das normas BS e ISO, são a confidencialidade, a integridade e a disponibilidade (referenciado no diverso normativo, considerando a sua língua de origem, como CIA – *Confidentiality, Integrity, Availability*).

Perante esta constatação, torna-se interessante verificar que a definição de qualquer destes aspectos base que enquadram a segurança da informação, têm como fundação as Pessoas e as suas actividades relacionadas com a informação, nomeadamente: acesso, modificação, autorização.

Por outro lado, outra das constituintes do Modelo considera três componentes que condicionam a segurança da informação, a actividade das organizações e o

enquadramento da Sociedade da Informação. Estas três componentes correspondem às Pessoas, às TIC e aos Processos.

Refira-se ainda que o Modelo conceptual, como referência essencial para visualização das áreas abrangidas, é apresentado em termos latos na figura 7.6.

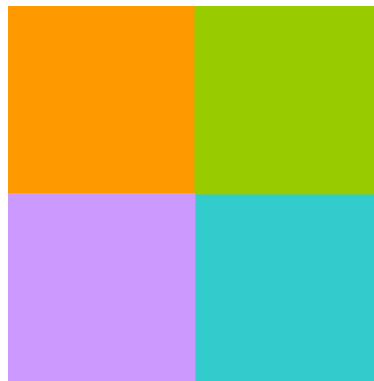


Figura 7.6 – Esquema conceptual do MIDImOS

A especificação do MIDImOS é realizada considerando as suas quatro componentes isoladamente com os respectivos referenciais associados, de acordo com o que foi anterior definido.

Qualquer das quatro componentes que isoladamente se apresentam nas figuras seguintes enquadram os referenciais *alfa*, *beta* e *gamma*, nas interacções existentes entre confidencialidade, integridade e disponibilidade por um lado, e Pessoas, TIC e processos pelo outro, procurando proporcionar uma visão mais abrangente das referidas interacções.

A componente do MIDImOS (Iniciação e Planeamento) que se apresenta na figura seguinte, relaciona-se directamente com o estabelecimento do SGSI, considerando-se também integrada nesta componente a correspondente etapa do SDLC, que compreende a definição de necessidades, a identificação das Pessoas envolvidas no processo de decisão, e os objectivos genéricos [Alter 1998, Grance *et al* 2003, ISO 2005b].

**Iniciação e
Planeamento**

**Implementação e
Teste**

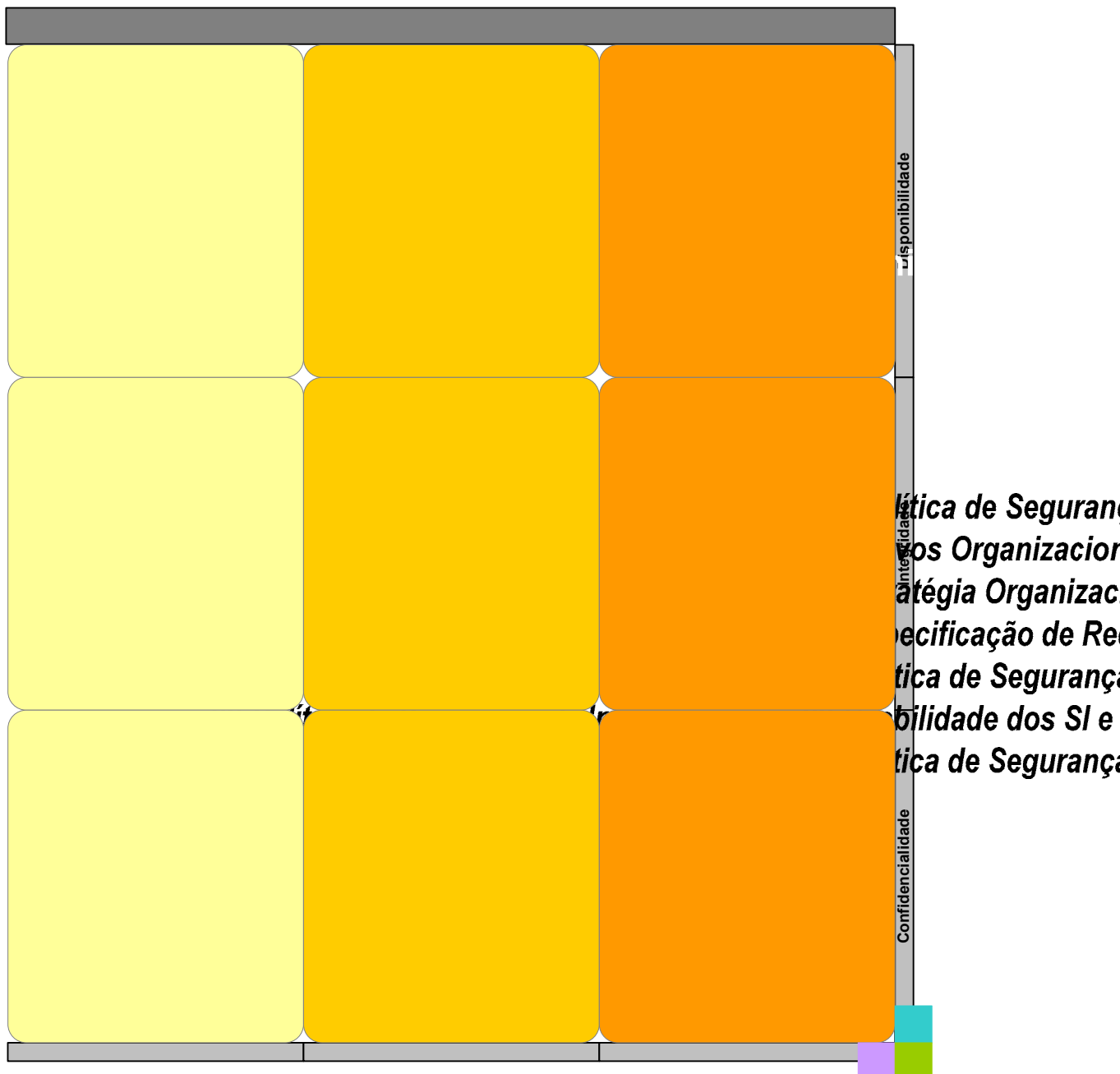


Figura 7.7 – MIDImOS - Iniciação e Planeamento

Já a componente seguinte do MIDIMQS (Conceção e Desenvolvimento), relaciona-se directamente com a implementação da componente de SGSI, considerando-se totalmente integrada nesta componente de concessão da informação e com o processo de construção ou aquisição da estratégia organizacional de acordo com as necessidades de desempenho das funções organizacionais (Grance *et al.* 1998, Grance *et al.* 2005b).

3 Documentos das Políticas de Segurança da Informação

10 Política de Segurança da Informação

85 Estrategia Organizacional e

Especificação de Requisitos

β8 Política de Segurança da Informação

y5 Política de Segurança da Informação

α10 Política de Segurança

05 Estratégia Organizac

Especificação de Re

Política de Segurança

y5 Política de Segurança

Concepção e Desenvolvimento			
Disponibilidade Integridade Confidencialidade	α10 Política de Segurança da Informação α11 Responsabilidades, Papéis e Obrigações do Pessoal β8 Política de Segurança da Informação γ5 Política de Segurança da Informação	α10 Política de Segurança da Informação β8 Política de Segurança da Informação β9 Usabilidade dos SI e das TIC γ5 Política de Segurança da Informação	α10 Política de Segurança da Informação β8 Política de Segurança da Informação γ5 Política de Segurança da Informação
	α10 Política de Segurança da Informação α11 Responsabilidades, Papéis e Obrigações do Pessoal β8 Política de Segurança da Informação γ5 Política de Segurança da Informação	α10 Política de Segurança da Informação β8 Política de Segurança da Informação γ5 Política de Segurança da Informação	α10 Política de Segurança da Informação β8 Política de Segurança da Informação γ5 Política de Segurança da Informação
	α6 Leis, Regulamentos e Políticas α10 Política de Segurança da Informação α11 Responsabilidades, Papéis e Obrigações do Pessoal β8 Política de Segurança da Informação γ5 Política de Segurança da Informação	α6 Leis, Regulamentos e Políticas α10 Política de Segurança da Informação β1 Aceitação e Desempenho β2 Activos Organizacionais β8 Política de Segurança da Informação γ5 Política de Segurança da Informação	α6 Leis, Regulamentos e Políticas α10 Política de Segurança da Informação β2 Activos Organizacionais β8 Política de Segurança da Informação γ5 Política de Segurança da Informação
	Pessoas	TIC	Processos

Figura 7.8 – MIDImOS - Concepção e Desenvolvimento

Por outro lado, esta componente do MIDImOS (Implementação e Teste), diz respeito à monitorização e revisão do SGSI, considerando-se também integrada nesta componente a correspondente etapa do SDLC, que tem a ver com a de operacionalização do sistema na organização [Alter 1998, Grance *et al* 2003, ISO 2005b].

	Pessoas	TIC	Processos
Confidencialidade	α4 Gestão de Acessos α9 Mudanças no SI e/ou no SGSI α10 Política de Segurança da Informação α11 Responsabilidades, Papéis e Obrigações do Pessoal α12 Sensibilização, Treino e Educação β1 Aceitação e Desempenho β4 Envolvimento das Pessoas β6 Formação β7 Mudanças nos SI e/ou nas TIC β8 Política de Segurança da Informação γ3 Gestão de Acessos γ5 Política de Segurança da Informação γ6 Sensibilização, Treino e Educação	α4 Gestão de Acessos α9 Mudanças no SI e/ou no SGSI α10 Política de Segurança da Informação β4 Envolvimento das Pessoas β6 Formação β7 Mudanças nos SI e/ou nas TIC β8 Política de Segurança da Informação γ3 Gestão de Acessos γ5 Política de Segurança da Informação	α3 Documentos das Políticas de Segurança da Informação α4 Gestão de Acessos α7 Métricas e Testes α9 Mudanças no SI e/ou no SGSI α10 Política de Segurança da Informação β4 Envolvimento das Pessoas β7 Mudanças nos SI e/ou nas TIC β8 Política de Segurança da Informação γ2 Avaliação e Auditorias γ3 Gestão de Acessos γ5 Política de Segurança da Informação
Integridade	α4 Gestão de Acessos α9 Mudanças no SI e/ou no SGSI α10 Política de Segurança da Informação α11 Responsabilidades, Papéis e Obrigações do Pessoal α12 Sensibilização, Treino e Educação β8 Política de Segurança da Informação γ5 Política de Segurança da Informação γ6 Sensibilização, Treino e Educação	α4 Gestão de Acessos α9 Mudanças no SI e/ou no SGSI α10 Política de Segurança da Informação β8 Política de Segurança da Informação γ5 Política de Segurança da Informação	α3 Documentos das Políticas de Segurança da Informação α4 Gestão de Acessos α7 Métricas e Testes α9 Mudanças no SI e/ou no SGSI α10 Política de Segurança da Informação β8 Política de Segurança da Informação γ2 Avaliação e Auditorias γ5 Política de Segurança da Informação
Disponibilidade	α4 Gestão de Acessos α9 Mudanças no SI e/ou no SGSI α10 Política de Segurança da Informação α11 Responsabilidades, Papéis e Obrigações do Pessoal α12 Sensibilização, Treino e Educação β8 Política de Segurança da Informação γ5 Política de Segurança da Informação γ6 Sensibilização, Treino e Educação	α4 Gestão de Acessos α9 Mudanças no SI e/ou no SGSI α10 Política de Segurança da Informação β2 Activos Organizacionais β8 Política de Segurança da Informação β9 Usabilidade dos SI e das TIC	α3 Documentos das Políticas de Segurança da Informação α4 Gestão de Acessos α7 Métricas e Testes α9 Mudanças no SI e/ou no SGSI α10 Política de Segurança da Informação β8 Política de Segurança da Informação γ2 Avaliação e Auditorias γ5 Política de Segurança da Informação
Implementação e Teste			

Figura 7.9 – MIDImOS - Implementação e Teste

A última componente do MIDImOS (Operação, Manutenção e Optimização), que não o é por estarmos perante um Modelo de melhoria continuada, tem a ver com a manutenção e melhoria do SGSI, considerando-se também integrada nesta componente a correspondente etapa do SDLC, que tem a operação progressiva do sistema, procurando proceder à sua melhoria a à correcção dos erros detectados [Alter 1998, Grance *et al* 2003, ISO 2005b].

Processos	TIC	Pessoas	
α2 Avaliação e Auditorias α5 Gestão dos Activos α8 Monitorização e Revisão da Segurança da Informação e/ou do SGSI α10 Política de Segurança da Informação β3 Ameaças e Violações da Segurança β7 Mudanças nos SI e/ou nas TIC β8 Política de Segurança da Informação γ1 Ameaças e Violações da Segurança γ2 Avaliação e Auditorias γ4 Gestão de Activos γ5 Política de Segurança da Informação	α2 Avaliação e Auditorias α5 Gestão dos Activos α8 Monitorização e Revisão da Segurança da Informação e/ou do SGSI α10 Política de Segurança da Informação β1 Aceitação e Desempenho β2 Activos Organizacionais β3 Ameaças e Violações da Segurança β7 Mudanças nos SI e/ou nas TIC β8 Política de Segurança da Informação γ1 Ameaças e Violações da Segurança γ2 Avaliação e Auditorias γ4 Gestão de Activos γ5 Política de Segurança da Informação	α1 Aceitação do SI e/ou do SGSI α5 Gestão dos Activos α8 Monitorização e Revisão da Segurança da Informação e/ou do SGSI α10 Política de Segurança da Informação β1 Aceitação e Desempenho β3 Ameaças e Violações da Segurança β4 Envolvimento das Pessoas β6 Formação β7 Mudanças nos SI e/ou nas TIC β8 Política de Segurança da Informação γ1 Ameaças e Violações da Segurança γ2 Avaliação e Auditorias γ5 Política de Segurança da Informação γ7 Utilização dos Activos	Confidencialidade
α2 Avaliação e Auditorias α5 Gestão dos Activos α8 Monitorização e Revisão da Segurança da Informação e/ou do SGSI α10 Política de Segurança da Informação β3 Ameaças e Violações da Segurança β8 Política de Segurança da Informação γ1 Ameaças e Violações da Segurança γ2 Avaliação e Auditorias γ4 Gestão de Activos γ5 Política de Segurança da Informação	α2 Avaliação e Auditorias α5 Gestão dos Activos α8 Monitorização e Revisão da Segurança da Informação e/ou do SGSI α10 Política de Segurança da Informação β1 Aceitação e Desempenho β3 Ameaças e Violações da Segurança β8 Política de Segurança da Informação γ1 Ameaças e Violações da Segurança γ2 Avaliação e Auditorias γ4 Gestão de Activos γ5 Política de Segurança da Informação	α1 Aceitação do SI e/ou do SGSI α5 Gestão dos Activos α8 Monitorização e Revisão da Segurança da Informação e/ou do SGSI α10 Política de Segurança da Informação β1 Aceitação e Desempenho β4 Envolvimento das Pessoas β3 Ameaças e Violações da Segurança β6 Formação β8 Política de Segurança da Informação γ1 Ameaças e Violações da Segurança γ2 Avaliação e Auditorias γ5 Política de Segurança da Informação γ7 Utilização dos Activos	Integridade
α2 Avaliação e Auditorias α5 Gestão dos Activos α8 Monitorização e Revisão da Segurança da Informação e/ou do SGSI α10 Política de Segurança da Informação β3 Ameaças e Violações da Segurança β8 Política de Segurança da Informação γ1 Ameaças e Violações da Segurança γ2 Avaliação e Auditorias γ4 Gestão de Activos γ5 Política de Segurança da Informação	α2 Avaliação e Auditorias α5 Gestão dos Activos α8 Monitorização e Revisão da Segurança da Informação e/ou do SGSI α10 Política de Segurança da Informação β1 Aceitação e Desempenho β2 Activos Organizacionais β3 Ameaças e Violações da Segurança β4 Envolvimento das Pessoas β8 Política de Segurança da Informação β9 Usabilidade dos SI e das TIC γ1 Ameaças e Violações da Segurança γ2 Avaliação e Auditorias γ4 Gestão de Activos γ5 Política de Segurança da Informação	α1 Aceitação do SI e/ou do SGSI α5 Gestão dos Activos α8 Monitorização e Revisão da Segurança da Informação e/ou do SGSI α10 Política de Segurança da Informação β1 Aceitação e Desempenho β3 Ameaças e Violações da Segurança β4 Envolvimento das Pessoas β6 Formação β8 Política de Segurança da Informação β9 Usabilidade dos SI e das TIC γ1 Ameaças e Violações da Segurança γ2 Avaliação e Auditorias γ5 Política de Segurança da Informação γ7 Utilização dos Activos	Disponibilidade
Operação, Manutenção e Optimização			

Figura 7.10 – MIDImOS - Operação, Manutenção e Optimização

7.4. Exemplos de Métricas

Perante a abrangência proporcionada pelo MIDImOS, definem-se seguidamente exemplos de métricas relacionadas com os referenciais constantes nas diversas áreas do Modelo que se relacionam directamente com as Pessoas.

Iniciação e Planeamento

Exemplo 1: Nível de segurança da informação.

Exemplo 2: N.º de utilizadores que conhece o documento das políticas de segurança.

Exemplo 3: Grau de participação dos utilizadores na especificação de requisitos.

Concepção e Desenvolvimento

Exemplo 4: % de utilizadores que conhece o seu papel na política de segurança da informação.

Exemplo 5: Grau de participação dos utilizadores na concepção do SI.

Implementação e Avaliação

Exemplo 6: N.º de acções de formação proporcionadas (por ex.: mensalmente, anualmente, qualquer outro período de tempo relevante).

Exemplo 7: N.º de utilizadores envolvidos nas acções de sensibilização para a segurança da informação.

Exemplo 8: Tempo decorrente entre a utilização inicial do sistema e a sua plena utilização pelos utilizadores.

Exemplo 9: Nível de envolvimento dos utilizadores na implementação do sistema.

Operação, Manutenção e Optimização

Exemplo x: N.º de violações de segurança comunicadas num determinado período.

Exemplo n-1: ...

Exemplo n: N.º de propostas de revisão do SGSI feitas pelos utilizadores *versus* n.º de propostas implementadas.

Estes exemplos devem ser considerados a título meramente indicativo, devido essencialmente à possibilidade de serem definidas métricas adequadas a cada organização e situação concreta, facto esse que implica que as métricas a adoptar não se devem restringir apenas aquelas que aqui se apresentam, ponderando-se a possibilidade

de serem especificadas métricas distintas e provavelmente mais apropriadas à aferição de cada situação concreta.

7.5. Conclusões

Considerando os problemas com que as organizações se confrontam na actualidade acerca da segurança da sua informação de negócio e com os SI e TIC que suportam a utilização dessa mesma informação, torna-se essencial encontrar as soluções adequadas à ultrapassagem dos referidos problemas, enquadrando essas soluções na missão e estratégia das organizações.

As características do Modelo definido atendem a dois grupos de tópicos, com perspectivas diferentes, mas qualquer deles relacionado com segurança da informação: (i) confidencialidade, integridade, disponibilidade; (ii) Pessoas, TIC, processos.

Concluindo-se da necessidade de desenvolver os SGSI em conjunto com o próprio SI, optou-se pela utilização de uma metodologia tradicional para propiciar as directrizes essenciais para o enquadramento da problemática da segurança, ou seja, o SDLC.

Estes dois grupos serão considerados em quatro aspectos distintos, enquadrados pelo modelo PDCA, que é utilizado pela norma ISO/IEC 27001, para suportar as actividades directamente associadas aos SGSI.

O Modelo desenvolvido (MIDImOS – **M**odelo de **I**nicição, **D**esenvolvimento, **I**mplementação e **O**ptimização da Segurança), além de considerar as características anteriormente referenciadas, terá em conta o normativo identificado, a revisão da literatura e métricas de referência, apresentando um conjunto de referenciais que possam simplificar todos os processos e actividades dos SI, das TIC e dos SGSI, onde as Pessoas são um activo importante.

O MIDImOS obtido no final do processo compreende quatro grandes áreas associadas às metodologias de desenvolvimento de sistemas e de SGSI. As áreas estabelecidas são as seguintes: Iniciação e Planeamento; Concepção e Desenvolvimento; Implementação e Avaliação; Operação, Manutenção e Optimização.

Conclui-se assim que o Modelo desenvolvido, suportado por um conjunto diversificado de referenciais derivados da revisão da literatura, de métricas e de normas, permite

responder a problemas de implementação de políticas de segurança da informação, facilitando a aceitação das mudanças relacionadas, por parte dos utilizadores.

Este Modelo apresenta-se então como um instrumento capaz envolver todos os interessados nas actividades organizacionais, nos processos associados à segurança, e nas mudanças fundamentais para garantir que essas se adequam às necessidades organizacionais e que em simultâneo são atendidos os requisitos identificados pelas Pessoas, não defraudando deste modo os seus anseios e expectativas.

Considerando-os apenas como meros indicadores, optou-se por apresentar algumas métricas por cada um dos componentes do MIDImOS, não esgotando de modo algum as quase infinitas opções de definição de métricas, concluindo-se que o MIDImOS pode e deve ser aplicado para enquadrar este tipo de actividade.

Referências bibliográficas

- Almeida, J.M.G., “Controlar o Futuro”, in José Dias Coelho (Coordenador), *Sociedade da Informação – O percurso Português*, Edições Sílabo, 2007, p.189-199.
- Alter, S., *Information Systems: A Management Perspective*, 3rd Edition, Addison-Wesley Publishing Company, 1998.
- Anunciação, P. e Zorrinho, C., *Urbanismo Organizacional – Como gerir o choque tecnológico nas empresas*, Edições Sílabo, 2006.
- Avison, D. and Fitzgerald, G., *Information Systems Development: Methodologies, Techniques and Tools*, 3rd Edition, McGraw-Hill, 2003.
- Barman, S., *Writing Information Security Policies*, New Riders Publishing, 2002.
- Bias, R.G. and Mayhew, D.J., *Cost-Justifying Usability*, Morgan Kaufmann Publishers, 1994.
- Caldeira, M. e Romão, M., “Porque falham os sistemas e tecnologias de informação nas PMEs Portuguesas”, Actas (formato digital) da 3^a Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.
- Carneiro, A., *Introdução à Segurança dos Sistemas de Informação*, FCA, 2002.
- Chew, E., Clay, A., Hash, J., Bartol, N. and Brown, A., *Guide for Developing Performance Metrics for Information Security*, Special Publication 800-80 (Initial Public Draft), National

- Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2006.
- COBIT, *Control Objectives for Information and related Technology (Version 4.0)*, IT Governance Institute, 2005.
- Coelho, J., “Arquitectura da Empresa Centrada nos Processos: O Factor determinante para o Alinhamento Estratégico dos SI”, in Luís Amaral, Rodrigo Magalhães, Carlos Campos Morais, António Serrano e Carlos Zorrinho (Editores), *Sistemas de Informação Organizacionais*, Edições Sílabo, 2005, p.141-197.
- Daly-Jones, O., Bevan, N. and Thomas, C., “Handbook of User-Centred Design – INUSE 6.2”, Version 1.2, Serco Usability Services – National Physical Laboratory, 12 February 1999, <http://www.ejeisa.com/nectar/inuse/6.2/index.htm> (15-11-2002).
- Dicionário Houaiss da Língua Portuguesa, Tomo III, Instituto António Houaiss, Temas e Debates, 2003.
- Dicionário da Língua Portuguesa, Porto Editora, 2006.
- Dinis, J.A., *Guerra de Informação – Perspectivas de Segurança e Competitividade*, Edições Sílabo, 2005.
- Fenton, J.H. and Wolfe, J.M., “Organizing for Success: Some Human Resources Issues in Information Security”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 4, 4th Edition, Auerbach Publications, 2003, p.313-324.
- FISMA, *Federal Information Security Management Act*, Senate and House of Representatives of the United States of America, 2002.
- GAISP, *Generally Accepted Information Security Principles (Version 3.0)*, Information Systems Security Association (ISSA), 2003.
- Grance, T., Hash, J. and Stevens, M., *Security Considerations in the Information System Development Life Cycle*, Special Publication 800-64, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2003.
- Henry, K., “The Human Side of Information Security”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 4, 4th Edition, Auerbach Publications, 2003, p.239-261.
- Herrmann, D.S., *Using the Common Criteria for IT Security Evaluation*, Auerbach Publications, 2003.

- Herold, R., “Information Protection: Organization, Roles, and Separation of Duties”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 4, 4th Edition, Auerbach Publications, 2003, p.415-439.
- Hoffer, J., George, J. and Valacich, J., *Modern Systems Analysis & Design*, 3rd Edition, Addison-Wesley Longman, 2001.
- ISF, *The Standard of Good Practice for Information Security (Version 4.1)*, Information Security Forum (ISF), 2005.
- ISO, *ISO/IEC 21827 – Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM)*, International Standard Organization, 2002.
- ISO, *BS ISO/IEC 17799 (BS 7799-1:2005) – Information Technology - Code of practice for information security management*, British Standard Institution, 2005.
- ISO, *BS ISO/IEC 27001 (BS 7799-2:2005) – Information Technology - Security Techniques - Information Security Management Systems - Requirements*, British Standard Institution, 2005.
- ISSAF, *Information Systems Security Assessment Framework (draft 0.2)*, Open Information Systems Security Group, 2005.
- Kabay, M.E., “Developing Security Policies”, in S. Bosworth and M.E. Kabay, (Editors), *Computer Security Handbook*, 4th Edition, John Wiley & Sons, 2002.
- King, C.M., Dalton, C.E. and Osmanoglu, T.E., *Security Architecture: Design, Deployment & Operations*, Osborne/McGraw-Hill, 2001.
- Kovács, I., “Trabalho, Qualificações e Aprendizagem ao longo da vida: Ilusões e problemas da sociedade de informação”, in VII Encontro Nacional da APSIOT, *Formação, Trabalho e Tecnologia: Para uma Nova Cultura Organizacional*, Celta Editora, 1998, p.69-84.
- Lindley, R.M., “Economias Baseadas no Conhecimento”, in Maria João Rodrigues (Coordenadora), *Para Uma Europa da Inovação e do Conhecimento*, Celta Editora, 2000, p.33-78.
- Llufriu, M., “Impacte das Tecnologias de Informação e Comunicação na Sociedade do Conhecimento”, in Luís Amaral, Rodrigo Magalhães, Carlos Campos Morais, António Serrano e Carlos Zorrinho (Editores), *Sistemas de Informação Organizacionais*, Edições Sílabo, 2005, p.95-112.

- Lopes, F.C. e Amaral, L.A., “Actividades de Intervenção de Sistemas de Informação”, Actas (formato digital) da 1ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade do Minho, Guimarães, 25-27 de Outubro de 2000.
- Lourenço, R.T. e O’Neill, H., “As Tecnologias de Informação e Comunicação na Gestão Empresarial e o papel dos Recursos Humanos na sua Potenciação”, Actas (formato digital) da 3ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.
- Mamede, H.S., *Segurança Informática nas Organizações*, FCA, 2006.
- Martin, E.W., Brown, C.V., DeHayes, D.W., Hoffer, J.A. and Perkins, W.C., *Managing Information Technology*, 4th Edition, Prentice Hall, 2002.
- Michaelis: Moderno Dicionário da Língua Portuguesa, Companhia Melhoramentos, 1998.
- Misiolek, N., Zakaria, N. and Zhang, P., “Trust in Organizational Acceptance of Information Technology: A Conceptual Model and Preliminary Evidence”, Proceedings of the Decision Sciences Institute 33rd Annual Meeting, November 2002.
- National Institute of Standards and Technology (NIST), *An Introduction to Computer Security: The NIST Handbook*, Technology Administration - U.S. Department of Commerce, Special Publication 800-12, 1998.
- Neves, J., “Personalidade, Percepção e Aprendizagem”, in J.M. Carvalho Ferreira, José Neves e António Caetano (Editores), *Manual de Psicossociologia das Organizações*, McGrawHill, 2001.
- OECD, *Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*, Organisation for Economic Co-operation and Development, 2002.
- Parkinson, D. (Editor), *Oxford Business English Dictionary*, Oxford University Press, 2005.
- Peltier, T.R., *Information Security Risk Analysis*, Auerbach Publications, 2001.
- Pfleeger, C.P. and Pfleeger S.L., *Security in Computing*, 3rd edition, Prentice Hall, 2003.
- Reis, C., *Planeamento Estratégico de Sistemas de Informação*, Editorial Presença, 1993.
- Reis, L., *Planeamento de Sistemas de Informação e da Contingência e da Recuperação*, Tese de Doutoramento, Universidade do Minho, 2000.
- Reis, L. e Amaral, L., “Gestão de Riscos num contexto de Planeamento da Contingência e Recuperação”, Actas (formato digital) da 3ª Conferência da Associação Portuguesa de

- Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.
- Rodrigues, L.S., *Arquitecturas dos Sistemas de Informação*, FCA, 2002.
- Ross, S., “Computer Security: A practical definition”, 1999, <http://www.albion.com/security> (31-10-2003).
- Santana, S. e Dias, A., “Condicionantes da introdução de TIC em instituições prestadoras de cuidados”, Actas (formato digital) da 6ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade do Minho e pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança, Bragança, 26-28 de Outubro de 2005.
- Serrano, A. e Caldeira, M., “Gestão de Investimentos em Sistemas e Tecnologias de Informação – uma revisão crítica”, *Revista da Associação Portuguesa de Sistemas de Informação*, 15, 2001, p.99-107.
- Swanson, M., *Guide for Developing Security Plans for Information Technology Systems*, Special Publication 800-18, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 1998.
- Swanson, M., *Security Self-Assessment Guide for Information Technology Systems*, Special Publication 800-26, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2001.
- Swanson, M., Bartol, N., Sabato, J., Hash, J. and Graffo, L., *Security Metrics Guide for Information Technology Systems*, Special Publication 800-55, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2003.
- Swanson, M. and Guttman, B., *Generally Accepted Principles and Practices for Securing Information Technology Systems*, Special Publication 800-14, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 1996.
- Tavares, L.V., Pereira, M.J., “The Value of an Information Systems”, in Luís Valadares Tavares e Manuel João Pereira (Organizadores), *Nova Economia e Tecnologias de Informação: Desafios para Portugal*, Universidade Católica Editora, 2000, p.4-21.
- Veiga, P., “Prefácio”, in Alberto Carneiro, *Introdução à Segurança dos Sistemas de Informação*, FCA, 2002.

Whitman, M.E. and Mattord, H.J., *Principles of Information Security*, 2nd Edition, Thomson Course Technology, 2005.

Whitten, A. and Tygar, J.D., “Usability of Security: A Case Study”, 18 December 1998.

Zúquete, A., *Segurança em Redes Informáticas*, FCA, 2006.

8

Estudo de Caso

O estudo de casos, constitui uma metodologia de investigação que pode ser aplicada quer à abordagem quantitativa quer à abordagem qualitativa [Yin 1994], pelo que, considerando um trabalho de investigação onde a percepção das Pessoas acerca de um conjunto diversificado de temas é crucial, entende-se que esta é a metodologia a aplicar.

Todavia, a área em causa, segurança da informação, encontra-se habitualmente condicionada por questões de privacidade que condicionam e/ou impedem a divulgação de informação fidedigna e suficiente para suportar trabalhos de investigação, necessitando de ser avaliada a hipótese de realização de um único estudo de caso que permita obter os dados necessários para o desenvolvimento do trabalho.

8.1. Métodos e Técnicas de Análise

A metodologia de investigação aplicada a este trabalho, Estudo de Casos, segundo Macedo *et al* [2005], procura responder às questões de partida colocadas na proposta de trabalhos, recorrendo a diversas técnicas de recolha de dados.

Neste trabalho as técnicas de recolha dos materiais empíricos a aplicar são o Estudo de Documentos, que inclui o normativo e a legislação aplicável, e o Questionário a ser submetido ao público-alvo sobre a área que constitui a base de especificação do objecto do estudo.

Constatando-se o facto de a segurança da informação em geral e a interacção das Pessoas com a informação em particular não ter sido objecto de estudos aprofundados, optou-se neste trabalho por proceder à identificação dos *standards* existentes, que abordem a problemática da segurança da informação.

Neste contexto, após a identificação de um conjunto significativo de *standards* e outros documentos relacionados (guias, manuais, códigos, e outros), procedeu-se ao estudo dos seus objectivos, respectiva estrutura e dos controlos ou tópicos especificados,

encontrando-se descritos no capítulo 2 (Enquadramento Normativo e Legal) os principais aspectos de cada norma abordada.

Recorde-se a propósito que o termo ‘norma’ foi utilizado para referir todos os documentos estudados no referido capítulo, mesmo aqueles que não correspondem a *standards* de facto.

Considerando o facto de a percepção das Pessoas, nomeadamente a forma como entendem os SI, as TIC, a informação e a sua segurança, não estar estabelecida de forma clara nas normas estudadas, foi decidido elaborar um questionário suportado num conjunto de questões que permitisse proceder a essa caracterização.

No processo de elaboração de um questionário deste tipo, procura-se que as questões colocadas sejam suficientemente abrangentes para permitirem a obtenção de dados que possam constituir-se como um complemento fundamental para a compreensão da problemática associada à segurança da informação, e à utilização dos SI e das TIC que os suportam.

8.2. Selecção de Casos

Considerando a área em estudo, normalmente condicionada por restrições de diversa ordem que impedem e/ou limitam a divulgação de informação relacionada, entende-se pertinente atender às envolventes que podem afectar uma adequada percepção da problemática da segurança.

Pretende-se assim que os casos a estudar englobem não só a segurança da informação, mas também o envolvimento das Pessoas nessas actividades, considerando ainda os SI e TIC associados à segurança, e sempre que possível, ter em atenção a aceitação das mudanças na organização por parte dessas mesmas Pessoas.

A selecção de casos de estudo na área da segurança da informação ou da segurança dos SI, procura identificar situações de implementação de SGSI que, utilizando o diverso normativo existente, se pudessem constituir como exemplos para suportar a definição de um conjunto de parâmetros adequados à utilização e/ou validação de um Modelo que proporcione o enquadramento da percepção das Pessoas e do seu envolvimento no planeamento e desenvolvimento integrado de SGSI com os SI, perspectivando assim uma abrangência da problemática da segurança da informação pelos SI.

Perante esta envolvimento, considerando a já referida existência de constrangimentos na divulgação de informação acerca da segurança organizacional, particularmente nos aspectos directamente relacionados com as actividades de negócio, é importante ter em atenção os casos a utilizar, dado o receio dos impactos negativos que possam vir a existir sobre a imagem pública das organizações, particularmente se isso afectar a sua credibilidade nos mercados onde actuam.

A investigação desenvolvida tendente à identificação e escolha de casos de estudo nesta área revelou diversas dificuldades, relacionadas fundamentalmente com o conjunto de aspectos já mencionados, confrontando-se com a insuficiente fundamentação e especificação dos poucos casos encontrados.

Neste contexto, considerando os constrangimentos e impedimentos anteriormente mencionados, opta-se pela utilização de um único caso de estudo sobre a área da segurança da informação.

Tomar esta opção implica que o caso escolhido seja suficientemente abrangente para suportar as respostas às questões de partida especificadas para enquadrar o desenvolvimento deste trabalho.

Deste modo, considerando os objectivos anteriormente delineados, a organização de suporte ao caso de estudo vai ser o Instituto Politécnico de Setúbal (IPS), incluindo implicitamente os diversos Serviços e Unidades Orgânicas que o constituem.

8.3. Definição do Âmbito do Estudo

Além da análise do normativo existente acerca da segurança da informação, incluindo os aspectos directamente relacionados com esta problemática, vai ser analisada a percepção das Pessoas acerca da situação da segurança da informação no IPS, recorrendo aos resultados obtidos com um questionário submetido a todo o pessoal do IPS, ou seja, docentes e não docentes.

Assume-se que os questionários a desenvolver devem ser respondidos por Pessoas com um contacto frequente com o Sistema Informático da Escola ou do Serviço respectivo, e com um conhecimento relevante das aplicações instaladas e respectiva aplicabilidade e

utilização, entendeu-se ainda que a inclusão dos alunos como parte da população²⁴-alvo, sendo estes maioritariamente utilizadores pontuais do sistema e com acesso a um número limitado de equipamentos e aplicações, as suas percepções não comportariam valor acrescentado para o trabalho.

Considerou-se todavia que seria pertinente proceder à identificação de um grupo de alunos, para efectuar o teste do questionário, definindo-se por isso que esse grupo seria constituído por alunos do curso de Gestão de Sistemas de Informação da Escola Superior de Ciências Empresariais, procurando-se uma amostra de 100 inquiridos (correspondente a 25 por cada um dos anos do curso).

Esta escolha deveu-se ao facto de ser possível identificar o tipo de utilização do Sistema Informático feita por aqueles alunos, considerando que o curso é o que na sua Escola apresenta uma maior especificidade e nível de conhecimentos tecnológicos, apresentando por isso a uma utilização mais frequente do sistema.

8.3.1. Caracterização da Instituição

O IPS foi criado em 1979, Decreto-Lei nº513-T/79, de 26 de Dezembro, com os seus Estatutos a serem aprovados pelo Despacho-Normativo n.º 6/95, de 22 de Dezembro [Andrade e Ferreira 2004].

O IPS integra cinco Escolas Superiores, a Escola Superior de Tecnologia de Setúbal (ESTSetúbal) com início de funcionamento em 1983, a Escola Superior de Educação (ESE) com início de funcionamento em 1985, a Escola Superior de Ciências Empresariais (ESCE) com início de funcionamento em 1994, a Escola Superior de Tecnologia do Barreiro (ESTBarreiro) com início de funcionamento em 1999, e a Escola Superior de Saúde (ESS) com início de funcionamento em 2000.

Em termos geográficos, quatro destas Escolas situam-se no Campus do IPS em Setúbal (ESE, ESTSetúbal, ESCE e ESS) e a quinta no Barreiro (ESTBarreiro).

O facto de se ter optado por uma Instituição do Ensino Superior deveu-se ao conhecimento detido sobre o seu funcionamento, aspecto crucial para uma clara percepção do funcionamento da organização e da sua ligação com o meio envolvente.

²⁴ Colecção de unidades individuais, com uma ou mais características comuns que se pretendem analisar [Martins e Cerveira 2006:13].

Factor essencial foi a abertura manifestada pelos responsáveis institucionais, que possibilitaram a realização do estudo numa área que, habitualmente, as organizações evitam referenciar como problemática, face aos efeitos negativos que pode ter sobre a imagem e a credibilidade da organização.

Um pormenor relevante para a escolha do IPS deveu-se também às mudanças por que passam actualmente as Instituições de Ensino Superior, nomeadamente na sua reorganização e nos novos formatos das ofertas formativas, factos que implicam necessariamente um aumento dos recursos tecnológicos colocados nas actividades lectivas e as consequentes implicações na segurança da informação e também dos SI e das TIC que a suportam, por o processo de aprendizagem se focar nos próprios alunos e exigir por isso uma maior interactividade por parte destes.

8.3.2. Caracterização da População-Alvo

Para além do pessoal em serviço nas Escolas Superiores (Docentes, Não Docentes e Técnicos de Informática), a população-alvo inclui o pessoal (Não Docentes e Técnicos de Informática) dos Serviços da Presidência, dos Serviços de Acção Social e do Centro de Informática.

A população-alvo do questionário, diz respeito a um universo de 521 pessoas, às quais foram entregues questionários para preenchimento, não estando incluído, por questões de logística e das actividades que desempenham, a totalidade do pessoal em serviço no IPS, ou seja, não se incluiu o pessoal operário, de limpeza e motoristas, devido ao facto de não disporem de acesso ao Sistema Informático do Serviço/Escola.

O pessoal Docente inclui Professores, Equiparados a Professor, Assistentes e Equiparados a Assistente, independentemente de se encontrarem em tempo integral ou tempo parcial.

O pessoal Não Docente inclui pessoas das carreiras Técnica Superior, Técnica, Assistente Administrativa e Técnico Profissional.

O pessoal Técnico inclui pessoas das carreiras de Especialista de Informática e de Técnico de Informática, além de considerar também os Encarregados de Trabalhos da área de Informática.

A opção por uma separação em termos de Docentes e de Não Docentes, reside no facto de a utilização dos Sistemas Informáticos e das respectivas aplicações se revestir de algumas diferenças, embora existem muitas questões idênticas a responder por qualquer dos grupos. Esta situação não impede que se possa proceder, se necessário, a uma apreciação integrada das respostas obtidas.

8.4. Elaboração dos Questionários

A elaboração inicial do questionário foi suportada principalmente na norma BS ISO/IEC 17799 [ISO 2005a], devido ao facto, constatado durante o estudo prévio do normativo, de esta norma cobrir a generalidade dos aspectos associados às questões iniciais do questionário.

As versões finais dos questionário basearam-se nos referenciais constantes do MIDImOS, de acordo com os aspectos que se pretendiam aferir no caso em estudo.

Neste sentido, foi elaborado um modelo preliminar do questionário, com 32 questões, modelo esse que, através de validações sucessivas, foi aumentado e otimizado durante o desenvolvimento das fases iniciais do trabalho.

O teste final do questionário foi realizado com a passagem de uma versão do questionário, com um total de 96 questões, a um grupo de alunos do curso de Gestão de Sistemas de Informação, no sentido de aferir a pertinência das questões colocadas e identificar aspectos que possam ter sido excluídos e sejam considerados importantes para um entendimento da percepção das Pessoas acerca da segurança da informação.

O resultado deste teste, baseado em 78 respostas dos alunos (cuja apresentação é efectuada no anexo D), permitiu a optimização final do questionário, referindo-se a alteração de algumas questões e opções de resposta permitidas.

Os resultados obtidos permitiram proceder a uma análise preliminar das respostas, identificando-se alguns cruzamentos de questões que devem ser tidos em atenção na apreciação global das respostas ao questionário final, particularmente nas opções comuns acerca da utilização dos computadores pessoais, quando comparadas com a utilização do sistema da Escola ou Serviço.

Nesta sequência, perante os resultados obtidos, o questionário foi objecto das alterações especificadas na tabela seguinte:

Referência	Questão	Alteração
B29	Que tipo de <i>software</i> utiliza no seu computador pessoal?	mais opções de resposta
C3	Caracterize a sua participação nessas mudanças.	mais opções de resposta
C25	Que tipo de <i>software</i> utiliza?	mais opções de resposta
C26	Caracterize a sua utilização do Sistema Informático do Serviço/Escola.	mais opções de resposta
C33	Quando não consegue imprimir documentos através da(s) impressora(s) partilhada(s) qual a atitude que assume?	mais opções de resposta
C34	Que atitude toma quando encontra documentos que não são seus na(s) impressora(s) partilhada(s)?	mais opções de resposta
C35	Que atitude toma quando não encontra documentos seus que mandou imprimir na(s) impressora(s) partilhada(s)?	mais opções de resposta
D5	Caracterize a sua participação nessas actividades.	mais opções de resposta
D11	Durante o tempo em que tem activa a sua sessão de trabalho, utiliza algum mecanismo de protecção de ecrã para quando não está a utilizar o computador?	questão nova
D13	Classifique, relativamente à segurança do Sistema Informático da Escola, os seguintes aspectos:	mais aspectos a classificar
D15	Classifique a facilidade de acesso físico ao Sistema Informático da Escola, nos seguintes pontos de acesso:	mais pontos de acesso a classificar
D17	Classifique, de acordo com o impacto na segurança do Sistema Informático do Serviço/Escola, os seguintes tipos de ameaças.	mais ameaças a classificar
E2	Com que frequência recebe formação necessária à utilização do Sistema Informático do Serviço/Escola?	questão nova
E9	Classifique, relativamente à usabilidade do Sistema Informático do Serviço/Escola, a relevância dos seguintes aspectos:	mais aspectos a classificar

Tabela 8.1 – Alterações às questões dos questionários

Com o objectivo de obter uma melhor caracterização das respostas, foram elaborados três modelos do questionário, um para cada tipo de população-alvo, apresentados no anexo B a este documento, mantendo-se no entanto comuns a maioria das questões.

O modelo de questionário elaborado para os Docentes proporciona a identificação das Escolas onde se integram, enquanto que o modelo para os Não Docentes não permite

proceder à identificação da Escola ou Serviço de origem, tendo sido esta decisão tomada no sentido de tornar impossível a identificação de qualquer inquirido(a).

Face às especificidades das funções desempenhadas, foi elaborado posteriormente um modelo destinado ao pessoal de informática, não identificando aqui a Escola ou o Serviço de origem, assim como também as respectivas categorias profissionais, face ao reduzido número destes profissionais, evitando-se assim qualquer possibilidade de identificação dos inquiridos.

Na elaboração do questionário, e na medida do possível, optou-se por evitar os termos mais técnicos, face à heterogeneidade da população alvo e à diversidade dos níveis de formação académica que possuem. A opção por questões fechadas, que teve também em atenção os aspectos anteriormente definidos, deve-se à novidade da problemática da segurança da informação, normalmente afastada das preocupações e actividades do dia-a-dia das Pessoas.

As questões colocadas apresentam-se em três tipos distintos: de escolha única, de escolha múltipla, e de classificação (valores entre 1 e 6). Algumas das questões de escolha única, ao invés de pretenderem a percepção das Pessoas acerca de uma determinada temática, destinam-se apenas a controlar o fluxo de preenchimento dos questionários.

O processo de desenho preliminar dos questionários foi enquadrado com fluxogramas, que por sua vez foram sucessivamente actualizados num processo interactivo de ajustes nos fluxogramas e nos questionários, considerando a necessidade de agrupar questões e controlar os ‘ciclos’ dentro dos questionários, em função das respostas obtidas.

O questionário, em qualquer dos seus modelos, encontra-se estruturado em 5 grupos de questões. O grupo A destina-se a caracterizar o(a) inquirido(a), o grupo B pretende obter uma caracterização da utilização do computador pessoal, enquanto que os grupos C, D e E se destinam a obter a percepção do(a) inquirido(a) acerca da utilização e da segurança da informação do Sistema Informático da Escola ou Serviço em que a Pessoa se integra.

O grupo A (**Identificação/Caracterização do(a) inquirido(a)**) destina-se essencialmente a caracterizar a situação pessoal de cada inquirido(a), nomeadamente idade, residência e experiência profissional, e ainda a formação académica e a sua

ligação com a instituição. Este grupo comporta 9 questões no modelo A (Docentes), 6 questões no modelo B (Não Docentes) e 6 questões no modelo C (Técnicos de Informática).

O grupo B (**Computador pessoal**) procura perceber a utilização dos computadores pessoais, nomeadamente o modo de utilização (partilha da utilização, acesso à Internet, etc.), a eventual utilização de *password* e respectiva gestão, utilização de mecanismos de protecção, realização de *backups*, frequência de utilização, e *software* utilizado. Este grupo comporta 29 questões no modelo A (Docentes), 29 questões no modelo B (Não Docentes) e 29 questões no modelo C (Técnicos de Informática).

O grupo C (**Sistema Informático do Serviço/Escola**) procura a percepção dos utilizadores acerca de mudanças e funcionamento do sistema, acesso ao sistema e utilização de *passwords*, utilização do sistema e *software*, utilização de áreas de trabalho nos servidores do sistema, e acesso e utilização de impressoras partilhadas. Este grupo comporta 36 questões no modelo A (Docentes), 38 questões no modelo B (Não Docentes) e 38 questões no modelo C (Técnicos de Informática).

O grupo D (**Segurança da Informação no Sistema Informático do Serviço/Escola**) aborda a existência de políticas de segurança e a participação do(a) inquirido(a) na sua definição, classificação da segurança para diversos aspectos relacionados com o sistema, acesso ao sistema, e classificação do impacto que diversas ameaças têm sobre o sistema. Este grupo comporta 17 questões no modelo A (Docentes), 17 questões no modelo B (Não Docentes) e 27 questões no modelo C (Técnicos de Informática).

O grupo E (**Usabilidade do Sistema Informático do Serviço/Escola**) pretende perceber a facilidade de utilização do sistema, e a classificação de diversos aspectos que podem afectar a sua usabilidade. Este grupo comporta 10 questões no modelo A (Docentes), 10 questões no modelo B (Não Docentes) e 9 questões no modelo C (Técnicos de Informática).

Em termos globais, o modelo A possui um total de 101 questões, o modelo B possui 100 questões, e o modelo C engloba 109 questões.

Os fluxogramas de cada um dos modelos de questionário são apresentados nas figuras seguintes, onde por uma questão de simplificação de leitura do próprio fluxograma se apresentam as perguntas na sua forma abreviada.

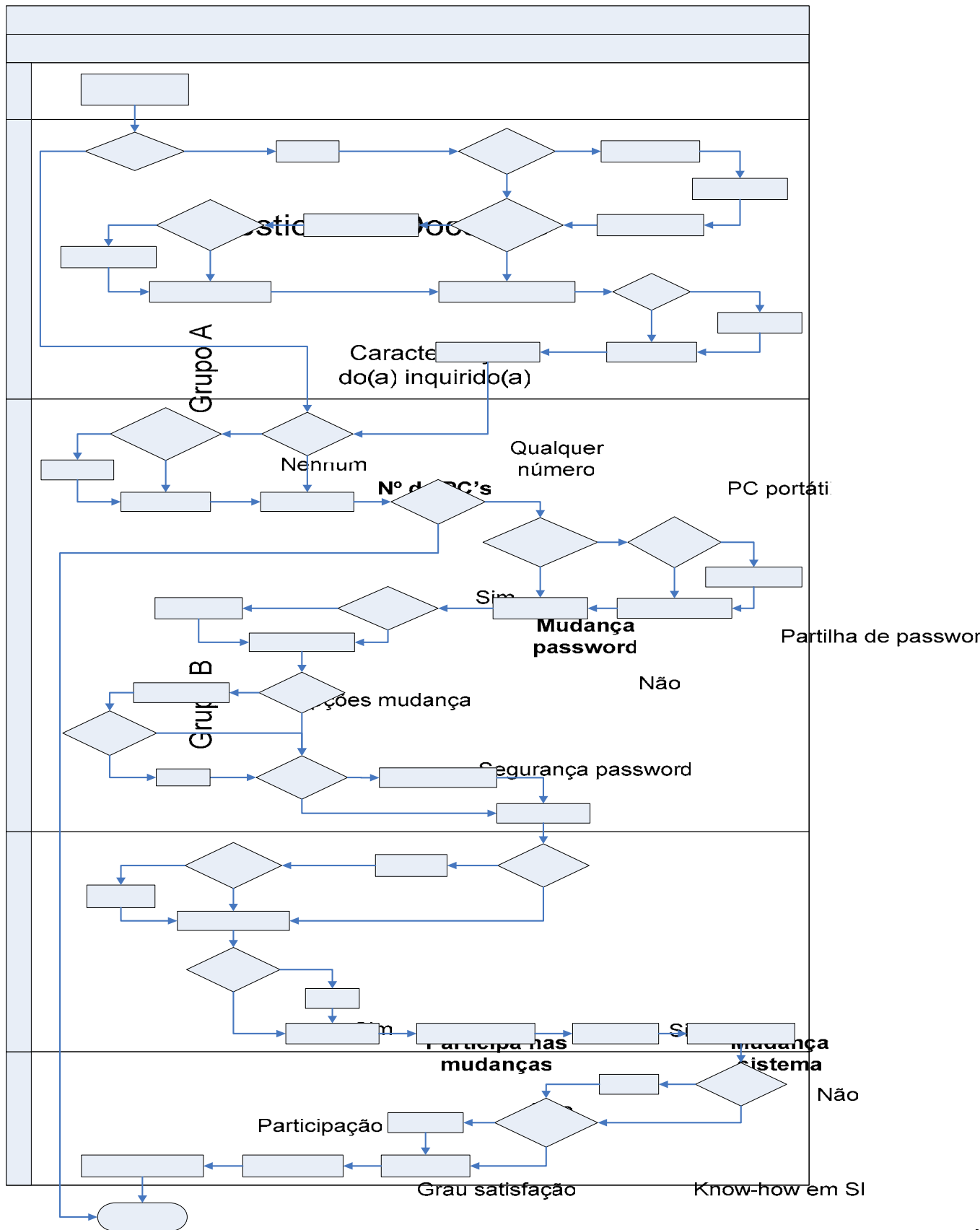


Figura 8.1 – Fluxograma do modelo A de questionário

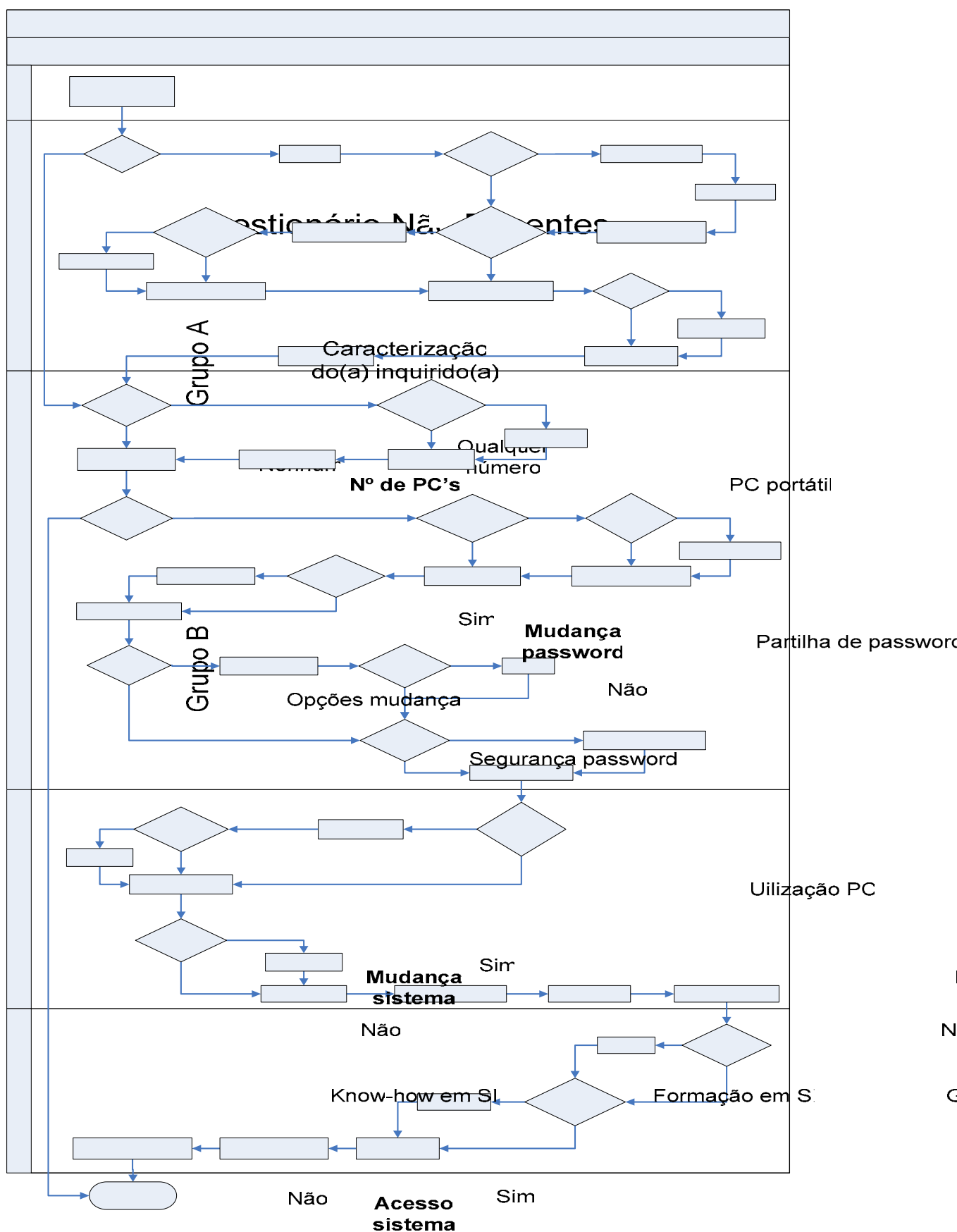


Figura 8.2 – Fluxograma do modelo B de questionário

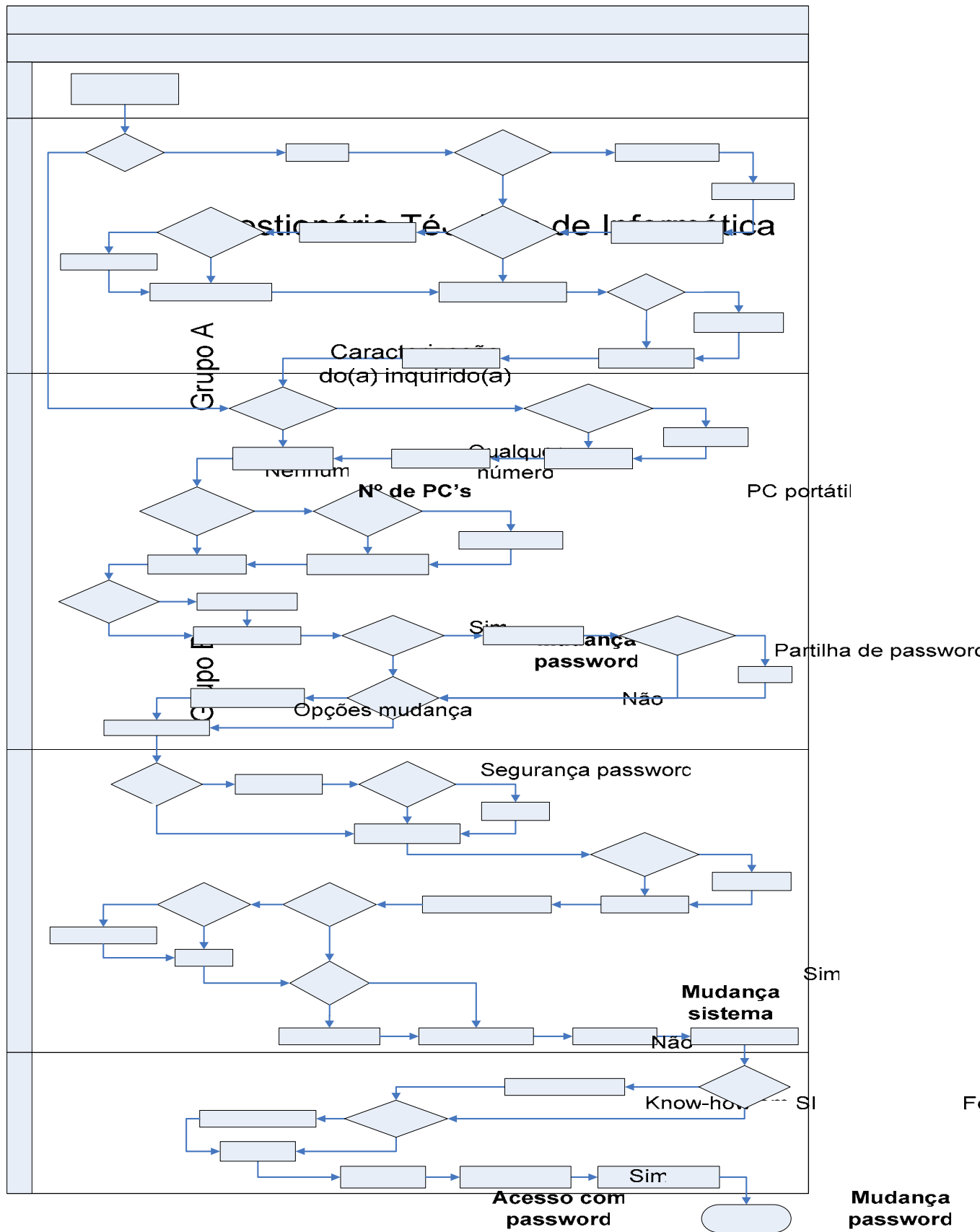


Figura 8.3 – Fluxograma do modelo C de questionário

Grupo C

Com o objectivo de proporcionar uma melhor abordagem às questões colocadas, apresenta-se no início de alguns grupos dos questionários, definições consideradas essenciais acerca de aspectos relevantes e cujo significado possa ser desconhecido por parte de alguns dos inquiridos, ou seja, mais concretamente as definições de: sistema informático no grupo C, segurança da informação no grupo D e usabilidade no grupo E.

As questões colocadas estão directamente relacionadas com a realidade da organização que constitui o caso de estudo e com a pesquisa bibliográfica efectuada para suportar o enquadramento necessário à proposta de trabalhos.

Neste sentido, apresentam-se referenciais (α , β , γ) do MIDImOS que se consideraram adequados a enquadrar a diversidade de questões associadas à problemática da segurança da informação, optando-se pela sua utilização para suportar o questionário a construir.

O enquadramento entre as questões a colocar nos questionários e os referenciais do MIDImOS, é apresentado nas tabelas seguintes, tendo em atenção apenas os grupos C, D e E de qualquer dos modelos de questionário, por serem os grupos onde se torna possível aferir questões directamente relacionadas com as normas de segurança.

As tabelas anteriormente referidas apresentam-se estruturadas por temáticas dentro de cada um dos grupos dos questionários, estruturação essa que será utilizada posteriormente neste capítulo no processo de análise das respostas obtidas através dos questionários.

Refira-se no entanto que os referenciais apresentados são aqueles que possuem a melhor adequação a cada questão, considerando-se todavia que é possível a utilização simultânea dos controlos abrangidos por qualquer dos referenciais, quer neste contexto quer quando se está perante a definição e implementação de um SGSI.

Qualquer referência efectuada, nas tabelas seguintes, ao Sistema Informático deve ser entendida em sentido lato, considerando que para os Docentes essa referência será sempre relativa ao sistema existente em cada Escola, enquanto que para os Não Docentes e Técnicos a referência dirá sempre respeito ao sistema existente no seu habitual local de trabalho.

Refira-se ainda que as legendas apresentadas nestas tabelas destinam-se apenas a permitir o controlo da numeração das questões colocadas em cada um dos modelos de questionário, tendo precisamente em atenção o facto de os modelos dos questionários não possuírem o mesmo número total de questões.

C – Sistema Informático (Funcionamento e Mudanças no Sistema Informático)	Referenciais MIDImOS
C1) Desde a sua entrada no Serviço/Escola existiu alguma mudança no Sistema Informático (<i>Hardware, Software, Procedimentos, etc.</i>)? ①	$\alpha 1, \alpha 9, \alpha 10, \beta 7, \beta 8, \gamma 2$
C2) Foi solicitada a sua participação/participou de alguma forma nessas mudanças? ①	$\alpha 1, \alpha 9, \alpha 10, \alpha 11, \beta 4$
C3) Caracterize a sua participação nessas mudanças. ①	$\alpha 1, \alpha 3, \alpha 9, \alpha 11, \beta 4, \beta 5, \gamma 4$
C4) Classifique o seu grau de participação nessas mudanças. (6 para elevado e 1 para baixo) ①	$\alpha 1, \alpha 2, \alpha 7, \alpha 9, \alpha 11, \beta 4$
C5) Classifique o seu grau de satisfação com as mudanças efectuadas. (6 para elevado e 1 para baixo) ①	$\alpha 1, \alpha 2, \alpha 7, \alpha 8, \alpha 9, \beta 1, \beta 4, \beta 7, \gamma 2$
C6) Classifique a sua percepção acerca do funcionamento do Sistema Informático depois das mudanças efectuadas. (6 para melhorou muito e 1 para não melhorou) ①	$\alpha 1, \alpha 2, \alpha 7, \alpha 8, \alpha 9, \beta 1, \beta 9$

Legenda:

① Todos os inquiridos com a mesma numeração.

Tabela 8.2 – Questões do grupo C dos questionários acerca do ‘Funcionamento e Mudanças no Sistema Informático’ *versus* Referenciais MIDImOS

C – Sistema Informático (Conhecimentos e Formação em Informática)	Referenciais MIDImOS
C7) Já tinha utilizado computadores antes de ser admitido(a) no IPS/Escola? ②	$\alpha 12, \beta 6, \gamma 6$
C7) Qual a frequência média das acções de formação em informática que recebeu? ③	$\alpha 12, \beta 6, \gamma 6$
C8) Realizou algum(uns) curso(s) de formação em Informática/Sistemas de Informação antes de ser admitido(a) no IPS/Escola? ②	$\alpha 12, \beta 6, \gamma 6$
C8) Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante) ③	$\alpha 2, \alpha 7, \alpha 12, \beta 6, \gamma 2, \gamma 6$
C7/9) Classifique o seu grau de conhecimentos na área da Informática/Sistemas de Informação. (6 para elevado e 1 para baixo) ④	$\alpha 1, \alpha 2, \alpha 7, \alpha 11, \beta 6, \gamma 2, \gamma 6$

Legenda:

② NãoDocentes.

③ Técnicos.

④ Todos os inquiridos, mas NãoDocentes e Técnicos com numeração diferenciada.

Tabela 8.3 – Questões do grupo C dos questionários acerca dos ‘Conhecimentos e Formação em Informática’ *versus* Referenciais MIDImOS

C – Sistema Informático (Password e Mecanismos de Acesso ao Sistema Informático)	Referenciais MIDImOS
<i>C8/10)</i> Dispõe de acesso ao Sistema Informático? ⑤	$\alpha 11, \beta 2, \beta 8, \gamma 3, \gamma 5, \gamma 7$
<i>C9/11/10)</i> O acesso ao Sistema Informático é feito através de <i>password</i> ? ⑥	$\alpha 4, \alpha 10, \beta 8, \gamma 3, \gamma 5$
<i>C18/20)</i> Além da <i>password</i> , especifique que tipo(s) de mecanismo(s) está(ão) implementado(s) para acesso ao Sistema Informático. ④	$\alpha 4, \alpha 8, \alpha 10, \beta 8, \gamma 3, \gamma 5$
<i>C10/12/11)</i> Já alterou a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático? ⑥	$\alpha 4, \beta 8$
<i>C11/13/12)</i> Com que frequência altera a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático? ⑥	$\alpha 4, \alpha 8, \alpha 11, \beta 8$
<i>C12/14/13)</i> Que opções efectua na escolha de nova(s) <i>password(s)</i> ? ⑥	$\alpha 4, \alpha 8, \alpha 11, \beta 8$
<i>C13/15/14)</i> Na definição de nova(s) <i>password(s)</i> opta por. ⑥	$\alpha 4, \alpha 8, \alpha 11, \beta 8$
<i>C14/16/15)</i> Qual o processo que utiliza para guardar a(s) sua(s) <i>password(s)</i> ? ⑥	$\alpha 4, \alpha 8, \alpha 11, \beta 8$
<i>C15/17/16)</i> Com quantas pessoas partilha a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático? ⑥	$\alpha 4, \alpha 8, \alpha 11, \beta 8$
<i>C16/18)</i> Utiliza a mesma <i>password</i> para diversas aplicações/sistemas? ④	$\alpha 4, \alpha 10, \alpha 11, \beta 8$
<i>C17)</i> Quantas <i>passwords</i> de acesso ao Sistema Informático utiliza? ③	$\alpha 4, \alpha 10, \beta 8$
<i>C17/19)</i> Classifique o grau de segurança da(s) sua(s) <i>password(s)</i> . (6 para elevado e 1 para baixo) ④	$\alpha 1, \alpha 2, \alpha 4, \alpha 7, \alpha 11, \beta 3, \gamma 2$

Legenda:

- ③ Técnicos.
- ④ Todos os inquiridos, mas NãoDocentes e Técnicos com numeração diferenciada.
- ⑤ Docentes e NãoDocentes, mas com numeração diferenciada.
- ⑥ Todos os inquiridos, mas com numeração diferenciada.

Tabela 8.4 – Questões do grupo C dos questionários acerca da ‘Password e Mecanismos de Acesso ao Sistema Informático’ versus Referenciais MIDImOS

C – Sistema Informático (Utilização do Correio Electrónico)	Referenciais MIDImOS
<i>C19/21)</i> Possui algum endereço de correio electrónico associado ao Sistema Informático? ④	$\alpha 4, \alpha 11, \beta 8, \gamma 7$
<i>C20/22)</i> Além desse, quantos endereços de correio electrónico possui? ④	$\alpha 4, \beta 8$
<i>C21/23)</i> Utiliza a mesma <i>password</i> para acesso ao correio electrónico e ao Sistema Informático? ④	$\alpha 4, \alpha 11, \beta 8$
<i>C22/24)</i> Existe implementado algum sistema de filtragem de mensagens de correio electrónico? ④	$\alpha 5, \alpha 8, \alpha 10, \beta 8, \gamma 5$

Legenda:

- ④ Todos os inquiridos, mas NãoDocentes e Técnicos com numeração diferenciada.

Tabela 8.5 – Questões do grupo C dos questionários acerca da ‘Utilização do Correio Electrónico’ versus Referenciais MIDImOS

C – Sistema Informático (Acesso e Utilização do Sistema Informático)	Referenciais MIDImOS
C23/25) Com que frequência acede ao Sistema Informático? ④	$\alpha 5, \gamma 7$
C24/26) Durante a utilização do Sistema Informático, qual o tempo médio diário de cada utilização? ④	$\alpha 5, \gamma 7$
C26/28) Caracterize a sua utilização do Sistema Informático. ④	$\alpha 5, \gamma 7$
C25/27) Que tipo de <i>software</i> utiliza? ④	$\alpha 5, \gamma 7$
C27/29) Utiliza alguma área de trabalho privada no(s) servidor(es) do Sistema Informático? ④	$\alpha 4, \gamma 3, \gamma 5, \gamma 7$
C28/30) Que tipo de informação guarda nessa área de trabalho? ④	$\alpha 5$
C29/31) Já perdeu informação guardada nessa área de trabalho? ④	$\alpha 5, \alpha 11, \gamma 1$
C30/32) Que acção tomou para recuperar essa informação? ④	$\alpha 5, \alpha 11, \beta 3, \beta 8, \gamma 1$
C31/33) O que aconteceu relativamente a essa situação? ④	$\alpha 5, \beta 3, \beta 8, \gamma 1$
C32/34) Possui acesso à impressão de documentos através do Sistema Informático utilizando impressora(s) partilhada(s)? ④	$\alpha 4, \alpha 5, \alpha 11, \gamma 3, \gamma 5, \gamma 7$
C33/35) Quando não consegue imprimir documentos através da(s) impressora(s) partilhada(s) qual a atitude que assume? ④	$\alpha 5, \alpha 8, \beta 8, \gamma 4$
C34/36) Que atitude toma quando encontra documentos que não são seus na(s) impressora(s) partilhada(s)? ④	$\alpha 8, \beta 3, \beta 8, \gamma 1$
C35/37) Que atitude toma quando não encontra documentos seus que mandou imprimir na(s) impressora(s) partilhada(s)? ④	$\alpha 5, \alpha 8, \beta 3, \beta 8, \gamma 1, \gamma 5$
C36/38) Consideraria a hipótese de aceder ao Sistema a partir da sua residência ou de outro local onde trabalhe regularmente? ④	$\alpha 4, \beta 2, \beta 8, \gamma 3, \gamma 7$

Legenda:

④ Todos os inquiridos, mas NãoDocentes e Técnicos com numeração diferenciada.

Tabela 8.6 – Questões do grupo C dos questionários acerca do ‘Acesso e Utilização do Sistema Informático’ *versus* Referenciais MIDImOS

D – Segurança da Informação no Sistema Informático (Políticas de Segurança da Informação e do Sistema Informático)	Referenciais MIDImOS
D1) Existem políticas de segurança do Sistema Informático? ①	$\alpha 3, \alpha 6, \alpha 10, \beta 8$
D2) Como tomou conhecimento dessas políticas? ①	$\alpha 3, \alpha 10, \beta 4, \beta 8, \gamma 5$
D3) Dos aspectos a seguir mencionados especifique quais são abrangidos pelas políticas definidas. ①	$\alpha 3, \alpha 6, \alpha 10, \beta 8, \gamma 5$
D4) Participou na elaboração/alteração dessas políticas? ①	$\alpha 3, \alpha 9, \alpha 10, \alpha 11, \beta 4$
D5) Caracterize a sua participação nessas actividades. ①	$\alpha 3, \alpha 9, \alpha 11, \beta 4, \beta 8, \gamma 4$
D6) Classifique o seu grau de participação nessas actividades. (6 para elevado e 1 para baixo) ①	$\alpha 2, \alpha 7, \alpha 9, \alpha 11, \beta 4, \gamma 2$

Legenda:

① Todos os inquiridos com a mesma numeração.

Tabela 8.7 – Questões do grupo D dos questionários acerca das ‘Políticas de Segurança da Informação e do Sistema Informático’ *versus* Referenciais MIDImOS

D – Segurança da Informação no Sistema Informático (Mecanismos de Protecção do Sistema Informático)	Referenciais MIDImOS
D10) Após o <i>login</i> no acesso ao Sistema Informático, existe definido algum tempo limite para que a sessão de trabalho esteja activa? ①	$\alpha 4, \alpha 8, \alpha 10, \gamma 1, \gamma 3$
D11) Durante o tempo em que tem activa a sua sessão de trabalho, utiliza algum mecanismo de protecção de ecrã para quando não está a utilizar o computador? ①	$\alpha 5, \alpha 8, \alpha 10, \gamma 1, \gamma 3, \gamma 4, \gamma 7$
D12) Além da <i>password</i> que mecanismo/ferramenta/software é utilizado para protecção do Sistema Informático? ③	$\alpha 4, \alpha 8, \alpha 10, \beta 8, \gamma 3, \gamma 5$
D13) Com que frequência se actualiza esse mecanismo/ferramenta/software? ③	$\alpha 4, \alpha 8, \alpha 10, \beta 8$

Legenda:

- ① Todos os inquiridos com a mesma numeração.
③ Técnicos.

Tabela 8.8 – Questões do grupo D dos questionários acerca dos ‘Mecanismos de Protecção do Sistema Informático’ *versus* Referenciais MIDImOS

D – Segurança da Informação no Sistema Informático (Realização de Cópias de Segurança)	Referenciais MIDImOS
D14) Está implementada alguma política de cópias de segurança da informação contida nos servidores? ③	$\alpha 3, \alpha 10, \beta 8, \gamma 5$
D15) Essa política de cópias de segurança da informação estabelece regras em função da criticidade da informação? ③	$\alpha 3, \alpha 10, \beta 8, \gamma 5$
D16) Caracterize essas regras para as cópias de segurança. ③	$\alpha 3, \alpha 8, \alpha 10, \beta 8, \gamma 5$
D17) Com que periodicidade são efectuadas as cópias de segurança da informação crítica? ③	$\alpha 8, \beta 8, \gamma 5$
D18) Que tipo de dispositivo é utilizado para efectuar as cópias de segurança? ③	$\alpha 5, \alpha 6, \beta 8, \gamma 4, \gamma 5$
D19) Onde são guardadas as cópias de segurança efectuadas? ③	$\alpha 6, \beta 8, \gamma 4$

Legenda:

- ③ Técnicos.

Tabela 8.9 – Questões do grupo D dos questionários acerca da ‘Realização de Cópias de Segurança’ *versus* Referenciais MIDImOS

D – Segurança da Informação no Sistema Informático (Percepção da Facilidade de Acesso ao Sistema Informático)	Referenciais MIDImOS
D15/25) Classifique a facilidade de acesso físico ao Sistema Informático, nos seguintes pontos de acesso. ⑦	$\alpha 2, \alpha 4, \alpha 7, \alpha 8, \beta 9, \gamma 1, \gamma 2, \gamma 3, \gamma 5, \gamma 7$

Legenda:

- ⑦ Todos os inquiridos, mas Técnicos com numeração diferenciada.

Tabela 8.10 – Questões do grupo D dos questionários acerca da ‘Percepção da Facilidade de Acesso ao Sistema Informático’ *versus* Referenciais MIDImOS

D – Segurança da Informação no Sistema Informático (Controlo dos Activos do Sistema e da sua Utilização)	Referenciais MIDImOS
D8) Já presenciou alguma(s) violação(ões) da segurança do Sistema Informático (por exemplo destruição/roubo de equipamentos, entradas em locais interditos, utilização de ficheiros/ <i>passwords</i> de outras pessoas, etc.)? ①	$\alpha 6, \alpha 10, \beta 3, \gamma 1, \gamma 5$
D9) Que atitude tomou quando presenciou essa(s) violação(ões)? ①	$\alpha 3, \alpha 6, \alpha 8, \alpha 10, \alpha 11, \beta 3, \gamma 1$
D16/26) Nos locais onde tem acesso ao Sistema Informático especifique que actividades estão proibidas. ⑦	$\alpha 4, \alpha 8, \beta 3, \gamma 1, \gamma 5$
D20) Existem registos do <i>hardware</i> e <i>software</i> existente no Serviço? ③	$\alpha 3, \alpha 5, \alpha 10, \beta 2, \beta 8$
D21) Com que periodicidade são actualizados esses registos? ③	$\alpha 5, \alpha 10, \beta 2, \beta 8$

Legenda:

- ① Todos os inquiridos com a mesma numeração.
- ③ Técnicos.
- ⑦ Todos os inquiridos, mas Técnicos com numeração diferenciada.

Tabela 8.11 – Questões do grupo D dos questionários acerca da ‘Controlo dos Activos do Sistema e da sua Utilização’ *versus* Referenciais MIDImOS

D – Segurança da Informação no Sistema Informático (Percepção da Segurança do Sistema Informático)	Referenciais MIDImOS
D7) Caracterize a sua participação nas acções de sensibilização para a problemática da segurança da informação? ①	$\alpha 10, \alpha 12, \beta 4, \beta 6, \gamma 6$
D12/22) Classifique a segurança do Sistema Informático. (6 para muito seguro e 1 para pouco seguro) ⑦	$\alpha 2, \alpha 7, \alpha 8, \alpha 10, \beta 8, \gamma 2$
D14/24) Classifique em que medida considera que a segurança do Sistema Informático é ou pode ser importante para as suas actividades. (6 para muito importante e 1 para pouco importante) ⑦	$\alpha 1, \alpha 2, \alpha 7, \alpha 11, \beta 9, \gamma 2, \gamma 5$
D13/23) Classifique, relativamente à segurança do Sistema Informático (6 para muito importante e 1 para pouco importante), os seguintes aspectos. ⑦	$\alpha 3, \alpha 7, \alpha 8, \alpha 10, \alpha 11, \beta 8, \gamma 2$
D17/27) Classifique, de acordo com o impacto na segurança do Sistema Informático (6 para muito importante e 1 para pouco importante), os seguintes tipos de ameaças. ⑦	$\alpha 2, \alpha 6, \alpha 7, \alpha 8, \alpha 10, \alpha 11, \beta 3, \gamma 1, \gamma 2, \gamma 5$

Legenda:

- ① Todos os inquiridos com a mesma numeração.
- ⑦ Todos os inquiridos, mas Técnicos com numeração diferenciada.

Tabela 8.12 – Questões do grupo D dos questionários acerca da ‘Percepção da Segurança do Sistema Informático’ *versus* Referenciais MIDImOS

E – Usabilidade do Sistema Informático (Formação na Utilização do Sistema)	Referenciais MIDImOS
<i>E1)</i> Recebeu formação na utilização do Sistema Informático? ①	$\alpha 12, \beta 6, \gamma 6$
<i>E2)</i> Com que frequência recebe formação necessária à utilização do Sistema Informático? ③	$\alpha 12, \beta 6, \gamma 6$
<i>E3/2)</i> Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante) ⑦	$\alpha 2, \alpha 7, \alpha 12, \beta 1, \gamma 2, \gamma 6$
<i>E3)</i> São proporcionadas acções de formação sobre a utilização do Sistema Informático aos utilizadores finais? ③	$\alpha 12, \beta 6, \gamma 6$
<i>E4)</i> Com que frequência são realizadas essas acções? ③	$\alpha 12, \beta 6, \gamma 6$
<i>E5)</i> São elaborados alguns documentos acerca da utilização do Sistema Informático para apoio aos utilizadores finais? ③	$\alpha 3, \gamma 5$
<i>E4)</i> Existe algum(uns) documento(s) acerca da utilização do Sistema Informático? ⑧	$\alpha 3, \gamma 5$
<i>E5)</i> Como tomou conhecimento desse(s) documento(s)? ⑧	$\alpha 3, \alpha 10, \gamma 5$
<i>E6)</i> Classifique a utilidade desse(s) documento(s). (6 para muito útil e 1 para pouco útil) ⑧	$\alpha 2, \alpha 3, \alpha 7, \gamma 2, \gamma 5$

Legenda:

- ① Todos os inquiridos com a mesma numeração.
- ③ Técnicos.
- ⑦ Todos os inquiridos, mas Técnicos com numeração diferenciada.
- ⑧ Docentes e NãoDocentes com a mesma numeração.

Tabela 8.13 – Questões do grupo E dos questionários acerca da ‘Formação na Utilização do Sistema’ *versus* Referenciais MIDImOS

E – Usabilidade do Sistema Informático (Facilidade de Utilização e Aprendizagem do Sistema)	Referenciais MIDImOS
<i>E7/6)</i> Classifique a facilidade de utilização do Sistema Informático (6 para fácil de utilizar e 1 para difícil de utilizar). ⑦	$\alpha 2, \alpha 5, \alpha 7, \beta 1, \beta 9, \gamma 2, \gamma 7$
<i>E8/7)</i> Classifique a facilidade de aprendizagem do Sistema Informático. (6 para fácil de aprender e 1 para difícil de aprender) ⑦	$\alpha 2, \alpha 5, \alpha 7, \alpha 12, \beta 1, \beta 9, \gamma 2, \gamma 6$
<i>E9/8)</i> Classifique, relativamente à usabilidade do Sistema Informático (6 para muito importante e 1 para pouco importante), a relevância dos seguintes aspectos. ⑦	$\alpha 2, \alpha 5, \alpha 7, \alpha 11, \alpha 12, \beta 1, \beta 9, \gamma 2, \gamma 6, \gamma 7$
<i>E10/9)</i> Classifique em que medida considera que a usabilidade do Sistema Informático é ou pode ser importante para as suas actividades. (6 para muito importante e 1 para pouco importante) ⑦	$\alpha 1, \alpha 2, \alpha 5, \alpha 7, \alpha 11, \beta 1, \beta 9, \gamma 2$

Legenda:

- ⑦ Todos os inquiridos, mas Técnicos com numeração diferenciada.

Tabela 8.14 – Questões do grupo E dos questionários acerca da ‘Facilidade de Utilização e Aprendizagem do Sistema’ *versus* Referenciais MIDImOS

Relativamente às tabelas anteriores, deve notar-se que o facto de para cada questão se apresentarem os referenciais aplicáveis, não implica necessariamente a obrigatoriedade de serem utilizados todos os controlos subjacentes a cada um dos referenciais mencionados nesta e nas tabelas seguintes.

A opção por um ou mais controlos depende do tipo de métrica que se pretende aplicar em cada caso concreto, onde um mesmo controlo pode suportar mais de que uma métrica.

Estes aspectos são fundamentais em diversas conjunturas e em particular quando o que se pretende é aferir situações relacionadas com percepções, atitudes e comportamentos das Pessoas na utilização dos SI, das TIC que os suportam e dos SGSI implementados, com vista à segurança da informação pessoal e organizacional como se verifica no presente caso.

Os questionários foram elaborados recorrendo a *software* específico destinado ao desenho de questionários para posterior leitura óptica, utilizando-se neste caso o *Designer* da Teleform. A aplicação que disponibiliza estas facilidades é a Cardiff Teleform (versão 10.0, de 6 de Julho de 2006) da Verity Inc., com a activação dos questionários, a subsequente leitura e a criação dos ficheiros com os dados empíricos recolhidos a ser efectuada com recurso às aplicações relacionadas, nomeadamente *Scan Station*, *Verifier* e *Reader*.

A utilização deste *software* foi possibilitada pela ESCE através da disponibilização da referida aplicação.

8.5. Análise dos Resultados dos Questionários

Conjuntamente com os questionários foi distribuído um documento, distinto para cada unidade do IPS, com instruções de preenchimento e de entrega dos mesmos após respondidos. No anexo C apresenta-se um modelo desse documento.

A tabela seguinte apresenta o controlo sumário do número de questionários distribuídos por cada modelo, procedendo-se também ao controlo dos que foram respondidos e respectiva percentagem relativamente aos que foram entregues.

Modelo do questionário	Entregues	Devolvidos	% Devolvidos
Questionário A – Docentes	388	137	35,31
Questionário B – Não Docentes	115	79	68,70
Questionário C – Técnicos de Informática	18	14	77,78
Total de questionários	521	230	44,15

Tabela 8.15 – Controlo dos questionários

Os resultados finais dos questionários serão objecto de tratamento estatístico, devido à necessidade de proceder a apreciações distintas em função de diversas agregações das questões e das respostas consideradas relevantes.

Deve também referir-se que as questões colocadas em qualquer dos questionários, possuem como objectivo único a obtenção da percepção das Pessoas acerca da utilização dos SI e das TIC, considerando um contexto onde os SI e as TIC se encontram directamente associadas à problemática da segurança da informação, não estando prevista por isso qualquer avaliação das políticas organizacionais acerca de qualquer dos assuntos referenciados.

Pelo que, face aos objectivos e conceitos anteriormente definidos, as respostas aos diversos grupos de questões serão analisadas através de uma agregação das questões interrelacionadas (previamente apresentadas neste capítulo para os grupos C, D e E, no enquadramento das questões com os referenciais MIDImOS), apresentando-se no final de cada secção um conjunto de itens a considerar, conjunta ou separadamente, para proceder à validação do Modelo construído.

Note-se ainda que as questões que foram colocadas nos diversos grupos dos questionários são aqui apresentadas em tabelas, referenciando, para cada grupo de inquiridos (por uma questão de simplificação da própria tabela, onde os Docentes são identificados como Doc, os Não Docentes como NDoc e os Técnicos como Téc) o número da respectiva questão do questionário.

As letras NR utilizadas nas diversas tabelas e/ou quadros derivados dos resultados dos questionários ou da sua apreciação posterior significam Não Respondeu.

8.5.1. Resultados do Grupo A – Identificação/Caracterização do(a) Inquirido(a)

Questões	Doc	NDoc	Téc
Escalão etário	A1)	A1)	A1)
Área de residência	A2)	A2)	A2)
Antiguidade no IPS/Escola	A3)	A3)	A3)
Experiência profissional	A4)	A4)	A4)
Habilitações Académicas	A5)	A5)	A5)
Área científica de docência	A6)	-	-
Área de formação	-	-	A6)
Carreira profissional	-	A6)	-
Identificação da Escola	A7)	-	-
Categoria profissional	A8)	-	-
Regime do contrato	A9)	-	-

Tabela 8.16 – Questões acerca da identificação/caracterização do(a) inquirido(a)

➤ *Escalão etário*

Em termos de identificação dos inquiridos tornou-se necessário proceder à diferenciação em função das opções de respostas relativamente ao Escalão etário, com o objectivo de evitar a possibilidade de identificar, no grupo dos Técnicos, a quem pertenciam as respostas.

Enquanto que nos grupos de Docentes e Não Docentes existem escalões etários com valores similares, nos Técnicos verifica-se uma concentração no escalão ‘Entre 25 anos e 35 anos’. Esta situação, escalões etários distintos, deriva essencialmente da grande rotatividade de pessoal existente neste grupo, constituído essencialmente por encarregados de trabalhos, optando-se por esta situação no sentido de evitar a identificação de qualquer dos inquiridos no grupo do Técnicos.

Contudo, é possível constatar que a grande maioria dos inquiridos tem idade inferior a 45 anos.

➤ *Área de residência*

No respeitante à área de residência dos inquiridos, considerando uma apreciação e termos gerais, constata-se que a maioria reside no concelho de Setúbal, embora essa constatação seja mais clara no grupo dos Não Docentes.

Mas se considerarmos uma análise dos grupos de *per si*, facilmente se constata que a maioria dos Docentes e Técnicos reside fora do Concelho de Setúbal.

➤ *Antiguidade no IPS/Escola*

➤ *Experiência profissional*

Relativamente à antiguidade no IPS/Escola, comparativamente com a experiência profissional dos inquiridos, constata-se uma relação quase perfeita com a opção ‘Mais de 5 anos’ a ser claramente maioritária em qualquer das situações, embora seja de registar que a diferença entre opções se apresenta mais clara no que diz respeito à ‘Experiência profissional’.

➤ *Habilitações Académicas*

Em termos de habilitações académicas, verifica-se que no grupo dos Docentes o Mestrado é a resposta mais frequente (63,50%), enquanto que no grupo dos Técnicos a opção Mestrado/Licenciatura (85,71%) é a mais frequente, quando o Bacharelato é suficiente para acesso à respectiva carreira profissional.

Já no respeitante ao grupo dos Não Docentes, embora a resposta maioritária (56,96%) seja ‘Secundário’, constata-se que a opção ‘Mestrado/Licenciatura/Bacharelato’ apresenta valores significativos (40,51), provavelmente influenciada pelo facto de neste grupo existirem 31,65% de ‘Técnicos Superiores/Técnicos’, de acordo com as respostas proporcionadas na questão A6).

➤ *Área científica de docência*

Neste âmbito constata-se que as áreas mais técnicas, relacionadas com a Informática ou áreas afins, são minoritárias, atingindo apenas 19,71% da totalidade dos inquiridos.

➤ *Área de formação*

Relativamente ao grupo dos Técnicos, a área científica predominante é a ‘Informática/Engenharia Informática’ com um valor de 71,43%.

Refira-se a propósito que no questionário não é colocada qualquer questão em termos de categoria/carreira profissional do grupo dos Técnicos, embora actualmente já tenham sido abertos concursos para as categorias de Especialista e de Técnico de Informática, devido à grande probabilidade das respostas aos

questionários poderem deixar de ser anónimas, essencialmente devido à pequena dimensão do universo em análise.

➤ *Carreira profissional*

No grupo dos Não Docentes constata-se que não existe uma predominância clara de qualquer das categorias profissionais onde os inquiridos se inserem.

➤ *Identificação da Escola*

No respeitante à Escola a que pertencem os inquiridos do grupo dos Docentes, verifica-se que a maioria das respostas é proporcionada pelos Docentes da ESCE (41,61%).

➤ *Categoria profissional*

➤ *Regime do contrato*

Relativamente à categoria profissional dos Docentes, constata-se que a maioria das respostas são proporcionadas por ‘Professores’ (36,50%) e por ‘Equiparados a Assistente’ (34,31%), sendo a soma destes valores (70,81%) bastante aproximada em termos dos valores obtidos no regime de contrato em ‘Dedicação exclusiva’ (76,64%).

8.5.2. Resultados do Grupo B – Computador Pessoal

A apreciação dos resultados deste grupo será efectuada em função da relação directa entre as questões colocadas e não apenas e só a sequência pela qual as mesmas foram apresentadas no questionário.

No contexto deste grupo de questões serão abordados os seguintes temas:

- Existência e partilha de computador pessoal;
- Acesso à Internet com o computador pessoal;
- Utilização de *password* no computador pessoal;
- Utilização de mecanismos de protecção;
- Realização de cópias de segurança;
- Utilização do computador pessoal;
- Percepção da segurança do computador pessoal.

8.5.2.1. Existência e Partilha de Computador Pessoal

Este conjunto de questões procura uma caracterização da utilização de computadores pessoais, onde a sua compreensão é essencial para um adequado enquadramento dos temas seguintes.

Questões	Doc	NDoc	Téc
A quantos computadores possui acesso na sua residência?	B1)	B1)	B1)
O computador pessoal a que acede é um portátil?	B2)	B2)	B2)
Com quantas pessoas partilha a utilização do computador pessoal na sua residência?	B5)	B5)	B5)

Tabela 8.17 – Questões acerca da existência e partilha de computador pessoal

- *A quantos computadores possui acesso na sua residência?*
- *O computador pessoal a que acede é um portátil?*
- *Com quantas pessoas partilha a utilização do computador pessoal na sua residência?*

Maioritariamente, os inquiridos possuem um único computador na sua residência, com excepção dos Docentes que referem a existência de dois computadores. Em termos absolutos, refira-se que, em qualquer dos grupos, um número superior a 70% dos inquiridos possui um a dois computadores nas suas residências.

Em termos de existência de computadores pessoais, embora não relevante em termos absolutos, pelo que não será objecto de uma análise detalhada, deve referir-se a inexistência de computadores pessoais na residência de quase 18% dos Não Docentes.

Deve ainda ser referida a existência, significativa, de computadores portáteis como computador de trabalho principal, constatando-se que os Docentes optam claramente (73,72%) por esta solução, embora esta seja também uma opção com alguma relevância nos outros grupos.

Verifica-se ainda que os respectivos computadores pessoais são maioritariamente partilhados com uma única pessoa ou mesmo com nenhuma, situação constatada com maior relevância no caso dos Docentes (72,22%) e dos Técnicos (84,61%).

Tópicos a considerar relativamente à existência e partilha de computador pessoal:

⇒ Utilização de computadores portáteis.

⇒ Partilha da utilização do computador pessoal.

8.5.2.2. Acesso à Internet com o Computador Pessoal

Agrupam-se aqui as questões relacionadas com a Internet, nomeadamente os acessos e o tipo de utilização que é feita.

Questões	Doc	NDoc	Téc
Acede à Internet com o seu computador pessoal?	B3)	B3)	B3)
Especifique em que locais acede à Internet com o seu computador pessoal?	B4)	B4)	B4)
Identifique a solução que adoptou para acesso à Internet com o seu computador pessoal.	B9)	B9)	B9)
Com que frequência acede à Internet com o seu computador pessoal?	B6)	B6)	B6)
Durante esses acessos à Internet, qual o tempo médio diário de utilização?	B7)	B7)	B7)

Tabela 8.18 – Questões acerca do acesso à Internet com o computador pessoal

- *Acede à Internet com o seu computador pessoal?*
- *Especifique em que locais acede à Internet com o seu computador pessoal?*
- *Identifique a solução que adoptou para acesso à Internet com o seu computador pessoal.*

Relativamente ao acesso à Internet constata-se que a grande maioria dos inquiridos utiliza os seus computadores pessoais para o realizar, actividade esta efectuada maioritariamente nas respectivas residências, embora neste aspecto assuma relevância a utilização dos seus computadores pessoais para aceder à Internet na Escola ou Serviço a que pertencem.

Em termos de solução adoptada, verifica-se que a opção pela Internet através dos operadores de TV por cabo é maioritária, notando-se que essa opção não é tão evidente por parte dos Docentes.

- *Com que frequência acede à Internet com o seu computador pessoal?*
- *Durante esses acessos à Internet, qual o tempo médio diário de utilização?*

Acerca da frequência de acesso, esta é feita todos os dias ou quase todos os dias, com um tempo médio diário de até três horas, constatando-se no caso dos Docentes uma utilização, com alguma relevância (25,4%), superior a três horas.

Tópicos a considerar relativamente ao acesso à Internet com o computador pessoal:

- ⇒ Locais de acesso à Internet.
- ⇒ Solução tecnológica adoptada.
- ⇒ Frequência de utilização.

8.5.2.3. Utilização de Password no Computador Pessoal

Nesta secção foram agrupadas as questões relacionadas com a utilização de *passwords* para acesso aos computadores pessoais e o modo como utilizam essas *passwords*, considerando também a forma como efectuem a sua gestão, devido essencialmente a questões de confidencialidade e segurança.

Questões	Doc	NDoc	Téc
Possui <i>password</i> para acesso ao seu computador pessoal?	B10)	B10)	B10)
Com quantas pessoas partilha a sua <i>password</i> ?	B11)	B11)	B11)
Já alterou a <i>password</i> de acesso ao seu computador pessoal?	B12)	B12)	B12)
Com que frequência altera a <i>password</i> de acesso ao seu computador pessoal?	B13)	B13)	B13)
Que opções efectua na escolha da sua nova <i>password</i> ?	B14)	B14)	B14)
Na definição de nova <i>password</i> opta por:	B15)	B15)	B15)
Qual o processo que utiliza para guardar a sua <i>password</i> ?	B17)	B17)	B17)

Tabela 8.19 – Questões acerca da utilização de password no computador pessoal

- *Possui password para acesso ao seu computador pessoal?*
- *Com quantas pessoas partilha a sua password?*

No respeitante à utilização de *password* para acesso aos computadores pessoais, apenas os Técnicos optam maioritariamente por essa opção (57,14%), referenciando-se opção similar, embora minoritária, por parte dos Docentes (42,34%) e Não Docentes (36,92%).

Relativamente à partilha dessa *password*, verifica-se que a opção mais frequente é pela não partilha, e quando esta acontece é maioritariamente feita com apenas com uma única pessoa.

- *Já alterou a password de acesso ao seu computador pessoal?*
- *Com que frequência altera a password de acesso ao seu computador pessoal?*

Relativamente à alteração da *password*, verifica-se que a maioria dos Docentes e dos Técnicos já procedeu à sua realização pelo menos uma vez, registando-se uma

frequência de alteração relativamente baixa (‘Raramente’ e ‘Semestralmente/Anualmente’), verificando-se a inexistência de um padrão claramente definido no caso dos Não Docentes.

➤ *Que opções efectua na escolha da sua nova password?*

➤ *Na definição de nova password opta por:*

Já nas opções tomadas para definição das novas *passwords*, a opção por uma combinação de números e letras é claramente maioritária, optando habitualmente pela escolha de um número aleatório de caracteres entre o máximo e o mínimo permitidos, todavia, deve referenciar-se a opção algo frequente de ‘nomes de familiares’, ‘apenas letras’ e ‘datas de nascimento/aniversário’.

➤ *Qual o processo que utiliza para guardar a sua password?*

No que diz respeito ao processo utilizado para guardar a *password*, a ‘memorização’ é o processo referido como o mais usual, com valores superiores a 95% em qualquer dos três grupos de inquiridos.

Tópicos a considerar relativamente à utilização de *password* no computador pessoal:

⇒ Reduzida utilização de *password*, associada à reduzida taxa de alterações efectuadas.

⇒ Opções assumidas na escolha de novas *passwords*.

8.5.2.4. Utilização de Mecanismos de Protecção

Pretende-se aqui obter uma percepção da existência e utilização de mecanismos de segurança complementares ao habitual par *userID/password*.

Questões	Doc	NDoc	Téc
Além da <i>password</i> que mecanismo/ferramenta/software utiliza para protecção do seu computador pessoal?	B18)	B18)	B18)
Com que frequência actualiza esse mecanismo/ferramenta/software?	B19)	B19)	B19)

Tabela 8.20 – Questões acerca da utilização de mecanismos de protecção

➤ *Além da password que mecanismo/ferramenta/software utiliza para protecção do seu computador pessoal?*

➤ *Com que frequência actualiza esse mecanismo/ferramenta/software?*

O mecanismo de protecção mais frequentemente adoptado é o ‘Antivírus’, com valores dos 70,77% aos 100%, notando-se também uma opção clara por ‘Firewall’ e

‘*Antispyware*’, com a sua frequência de actualização a ser maioritariamente coincidente com a actualização do próprio mecanismo.

Tópicos a considerar relativamente à utilização de mecanismos de protecção:

⇒ Utilização de mecanismos complementares da *password*.

8.5.2.5. Realização de Cópias de Segurança

Esta secção pretende avaliar a forma como as Pessoas encaram a realização de cópias de segurança, as diversas opções que tomam para a sua concretização, e as opções de armazenamento dessas mesmas cópias.

Questões	Doc	NDoc	Téc
Efectua cópias de segurança (<i>backups</i>) da informação contida no seu computador pessoal?	B20)	B20)	B20)
Com que periodicidade efectua cópias de segurança (<i>backups</i>)?	B21)	B21)	B21)
Especifique a opção mais frequente para realização das cópias de segurança (<i>backups</i>)?	B22)	B22)	B22)
Que tipo de dispositivo utiliza para efectuar as cópias de segurança (<i>backups</i>)?	B23)	B23)	B23)
Especifique onde guarda as cópias de segurança (<i>backups</i>) que efectua.	B24)	B24)	B24)

Tabela 8.21 – Questões acerca da realização de cópias de segurança

- *Efectua cópias de segurança (backups) da informação contida no seu computador pessoal?*
- *Com que periodicidade efectua cópias de segurança (backups)?*
- *Especifique a opção mais frequente para realização das cópias de segurança (backups)?*

A maioria dos Docentes e Técnicos opta por realizar cópias de segurança dos seus ficheiros, respectivamente 69,34% e 78,57%, enquanto que apenas 41,54% dos Não Docentes toma essa opção.

As opções divergem entre os três grupos, onde a opção mais relevante para os Docentes é ‘na conclusão de cada projecto/trabalho/etc.’, enquanto que os Não Docentes e Técnicos escolhem a opção de ‘raramente’, com qualquer destas opções a apresentar valores inferiores a 50% dos inquiridos.

Relativamente à escolha dos ficheiros a salvar, as opções assumidas também divergem, com relevância para o facto de 66,67% dos Técnicos não responderem a esta questão.

No respeitante à realização de cópias de segurança (*backups*), é interessante verificar que, em termos globais, a maioria dos inquiridos opta por as efectuar, mesmo assumindo algumas diferenças nas opções tomadas para a concretização dessas actividades.

- *Que tipo de dispositivo utiliza para efectuar as cópias de segurança (backups)?*
- *Especifique onde guarda as cópias de segurança (backups) que efectua.*

Relativamente ao dispositivo escolhido para a realização de *backups*, nota-se a opção maioritária pela utilização de ‘CD/DVD’ por qualquer dos três grupos, com a escolha de ‘Memórias *flash* amovíveis’ e de ‘Discos externos’ apresentar valores igualmente relevantes.

Neste âmbito constata-se que qualquer dos grupos opta pelo seu arquivamento na mesma sala onde se encontra o seu computador pessoal (valores entre os 58,76 e os 75,86%).

Tópicos a considerar relativamente à realização de cópias de segurança:

- ⇒ Opções assumidas na realização de *backups*.
- ⇒ Escolha dos dispositivos de *backup* e respectivo armazenamento.

8.5.2.6. Utilização do Computador Pessoal

Este grupo pretende obter um entendimento acerca da utilização que as Pessoas fazem dos seus computadores pessoais, procurando essencialmente perceber a frequência da sua utilização e o tipo de trabalhos efectuados.

Questões	Doc	NDoc	Téc
Com que frequência utiliza o seu computador pessoal?	B26)	B26)	B26)
Durante a utilização do seu computador pessoal, qual o tempo médio diário de utilização?	B28)	B28)	B28)
Caracterize a sua utilização do seu computador pessoal.	B27)	B27)	B27)
Que tipo de <i>software</i> utiliza no seu computador pessoal?	B29)	B29)	B29)

Tabela 8.22 – Questões acerca da utilização do computador pessoal

- *Com que frequência utiliza o seu computador pessoal?*
- *Durante a utilização do seu computador pessoal, qual o tempo médio diário de utilização?*

A frequência de utilização do computador pessoal encontra-se diferenciada entre Docentes, que referem maioritariamente a sua utilização diária (70,80%), e os Não Docentes e Técnicos que optam pela sua utilização quase diária (com 35,38 e 42,86% respectivamente) ou diária (com 32,31 e 28,57% respectivamente).

Em sentido similar é possível verificar que a média diária de utilização é mais elevada no grupo dos Docentes do que nos outros dois grupos.

- *Caracterize a sua utilização do seu computador pessoal.*
- *Que tipo de software utiliza no seu computador pessoal?*

Já no que diz respeito à caracterização da utilização do computador pessoal, constata-se que qualquer dos grupos assume como mais relevantes as opções de ‘Elaboração de relatórios e outros trabalhos’, ‘Pesquisas na Internet’ e ‘Envio/recepção de correio electrónico’.

Relativamente ao sistema operativo a opção de qualquer dos grupos é pelo Windows, tendência esta que é similar no *software* onde as principais opções recaem sobre a utilização dos aplicativos de folha de cálculo, de apresentações e de processamento de texto.

Tópicos a considerar relativamente à utilização do computador pessoal:

- ⇒ Tipo de utilização do computador pessoal.
- ⇒ *Software* utilizado no computador pessoal.

8.5.2.7. Percepção da Segurança do Computador Pessoal

Na análise das respostas às questões que implicam proceder a uma classificação, que tem apenas em conta o nível de conhecimentos do inquirido e a sua percepção, condicionada obviamente por esses conhecimentos de base e por aspectos culturais, opta-se por proceder à sua apreciação separada por cada um dos grupos distintos, apenas existindo uma apreciação global quando tal se justifique.

Questões	Doc	NDoc	Téc
Classifique a segurança do seu acesso? (6 para muito seguro e 1 para pouco seguro)	B8)	B8)	B8)
Classifique o grau de segurança da sua <i>password</i> . (6 para elevado e 1 para baixo)	B16)	B16)	B16)
Classifique o grau de segurança do seu computador pessoal. (6 para elevado e 1 para baixo)	B25)	B25)	B25)

Tabela 8.23 – Questões acerca da classificação de aspectos de segurança do computador pessoal

Os quadros 8.1, 8.2 e 8.3 apresentam as respostas obtidas a três questões concretas (identificadas na tabela anterior) relacionadas com a classificação de aspectos de segurança do computador pessoal, agrupando-se as respostas a cada uma das questões em função do tipo de inquirido(a): Docentes, Não Docentes e Técnicos.

A escolha deste tipo de apresentação dos dados obtidos deriva essencialmente de se pretender uma visualização integrada das respostas recolhidas, especialmente quando se está perante questões da mesma temática com uma forte interligação entre si, como é o caso presente.

Ao longo deste capítulo e em situações idênticas às apresentadas, serão aplicados os mesmos pressupostos.

B8) Classifique a segurança do seu acesso. (6 para muito seguro e 1 para pouco seguro)						
B16) Classifique o grau de segurança da sua <i>password</i> . (6 para elevado e 1 para baixo)						
B25) Classifique o grau de segurança do seu computador pessoal. (6 para elevado e 1 para baixo)						
Opções	Docentes		B8)		B16)	
			nº	%	nº	%
1			2	1,59	3	5,17
2			6	4,76	3	5,17
3			23	18,25	9	15,52
4			33	26,19	15	25,86
5			43	34,13	18	31,03
6			13	10,32	9	15,52
Não Responderam		6	4,76	1	1,72	8
Total de Respostas		126		58		137

Quadro 8.1 – Segurança do computador pessoal na perspectiva dos Docentes

B8) Classifique a segurança do seu acesso. (6 para muito seguro e 1 para pouco seguro)

B16) Classifique o grau de segurança da sua password. (6 para elevado e 1 para baixo)

B25) Classifique o grau de segurança do seu computador pessoal. (6 para elevado e 1 para baixo)

Opções	Não Docentes	B8)		B16)		B25)	
		nº	%	nº	%	nº	%
1		0	0,00	0	0,00	6	9,23
2		2	4,00	1	4,00	3	4,62
3		14	28,00	8	32,00	16	24,62
4		17	34,00	10	40,00	26	40,00
5		14	28,00	6	24,00	9	13,85
6		1	2,00	0	0,00	2	3,08
	Não Responderam	2	4,00	0	0,00	3	4,62
	Total de Respostas	50		25		65	

Quadro 8.2 – Segurança do computador pessoal na perspectiva dos Não Docentes

B8) Classifique a segurança do seu acesso. (6 para muito seguro e 1 para pouco seguro)							
B16) Classifique o grau de segurança da sua password. (6 para elevado e 1 para baixo)							
B25) Classifique o grau de segurança do seu computador pessoal. (6 para elevado e 1 para baixo)							
Opções	Técnicos	B8)		B16)		B25)	
		nº	%	nº	%	nº	%
1		1	7,69	0	0,00	0	0,00
2		0	0,00	0	0,00	0	0,00
3		1	7,69	1	12,50	2	14,29
4		5	38,46	2	25,00	5	35,71
5		4	30,77	3	37,50	3	21,43
6		2	15,38	2	25,00	4	28,57
Não Responderam		0	0,00	0	0,00	0	0,00
Total de Respostas		13		8		14	

Quadro 8.3 – Segurança do computador pessoal na perspectiva dos Técnicos

No respeitante aos aspectos associados à segurança, nomeadamente no acesso à Internet, da *password* e do próprio computador pessoal, constata-se que os Docentes optam pelos níveis 4 e 5, enquanto que os Não Docentes referem maioritariamente os níveis 3 e 4.

Relativamente aos Técnicos verifica-se a opção maioritária pelos níveis 4 e 5, com excepção dos aspectos associados com a segurança do computador pessoal, onde são referenciados os níveis 4 e 6.

Tópicos a considerar relativamente à percepção da segurança do computador pessoal:

⇒ Classificação atribuída aos níveis de segurança.

8.5.3. Resultados do Grupo C – Sistema Informático

A apreciação dos resultados deste grupo será efectuada em função da relação directa entre as questões colocadas e não apenas e só a sequência pela qual as mesmas foram apresentadas no questionário.

Neste grupo de questões serão abordados os seguintes temas:

- Funcionamento e mudanças no Sistema Informático;
- Conhecimentos e formação em informática;
- *Password* e mecanismos de acesso ao Sistema Informático;
- Utilização do correio electrónico;
- Acesso e utilização do Sistema Informático.

8.5.3.1. Funcionamento e Mudanças no Sistema Informático

As questões associadas nesta secção pretendem obter a percepção das Pessoas acerca das eventuais alterações efectuadas nos sistemas, assim como os seus níveis de participação das Pessoas nessas mudanças e sua satisfação com essas mesmas mudanças.

Questões	Doc	NDoc	Téc
Desde a sua entrada no Serviço/Escola existiu alguma mudança no Sistema Informático (<i>Hardware, Software, Procedimentos, etc.</i>)?	C1)	C1)	C1)
Foi solicitada a sua participação/participou de alguma forma nessas mudanças?	C2)	C2)	C2)
Caracterize a sua participação nessas mudanças.	C3)	C3)	C3)
Classifique o seu grau de participação nessas mudanças. (6 para elevado e 1 para baixo)	C4)	C4)	C4)
Classifique o seu grau de satisfação com as mudanças efectuadas. (6 para elevado e 1 para baixo)	C5)	C5)	C5)
Classifique a sua percepção acerca do funcionamento do Sistema Informático depois das mudanças efectuadas. (6 para melhorou muito e 1 para não melhorou)	C6)	C6)	C6)

Tabela 8.24 – Questões acerca do funcionamento e mudanças no sistema informático

- *Desde a sua entrada no Serviço/Escola existiu alguma mudança no Sistema Informático (Hardware, Software, Procedimentos, etc.)?*
- *Foi solicitada a sua participação/participou de alguma forma nessas mudanças?*
- *Caracterize a sua participação nessas mudanças.*

A grande maioria dos inquiridos já passou por situações de mudanças no sistema informático, embora a sua participação nessas actividades tenha um nível reduzido,

com excepção dos Técnicos, como seria expectável, cujo envolvimento é quase total mas divergente nas opções referenciadas por estes inquiridos.

Relativamente ao tipo de actividades desenvolvidas, constata-se que, com excepção dos Técnicos, a maioria das opções assumidas corresponde à ‘Aquisição de *Software/Hardware*’ e à ‘Definição/Implementação de Procedimentos’.

Os quadros 8.4, 8.5 e 8.6 apresentam as respostas obtidas a três questões concretas (identificadas na tabela anterior) relacionadas com a avaliação das mudanças, agrupando as respostas em função do tipo de inquirido(a): Docentes, Não Docentes e Técnicos.

No que diz respeito à avaliação dessas mudanças, nomeadamente grau de participação e satisfação e funcionamento do sistema, a análise das respostas foi efectuada considerando as perspectivas isoladas apresentadas por cada grupo de inquiridos.

C4) Classifique o seu grau de participação nessas mudanças. (6 para elevado e 1 para baixo)							
C5) Classifique o seu grau de satisfação com as mudanças efectuadas. (6 para elevado e 1 para baixo)							
C6) Classifique a sua percepção acerca do funcionamento do Sistema Informático depois das mudanças efectuadas. (6 para melhorou muito e 1 para não melhorou)							
	Docentes	C4)		C5)		C6)	
	Opções	nº	%	nº	%	nº	%
	1	5	12,50	2	1,69	3	2,54
	2	8	20,00	2	1,69	4	3,39
	3	10	25,00	16	13,56	14	11,86
	4	9	22,50	37	31,36	40	33,90
	5	5	12,50	49	41,53	47	39,83
	6	3	7,50	10	8,47	8	6,78
	<i>Não Responderam</i>	0	0,00	2	1,69	2	1,69
	Total de Respostas	40		118		118	

Quadro 8.4 – Avaliação das mudanças na perspectiva dos Docentes

C4) Classifique o seu grau de participação nessas mudanças. (6 para elevado e 1 para baixo)							
C5) Classifique o seu grau de satisfação com as mudanças efectuadas. (6 para elevado e 1 para baixo)							
C6) Classifique a sua percepção acerca do funcionamento do Sistema Informático depois das mudanças efectuadas. (6 para melhorou muito e 1 para não melhorou)							
Opções	C4)		C5)		C6)		
	nº	%	nº	%	nº	%	
1	1	3,33	1	1,79	3	5,36	
2	6	20,00	2	3,57	2	3,57	
3	8	26,67	14	25,00	10	17,86	
4	8	26,67	21	37,50	26	46,43	
5	4	13,33	15	26,79	8	14,29	
6	1	3,33	1	1,79	5	8,93	
Não Responderam	2	6,67	2	3,57	2	3,57	
Total de Respostas	30		56		56		

Quadro 8.5 – Avaliação das mudanças na perspectiva dos Não Docentes

C4) Classifique o seu grau de participação nessas mudanças. (6 para elevado e 1 para baixo)							
C5) Classifique o seu grau de satisfação com as mudanças efectuadas. (6 para elevado e 1 para baixo)							
C6) Classifique a sua percepção acerca do funcionamento do Sistema Informático depois das mudanças efectuadas. (6 para melhorou muito e 1 para não melhorou)							
Opções	C4)		C5)		C6)		
	nº	%	nº	%	nº	%	
1	0	0,00	0	0,00	0	0,00	
2	0	0,00	1	7,14	2	14,29	
3	2	15,38	2	14,29	0	0,00	
4	3	23,08	4	28,57	6	42,86	
5	3	23,08	6	42,86	6	42,86	
6	5	38,46	1	7,14	0	0,00	
Não Responderam	0	0,00	0	0,00	0	0,00	
Total de Respostas	13		14		14		

Quadro 8.6 – Avaliação das mudanças na perspectiva dos Técnicos

Relativamente aos Docentes constata-se um reduzido grau de participação nas mudanças (níveis 3 e 4), com grau de satisfação com essas mudanças a ser relativamente elevado (níveis 4 e 5), verificando-se idêntica percepção acerca das melhorias para o sistema informático.

No respeitante aos outros inquiridos, verifica-se que o grupo dos Não Docentes apresenta uma classificação assente essencialmente nos níveis 3 e 4. O grupo dos

Técnicos refere um elevado grau de participação, classificando todavia os outros aspectos nos níveis 4 e 5.

Tópicos a considerar acerca do funcionamento e mudanças no Sistema Informático:

⇒ Aumentar a participação das Pessoas nas mudanças organizacionais.

8.5.3.2. *Conhecimentos e Formação em Informática*

Esta secção engloba aspectos associados aos conhecimentos na utilização de computadores e acções de formação efectuadas, procedendo-se aqui a uma separação pelos diversos grupos profissionais, quando tal se considerou necessário, surgindo por isso questões diferenciadas por cada tipo de questionário.

Questões	Doc	NDoc	Téc
Já tinha utilizado computadores antes de ser admitido(a) no IPS/Escola?	-	C7)	-
Realizou algum(uns) curso(s) de formação em Informática/Sistemas de Informação antes de ser admitido(a) no IPS/ Escola?	-	C8)	-
Qual a frequência média anual das acções de formação em informática que recebeu?	-	-	C7)
Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)	-	-	C8)
Classifique o seu grau de conhecimentos na área da Informática/ Sistemas de Informação. (6 para elevado e 1 para baixo)	C7)	C9)	C9)

Tabela 8.25 – Questões acerca dos conhecimentos e formação em informática

- *Já tinha utilizado computadores antes de ser admitido(a) no IPS/Escola?*
- *Realizou algum(uns) curso(s) de formação em Informática/Sistemas de Informação antes de ser admitido(a) no IPS/Escola?*

Das respostas a estas questões, colocadas apenas aos Não Docentes, constata-se que a grande maioria possuía experiência prévia na utilização de computadores (83,54%), enquanto que de entre estes apenas 60,61% já tinham participado em acções de formação em Informática/Sistemas de Informação.

- *Qual a frequência média anual das acções de formação em informática que recebeu?*
- *Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)*

As respostas a estas questões, colocadas apenas aos Técnicos, permitem verificar que a média anual de acções de formação frequentada se situa entre uma (35,71%) e duas (50,00%), atribuindo à sua relevância valores entre 5 (50,00%) e 6 (28,57%).

C7) Classifique o seu grau de conhecimentos na área da Informática/Sistemas de Informação. (6 para elevado e 1 para baixo)						
Opções	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	6	4,38	1	1,52	0	0,00
2	8	5,84	1	1,52	0	0,00
3	47	34,31	16	24,24	0	0,00
4	34	24,82	39	59,09	4	28,57
5	28	20,44	8	12,12	7	50,00
6	11	8,03	0	0,00	3	21,43
Não Responderam	3	2,19	1	1,52	0	0,00
Total de Respostas	137		66		14	

Quadro 8.7 – Avaliação dos conhecimentos em informática

A avaliação dos inquiridos acerca dos respectivos conhecimentos em Informática/Sistemas de Informação realça a diferenciação entre os diversos grupos, visto que os Docentes assumem como referência os níveis 3 (34,31%) e 4 (24,82%), os Não Docentes apresentam também os níveis 3 (24,24%) e 4 (59,09%), só que com valores percentuais distintos, já os Técnicos mencionam os níveis 4 (28,57%) e 5 (50,00%).

Tópicos a considerar relativamente a conhecimentos e formação em informática:

⇒ Definir e implementar plano de formação na área de informática.

8.5.3.3. Password e Mecanismos de Acesso ao Sistema Informático

De forma similar ao já efectuado no grupo B, nesta secção foram agrupadas as questões relacionadas com a utilização de *passwords* para acesso aos sistemas da instituição e o modo como utilizam essas *passwords*, considerando também a forma como efectuem a sua gestão e as implicações acerca dos aspectos de confidencialidade e segurança.

Nesta secção foram agrupadas, além das anteriormente referidas, questões próprias da utilização de sistemas partilhados por centenas de Pessoas.

Questões	Doc	NDoc	Téc
Dispõe de acesso ao Sistema Informático?	C8)	C10)	-
O acesso ao Sistema Informático é feito através de <i>password</i> ?	C9)	C11)	C10)
Além da <i>password</i> , especifique que tipo(s) de mecanismo(s) está(ão) implementado(s) para acesso ao Sistema Informático.	C18)	C20)	C20)
Já alterou a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático?	C10)	C12)	C11)
Com que frequência altera a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático?	C11)	C13)	C12)
Que opções efectua na escolha de nova(s) <i>password(s)</i> ?	C12)	C14)	C13)
Na definição de nova(s) <i>password(s)</i> opta por:	C13)	C15)	C14)
Qual o processo que utiliza para guardar a(s) sua(s) <i>password(s)</i> ?	C14)	C16)	C15)
Com quantas pessoas partilha a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático?	C15)	C17)	C16)
Utiliza a mesma <i>password</i> para diversas aplicações/ sistemas?	C16)	C18)	C18)
Quantas <i>passwords</i> de acesso ao Sistema Informático utiliza?	-	-	C17)
Classifique o grau de segurança da(s) sua(s) <i>password(s)</i> . (6 para elevado e 1 para baixo)	C17)	C19)	C19)

Tabela 8.26 – Questões acerca da *password* e mecanismos de acesso ao sistema informático

- *Dispõe de acesso ao Sistema Informático?*
- *O acesso ao Sistema Informático é feito através de password?*
- *Além da password, especifique que tipo(s) de mecanismo(s) está(ão) implementado(s) para acesso ao Sistema Informático.*

Através deste grupo de questões torna-se claro que a grande maioria das Pessoas possui acesso ao Sistema Informático, utilizando *password* como meio quase exclusivo de acesso.

É ainda de referir que, relativamente à existência de outro tipo de acesso, a maioria dos inquiridos refere a inexistência de qualquer outro, considerando-se irrelevantes as outras opções mencionadas.

- *Já alterou a(s) sua(s) password(s) de acesso ao Sistema Informático?*
- *Com que frequência altera a(s) sua(s) password(s) de acesso ao Sistema Informático?*

No respeitante à alteração da *password*, verifica-se que a maioria dos inquiridos já procedeu à sua realização pelo menos uma vez, registando-se todavia uma frequência de alteração relativamente baixa (‘Raramente’ e ‘Semestralmente/Anualmente’).

➤ *Que opções efectua na escolha de nova(s) password(s)?*

➤ *Na definição de nova(s) password(s) opta por:*

Relativamente às opções tomadas para definição das novas *passwords*, a opção por uma combinação de números e letras é claramente maioritária nos grupos dos Docentes e dos Técnicos, enquanto que os Não Docentes apresentam um leque alargado de escolhas. Todavia, deve referenciar-se a opção algo frequente de ‘nomes de familiares’.

Já no que diz respeito à dimensão das *passwords*, a opção maioritária corresponde à escolha de um ‘número aleatório de caracteres entre o máximo e o mínimo’ permitidos.

➤ *Qual o processo que utiliza para guardar a(s) sua(s) password(s)?*

Acerca desta questão, a ‘memorização’ é o processo referido como o mais usual, com valores superiores a 85% em qualquer dos três grupos de inquiridos.

➤ *Com quantas pessoas partilha a(s) sua(s) password(s) de acesso ao Sistema Informático?*

➤ *Utiliza a mesma password para diversas aplicações/sistemas?*

➤ *Quantas passwords de acesso ao Sistema Informático utiliza?*

No respeitante à partilha da *password*, constata-se que a grande maioria não partilha a sua *password*, com um número significativo de Não Docentes (cerca de 45%) a efectuar a partilha da sua *password*.

Já a utilização da mesma *password* para diversas aplicações é apresentada como afirmativa para a maioria dos Docentes e Técnicos, com a opção contrária a ser tomada pelos Não Docentes.

Face à especificidade das suas funções esta é uma questão que apenas foi colocada aos Técnicos, verificando-se que a maioria opta pela utilização de 3 ou mais *passwords* (cerca de 71%).

C17) Classifique o grau de segurança da(s) sua(s) <i>password</i> (s). (6 para elevado e 1 para baixo)							
Opções	Docentes		Não Docentes		Técnicos		
	nº	%	nº	%	nº	%	
1	2	1,50	0	0,00	0	0,00	
2	9	6,77	3	4,05	1	7,14	
3	21	15,79	18	24,32	1	7,14	
4	51	38,35	29	39,19	3	21,43	
5	32	24,06	17	22,97	8	57,14	
6	11	8,27	4	5,41	1	7,14	
<i>Não Responderam</i>	7	5,26	3	4,05	0	0,00	
Total de Respostas	133		74		14		

Quadro 8.8 – Grau de segurança da *password*

No respeitante à percepção das Pessoas acerca do grau de segurança das respectivas *passwords*, refira-se que os Docentes e os Técnicos possuem opções similares, escolhendo maioritariamente os níveis 4 e 5 embora com percentagens inversas, enquanto que os Não Docentes escolhem maioritariamente os níveis 3 e 4.

Tópicos a considerar relativamente à *password* e mecanismos de acesso ao Sistema Informático:

⇒ Definir e implementar procedimentos acerca dos acessos ao sistema e dos respectivos mecanismos de acesso.

8.5.3.4. Utilização do Correio Electrónico

Nesta secção pretende-se aferir os níveis de utilização do correio electrónico e da sua segurança.

Questões	Doc	NDoc	Téc
Possui algum endereço de correio electrónico associado ao Sistema Informático?	C19)	C21)	C21)
Além desse, quantos endereços de correio electrónico possui?	C20)	C22)	C22)
Utiliza a mesma <i>password</i> para acesso ao correio electrónico e ao Sistema Informático?	C21)	C23)	C23)
Existe implementado algum sistema de filtragem de mensagens de correio electrónico?	C22)	C24)	C24)

Tabela 8.27 – Questões acerca da utilização do correio electrónico

- *Possui algum endereço de correio electrónico associado ao Sistema Informático?*
- *Além desse, quantos endereços de correio electrónico possui?*

Nestas questões verifica-se que a grande maioria dos inquiridos possui um endereço de correio electrónico associado ao Sistema Informático, registando-se todavia que a maioria possui mais um ou dois endereços de correio electrónico.

- *Utiliza a mesma password para acesso ao correio electrónico e ao Sistema Informático?*
- *Existe implementado algum sistema de filtragem de mensagens de correio electrónico?*

Relativamente à segurança associada ao correio electrónico, constata-se que a maioria dos inquiridos opta por utilizar *password* distinta da utilizada para acesso ao sistema informático, mencionando ainda que a maioria utiliza sistema de filtragem de mensagens de correio electrónico.

Tópicos a considerar relativamente à utilização do correio electrónico:

⇒ Definir, implementar e divulgar procedimentos acerca da utilização do correio electrónico.

8.5.3.5. Acesso e Utilização do Sistema Informático

Esta secção agrupa o conjunto de questões relativas aos acessos ao Sistema Informático, considerando a sua frequência de utilização, os tempos médios de duração desses mesmos acessos.

Estão ainda incluídos os acessos a áreas privada nos servidores de cada unidade orgânica ou serviço, o acesso e utilização de impressão partilhada assim como também os aspectos de segurança associados à utilização que é feita desses recursos, nomeadamente o controlo da impressão e recolha dos documentos que são impressos pelos diversos utilizadores.

Questões	Doc	NDoc	Téc
Com que frequência acede ao Sistema Informático?	C23)	C25)	C25)
Durante a utilização do Sistema Informático, qual o tempo médio diário de cada utilização?	C24)	C26)	C26)
Caracterize a sua utilização do Sistema Informático.	C26)	C28)	C28)
Que tipo de <i>software</i> utiliza?	C25)	C27)	C27)
Utiliza alguma área de trabalho privada no(s) servidor(es) do Sistema Informático?	C27)	C29)	C29)
Que tipo de informação guarda nessa área de trabalho?	C28)	C30)	C30)
Já perdeu informação guardada nessa área de trabalho?	C29)	C31)	C31)
Que acção tomou para recuperar essa informação?	C30)	C32)	C32)
O que aconteceu relativamente a essa situação?	C31)	C33)	C33)
Possui acesso à impressão de documentos através do Sistema Informático utilizando impressora(s) partilhada(s)?	C32)	C34)	C34)
Quando não consegue imprimir documentos através da(s) impressora(s) partilhada(s) qual a atitude que assume?	C33)	C35)	C35)
Que atitude toma quando encontra documentos que não são seus na(s) impressora(s) partilhada(s)?	C34)	C36)	C36)
Que atitude toma quando não encontra documentos seus que mandou imprimir na(s) impressora(s) partilhada(s)?	C35)	C37)	C37)
Consideraria a hipótese de aceder ao Sistema Informático a partir da sua residência ou de outro local onde trabalhe regularmente?	C36)	C38)	C38)

Tabela 8.28 – Questões acerca do acesso e utilização do sistema informático

- *Com que frequência acede ao Sistema Informático?*
- *Durante a utilização do Sistema Informático, qual o tempo médio diário de cada utilização?*

A utilização diária do Sistema Informático é claramente maioritária por parte dos Não Docentes e Técnicos, encontrando-se diferenciada entre Docentes, que referem a sua utilização diária (52,99%), e os que optam pela sua utilização quase diária (38,81%).

Em sentido similar é possível verificar que a média diária de utilização é mais baixa no grupo dos Docentes do que nos outros dois grupos.

- *Caracterize a sua utilização do Sistema Informático.*
 - *Que tipo de software utiliza?*
- Já no que diz respeito à caracterização da utilização do Sistema Informático, constata-se que qualquer dos grupos assume como menos relevante a opção de ‘Análise estatística/projecções’.

Relativamente ao sistema operativo a opção de qualquer dos grupos é pelo Windows, tendência esta que é similar nos aplicativos de *software* onde as principais opções recaem sobre a utilização dos aplicativos de folha de cálculo, de apresentações e de processamento de texto.

- *Utiliza alguma área de trabalho privada no(s) servidor(es) do Sistema Informático?*
- *Que tipo de informação guarda nessa área de trabalho?*

A maioria dos Docentes e dos Técnicos utilizam uma área de trabalho privada, com opção contrária a ser assumida por parte dos Não Docentes.

No que diz respeito ao tipo de informação guarda, verifica-se que a opção menos escolhida é a de ‘Ficheiros pessoais’.

- *Já perdeu informação guardada nessa área de trabalho?*
- *Que acção tomou para recuperar essa informação?*
- *O que aconteceu relativamente a essa situação?*

No que diz respeito à informação guardada nessa área, verifica-se que as suas perdas são mínimas, e quando existem têm sido quase sempre possível efectuar a sua recuperação.

- *Possui acesso à impressão de documentos através do Sistema Informático utilizando impressora(s) partilhada(s)?*
- *Quando não consegue imprimir documentos através da(s) impressora(s) partilhada(s) qual a atitude que assume?*

Já relativamente ao acesso a impressoras partilhadas, verifica-se que a maioria dos inquiridos procede à sua utilização, optando por, quando não consegue imprimir qualquer documento, verificar se a impressora tem algum problema e tentar imprimir novamente, seja na mesma impressora ou em outra disponível.

- *Que atitude toma quando encontra documentos que não são seus na(s) impressora(s) partilhada(s)?*
- *Que atitude toma quando não encontra documentos seus que mandou imprimir na(s) impressora(s) partilhada(s)?*

Acerca da segurança dos documentos impressos ou por imprimir, constata-se que a maioria dos inquiridos, quando encontra documentos que não são seus na impressora ‘Tenta entregar/entregou ao seu proprietário’ ou ‘Deixa junto à impressora’.

No caso de não encontrar documentos seus, optam por imprimir novamente ou verificar se aguardam por impressão, realçando-se no entanto que a maioria dos Técnicos refere que essa situação nunca aconteceu.

- *Consideraria a hipótese de aceder ao Sistema Informático a partir da sua residência ou de outro local onde trabalhe regularmente?*

Relativamente à possibilidade de aceder remotamente ao Sistema Informático, a maioria das respostas refere a opção afirmativa.

Tópicos a considerar relativamente ao acesso e utilização do Sistema Informático:

- ⇒ Definir e implementar procedimentos de utilização dos activos do sistema.
- ⇒ Publicar e divulgar o documento de suporte às políticas de segurança.

8.5.4. Resultados do Grupo D – Segurança da Informação

A apreciação dos resultados deste grupo será efectuada tendo em atenção a relação directa entre as questões colocadas e não apenas e só a sequência pela qual as mesmas foram apresentadas no questionário.

Neste contexto serão abordados os seguintes temas:

- Políticas de segurança da informação e do Sistema Informático;
- Mecanismos de protecção do Sistema Informático;
- Realização de cópias de segurança;
- Percepção da facilidade de acesso ao Sistema Informático;
- Controlo dos activos do sistema e da sua utilização;
- Percepção da segurança do Sistema Informático.

8.5.4.1. Políticas de Segurança da Informação e do Sistema Informático

Esta secção agrupa as questões associadas às políticas de segurança dos Sistemas Informáticos, nomeadamente o seu desenvolvimento e abrangência.

Neste conjunto de questões procura-se também conhecer o envolvimento das Pessoas nas actividades relacionadas com a definição e/ou implementação dessas mesmas políticas.

Questões	Doc	NDoc	Téc
Existem políticas de segurança do Sistema Informático?	D1)	D1)	D1)
Como tomou conhecimento dessas políticas?	D2)	D2)	D2)
Dos aspectos a seguir mencionados, especifique quais são abrangidos pelas políticas definidas.	D3)	D3)	D3)
Participou na elaboração/alteração dessas políticas?	D4)	D4)	D4)
Caracterize a sua participação nessas actividades.	D5)	D5)	D5)
Classifique o seu grau de participação nessas actividades. (6 para elevado e 1 para baixo)	D6)	D6)	D6)

Tabela 8.29 – Questões acerca das políticas de segurança da informação e do sistema informático

- *Existem políticas de segurança do Sistema Informático?*
- *Como tomou conhecimento dessas políticas?*
- *Dos aspectos a seguir mencionados, especifique quais são abrangidos pelas políticas definidas.*

Relativamente à existência de políticas de segurança, constata-se que a maioria dos Docentes e Não Docentes (56,72% e 51,32% respectivamente) desconhece a existência de políticas, enquanto que a quase totalidade dos Técnicos (92,86%) confirma a sua existência.

No respeitante à forma como tomaram conhecimento dessas políticas, verifica-se que a maioria dos inquiridos refere ter sido através dos serviços de informática ou do responsável do serviço e por informação de colega.

As questões mais referenciadas pelos inquiridos acerca dos aspectos abrangidos pelas políticas de segurança são a ‘definição de acessos ao sistema’, a ‘utilização do correio electrónico’ e ‘acesso aos servidores’.

- *Participou na elaboração/alteração dessas políticas (normas/regulamentos/regras/procedimentos)?*
- *Caracterize a sua participação nessas actividades.*

No respeitante à participação dos inquiridos nas actividades relacionadas com a elaboração/alteração das políticas de segurança esta é identificada como muito baixa, existindo participações muito diversas por parte das poucas Pessoas que foram envolvidas.

D6) Classifique o seu grau de participação nessas actividades. (6 para elevado e 1 para baixo)							
Opções	Docentes		Não Docentes		Técnicos		
	nº	%	nº	%	nº	%	
1	1	16,67	0	0,00	0	0,00	
2	0	0,00	1	20,00	0	0,00	
3	2	33,33	1	20,00	0	0,00	
4	1	16,67	1	20,00	3	60,00	
5	0	0,00	0	0,00	1	20,00	
6	0	0,00	0	0,00	1	20,00	
Não Responderam	2	33,33	2	40,00	0	0,00	
Total de Respostas	6		5		5		

Quadro 8.9 – Grau de participação na elaboração/alteração das políticas de segurança

No que respeita à classificação dessa participação, os resultados obtidos divergem bastante, devido essencialmente ao reduzido número de Pessoas que participaram nestas actividades.

Tópicos a considerar relativamente às políticas de segurança da informação e do Sistema Informático:

- ⇒ Divulgação do documento da política de segurança e outros relacionados.
- ⇒ Envolvimento das Pessoas na elaboração das políticas.

8.5.4.2. Mecanismos de Protecção do Sistema Informático

Esta secção agrupa as questões relacionadas com mecanismos relacionados com a segurança da informação, além da *password*.

Questões	Doc	NDoc	Téc
Após o <i>login</i> no acesso ao Sistema Informático, existe definido algum tempo limite para que a sessão de trabalho esteja activa?	D10)	D10)	D10)
Durante o tempo em que tem activa a sua sessão de trabalho, utiliza algum mecanismo de protecção de ecrã para quando não está a utilizar o computador?	D11)	D11)	D11)
Além da <i>password</i> que mecanismo/ferramenta/software é utilizado para protecção do Sistema Informático.	-	-	D12)
Com que frequência se actualiza esse mecanismo/ferramenta/software.	-	-	D13)

Tabela 8.30 – Questões acerca dos mecanismos de protecção do sistema informático

- *Após o login no acesso ao Sistema Informático, existe definido algum tempo limite para que a sessão de trabalho esteja activa?*
- *Durante o tempo em que tem activa a sua sessão de trabalho, utiliza algum mecanismo de protecção de ecrã para quando não está a utilizar o computador?*

Relativamente à existência de tempos limites para a sessão se encontrar activa, a maioria dos inquiridos refere que não existe ou que não sabe da sua existência.

No respeitante à da utilização de um mecanismo de protecção de ecrã enquanto a sessão está activa, a maioria dos Docentes (53,73%) refere que não a utiliza, com a opção contrária a ser tomada pelos Não Docentes (55,26%) e pelos Técnicos (92,86%).

- *Além da password que mecanismo/ferramenta/software é utilizado para protecção do Sistema Informático.*
- *Com que frequência se actualiza esse mecanismo/ferramenta/software.*

Este grupo de questões que diz apenas respeito aos Técnicos, situações relacionadas apenas com as suas actividades, permite constatar que os mecanismos mais utilizados são ‘Antivirus’ (100,00%), ‘Antispyware’ (92,86%) e ‘Firewall’ (85,71%), que são actualizados sempre que existe uma actualização por parte do fornecedor.

Tópicos a considerar relativamente aos mecanismos de protecção do Sistema Informático:

⇒ Definir gama de mecanismos de segurança a utilizar.

8.5.4.3. Realização de Cópias de Segurança

Esta secção pretende identificar as políticas de *backups*, e as diversas opções tomadas para a sua concretização.

Questões	Doc	NDoc	Téc
Está implementada alguma política de segurança da informação contida nos servidores?	-	-	D14)
Essa política de cópias de segurança da informação estabelece regras em função da criticidade da informação?	-	-	D15)
Caracterize essas regras para as cópias de segurança?	-	-	D16)
Com que periodicidade são efectuadas as cópias de segurança da informação crítica.	-	-	D17)
Que tipo de dispositivo é utilizado para efectuar as cópias de segurança.	-	-	D18)
Onde são guardadas as cópias de segurança efectuadas.	-	-	D19)

Tabela 8.31 – Questões acerca da realização de cópias de segurança

- *Está implementada alguma política de segurança da informação contida nos servidores?*
- *Essa política de cópias de segurança da informação estabelece regras em função da criticidade da informação?*
- *Caracterize essas regras para as cópias de segurança?*
- *Com que periodicidade são efectuadas as cópias de segurança da informação crítica.*

A análise deste grupo permite constatar que existem políticas de segurança, com estas a serem maioritariamente definidas em função da criticidade da informação, englobando a totalidade da informação, mas com periodicidades distintas em função da criticidade identificada.

Em termos de periodicidade, a informação crítica é objecto de cópias de segurança diárias.

- *Que tipo de dispositivo é utilizado para efectuar as cópias de segurança.*
- *Onde são guardadas as cópias de segurança efectuadas.*

Relativamente ao dispositivo escolhido, a opção maioritária é a utilização de ‘Tapes’, com a escolha do ‘Disco do servidor’ e de ‘Discos externos’ a serem preferências igualmente relevantes.

Neste âmbito constata-se que a opção de arquivamento mais escolhida é na ‘sala de servidores’ (50,00%), tal como também é relevante a opção por ‘outro espaço do Serviço’ (28,57%).

Tópicos a considerar relativamente à realização de cópias de segurança:

⇒ Política de *backups*.

8.5.4.4. Percepção da Facilidade de Acesso ao Sistema Informático

Esta secção pretende caracterizar a percepção das Pessoas acerca da facilidade de acesso físico ao Sistema Informático em diversos locais de acesso.

Considerando a diversidade de formações dos inquiridos, a análise das respostas será inicialmente efectuada de forma separada por cada um dos grupos e só depois de forma agregada, considerando nesta situação apenas os valores percentuais obtidos.

D15) Classifique a facilidade de acesso físico ao Sistema Informático (6 para muito difícil e 1 para muito fácil), nos seguintes pontos de acesso:							
	1	2	3	4	5	6	NR
(a) Sala de servidores	8,21	4,48	8,96	14,18	16,42	23,13	24,63
(b) Serviços de Informática	7,46	14,18	11,94	17,91	18,66	9,70	20,15
(c) Serviços administrativos/académicos/etc.	6,72	13,43	12,69	21,64	14,93	8,21	22,39
(d) Gabinetes de colegas	10,45	14,18	17,91	14,93	15,67	6,72	20,15
(e) Salas de reunião	12,69	11,94	15,67	17,91	8,96	6,72	26,12
(f) Átrios/corredores	23,13	12,69	10,45	13,43	8,96	6,72	24,63
(g) Área circundante do Serviço/Escola	20,15	9,70	13,43	11,94	11,19	7,46	26,12
(h) Salas de aula	13,43	14,18	19,40	14,93	12,69	8,96	16,42
(i) Laboratórios de Informática	11,19	13,43	16,42	16,42	15,67	4,48	22,39
(j) Salas de informática para alunos	15,67	15,67	17,91	8,21	10,45	6,72	25,37

Quadro 8.10 – Percepção dos Docentes acerca da facilidade de acesso ao sistema

O acesso referenciado como mais difícil é a ‘sala de servidores’, enquanto que o mais fácil corresponde aos ‘átrios/corredores’.

Deve todavia referenciar-se a grande dispersão das respostas pelos diversos níveis de classificação, e ainda que existe um número apreciável de Docentes que não responderam a esta questão.

D15) Classifique a facilidade de acesso físico ao Sistema Informático (6 para muito difícil e 1 para muito fácil), nos seguintes pontos de acesso:							
	1	2	3	4	5	6	NR
(a) Sala de servidores	5,26	5,26	14,47	10,53	17,11	31,58	15,79
(b) Serviços de Informática	9,21	6,58	23,68	23,68	14,47	9,21	13,16
(c) Serviços administrativos/académicos/etc.	9,21	10,53	25,00	21,05	11,84	7,89	14,47
(d) Gabinetes de colegas	13,16	13,16	19,74	22,37	7,89	5,26	18,42
(e) Salas de reunião	9,21	21,05	23,68	10,53	7,89	10,53	17,11
(f) Átrios/corredores	18,42	15,79	22,37	7,89	5,26	9,21	21,05
(g) Área circundante do Serviço/Escola	7,89	10,53	23,68	14,47	5,26	13,16	25,00
(h) Laboratórios de Informática	3,95	10,53	21,05	18,42	9,21	11,84	25,00

Quadro 8.11 – Percepção dos Não Docentes acerca da facilidade de acesso ao sistema

O acesso referenciado como mais difícil é a ‘sala de servidores’, enquanto que o mais fácil corresponde aos ‘átrios/corredores’.

Deve todavia referenciar-se a grande diversidade de classificações, e ainda que existe um número apreciável de Não Docentes que não classificaram alguns locais de acesso.

D25) Classifique a facilidade de acesso físico ao Sistema Informático (6 para muito difícil e 1 para muito fácil), nos seguintes pontos de acesso:							
	1	2	3	4	5	6	NR
(a) Sala de servidores	0,00	0,00	7,14	0,00	35,71	57,14	0,00
(b) Serviços de Informática	0,00	0,00	14,29	21,43	50,00	14,29	0,00
(c) Serviços administrativos/académicos/etc.	0,00	7,14	28,57	50,00	7,14	7,14	0,00
(d) Gabinetes de colegas	0,00	0,00	28,57	28,57	35,71	7,14	0,00
(e) Salas de reunião	0,00	0,00	42,86	42,86	0,00	14,29	0,00
(f) Átrios/corredores	0,00	7,14	42,86	35,71	7,14	7,14	0,00
(g) Área circundante do Serviço/Escola	28,57	21,43	14,29	14,29	7,14	7,14	7,14
(h) Laboratórios de Informática	28,57	21,43	7,14	21,43	7,14	7,14	7,14

Quadro 8.12 – Percepção dos Técnicos acerca da facilidade de acesso ao sistema

O acesso referenciado como mais difícil é a ‘sala de servidores’, enquanto que os mais fáceis correspondem à ‘área circundante do Serviço/Escola’ e aos ‘laboratórios de informática’.

Contrariamente aos outros grupos, verifica-se aqui uma maior convergência nas opções e que a grande maioria procedeu à classificação de todos os locais de acesso.

Tópicos a considerar relativamente à percepção da facilidade de acesso ao Sistema Informático:

⇒ Elaborar e divulgar documento de utilização do Sistema Informático.

8.5.4.5. Controlo dos Activos do Sistema e da sua Utilização

Esta secção agrega as questões relacionadas com a percepção das Pessoas acerca do controlo da utilização adequada do sistema e dos respectivos activos.

Questões	Doc	NDoc	Téc
Já presenciou alguma(s) violação(ões) da segurança do Sistema Informático (por exemplo destruição/roubo de equipamentos, entradas em locais interditos, utilização de ficheiros/ <i>passwords</i> de outras pessoas, etc.)?	D8)	D8)	D8)
Que atitude tomou quando presenciou essa(s) violação(ões)?	D9)	D9)	D9)
Nos locais onde tem acesso ao Sistema Informático, especifique que actividades estão proibidas.	D16)	D26)	D26)
Existem registos do <i>hardware</i> e <i>software</i> existente no Serviço?	-	-	D20)
Com que periodicidade são actualizados esses registos.	-	-	D21)

Tabela 8.32 – Questões acerca do controlo dos activos do sistema e da sua utilização

- *Já presenciou alguma(s) violação(ões) da segurança do Sistema Informático (por exemplo destruição/roubo de equipamentos, entradas em locais interditos, utilização de ficheiros/passwords de outras pessoas, etc.)?*

- *Que atitude tomou quando presenciou essa(s) violação(ões)?*

Relativamente a violações da segurança da informação, constata-se que a maioria dos inquiridos referenciou não ter assistido a qualquer violação, com 42,86% dos Técnicos a assumir já ter assistido a violações da segurança do sistema.

As atitudes mais referenciadas por aqueles que presenciaram violações da segurança do sistema são ‘advertir o(a) infractor(a)’ e ainda informar os responsáveis institucionais ou os serviços de informática.

- *Nos locais onde tem acesso ao Sistema Informático, especifique que actividades estão proibidas.*

Em termos das actividades proibidas, referira-se que os inquiridos mencionam maioritariamente ‘Fumar’, ‘Movimentar computadores instalados’ e ‘Instalar/desinstalar software’.

- *Existem registos do hardware e software existente?*

- *Com que periodicidade são actualizados esses registos.*

No que diz respeito ao controlo dos activos do sistema, questões apenas colocadas aos Técnicos, a grande maioria refere a existência de registos, mencionando, também maioritariamente, que a sua actualização se realiza ‘Sempre que necessário’.

Tópicos a considerar relativamente ao controlo dos activos do sistema e da sua utilização:

- ⇒ Definir e divulgar procedimentos de actuação em caso de ocorrerem violações de segurança.
- ⇒ Definir e divulgar os procedimentos adequados ao controlo dos activos.

8.5.4.6. Percepção da Segurança do Sistema Informático

Esta secção agrega as questões relacionadas com a percepção das Pessoas acerca da segurança do Sistema Informático, considerando a sua participação em acções formativas e o seu entendimento sobre o nível de segurança, e ainda o nível de classificação atribuído.

Relativamente ao conjunto de questões acerca dos aspectos relevantes para a segurança e dos impactos de diversos tipos de ameaças, a análise das respostas será inicialmente efectuada de forma separada e só depois de forma agregada, considerando a diversidade de formações dos inquiridos.

Os resultados a expor de forma agregada serão apresentados apenas com os valores percentuais obtidos.

Questões	Doc	NDoc	Téc
Caracterize a sua participação nas acções de sensibilização para a problemática da segurança da informação?	D7)	D7)	D7)
Classifique a segurança do Sistema Informático. (6 para muito seguro e 1 para pouco seguro)	D12)	D12)	D22)
Classifique em que medida considera que a segurança do Sistema Informático é ou pode ser importante para as suas actividades laborais/lectivas e de investigação. (6 para muito importante e 1 para pouco importante)	D14)	D14)	D24)
Classifique, relativamente à segurança do Sistema Informático (6 para muito importante e 1 para pouco importante), os seguintes aspectos:	D13)	D13)	D23)
Classifique, de acordo com o impacto na segurança do Sistema Informático (6 para muito importante e 1 para pouco importante), os seguintes tipos de ameaças.	D17)	D17)	D27)

Tabela 8.33 – Questões acerca da percepção da segurança do sistema informático

➤ *Caracterize a sua participação nas acções de sensibilização para a problemática da segurança da informação?*

No respeitante à participação em acções de sensibilização de segurança da informação, a maioria dos Docentes e Não Docentes refere não ter tido conhecimento de qualquer acção, enquanto que os Técnicos menciona o conhecimento da sua existência.

No contexto apresentado é importante relevar o facto de nem todos os Técnicos terem participado nessas acções.

Os quadros 8.13, 8.14 e 8.15 apresentam as respostas obtidas a duas questões concretas (identificadas na tabela anterior) relacionadas com a classificação da segurança do Sistema Informático, agrupando as respostas em função do tipo de inquirido(a): Docentes, Não Docentes e Técnicos.

De forma similar são também apresentadas as respostas obtidas por cada grupo de inquiridos relativamente à importância da segurança para as actividades que desenvolvem.

D12) Classifique a segurança do Sistema Informático. (6 para muito seguro e 1 para pouco seguro)					
D14) Classifique em que medida considera que a segurança do Sistema Informático é ou pode ser importante para as suas actividades laborais/lectivas e de investigação. (6 para muito importante e 1 para pouco importante)					
	Docentes	D12)		D14)	
		nº	%	nº	%
	1	1	0,75	1	0,75
	2	4	2,99	1	0,75
	3	20	14,93	10	7,46
	4	65	48,51	19	14,18
	5	30	22,39	45	33,58
	6	3	2,24	53	39,55
	<i>Não Responderam</i>	11	8,21	5	3,73
	Total de Respostas	134		134	

Quadro 8.13 – Percepção dos Docentes acerca da segurança do sistema

D12) Classifique a segurança do Sistema Informático. (6 para muito seguro e 1 para pouco seguro)					
D14) Classifique em que medida considera que a segurança do Sistema Informático é ou pode ser importante para as suas actividades laborais/lectivas e de investigação. (6 para muito importante e 1 para pouco importante)					
	Não Docentes	D12)		D14)	
		nº	%	nº	%
	1	0	0,00	0	0,00
	2	5	6,58	1	1,32
	3	20	26,32	1	1,32
	4	23	30,26	12	15,79
	5	23	30,26	29	38,16
	6	2	2,63	31	40,79
	<i>Não Responderam</i>	3	3,95	2	2,63
	Total de Respostas	76		76	

Quadro 8.14 – Percepção dos Não Docentes acerca da segurança do sistema

D12) Classifique a segurança do Sistema Informático. (6 para muito seguro e 1 para pouco seguro)					
D14) Classifique em que medida considera que a segurança do Sistema Informático é ou pode ser importante para as suas actividades laborais/lectivas e de investigação. (6 para muito importante e 1 para pouco importante)					
	Técnicos	D22)		D24)	
		nº	%	nº	%
	1	0	0,00	0	0,00
	2	0	0,00	0	0,00
	3	2	14,29	3	21,43
	4	5	35,71	8	57,14
	5	6	42,86	2	14,29
	6	1	7,14	0	0,00
	<i>Não Responderam</i>	0	0,00	1	7,14
	Total de Respostas	14		14	

Quadro 8.15 – Percepção dos Técnicos acerca da segurança do sistema

Em termos de classificação da segurança a maioria dos inquiridos atribui uma classificação maioritária nos níveis 4 e 5, variando no entanto os respectivos valores percentuais, que nos Docentes são de 48,51% no nível 4 e de 22,39 no nível 5, enquanto que os Não Docentes consideram 30,26% em qualquer deles, já os Técnicos atribuem 48,51% ao nível 4 e 22,39% ao nível 5.

Relativamente à importância da segurança para as actividades desenvolvidas por qualquer dos grupos de inquiridos, verifica-se que os Docentes e os Não Docentes consideram maioritariamente os níveis 5 (33,58% e 38,16% respectivamente) e 6 (39,55% e 40,79% respectivamente), enquanto que os Técnicos consideram como sendo mais relevantes os níveis 3 (21,43%) e 4 (57,14%).

Os quadros 8.16, 8.17 e 8.18 apresentam as respostas obtidas relativamente à classificação, em termos de importância, de diversos aspectos relacionados com a segurança do Sistema Informático, agrupando as respostas em função do tipo de inquirido(a): Docentes, Não Docentes e Técnicos.

D13) Classifique, relativamente à segurança do Sistema Informático (*6 para muito importante e 1 para pouco importante*), os seguintes aspectos:

	1	2	3	4	5	6	NR
(a) Utilizadores	1,49	1,49	10,45	13,43	33,58	26,87	12,69
(b) Técnicos de informática	2,24	0,75	6,72	11,94	27,61	35,07	15,67
(c) Leis/Políticas/Regulamentos/Procedimentos	2,99	1,49	12,69	20,90	30,60	12,69	18,66
(d) Computadores Pessoais (<i>Hardware</i>)	4,48	2,24	11,94	26,12	24,63	11,94	18,66
(e) Periféricos (Impressoras, Scanners, etc.)	8,96	8,21	13,43	19,40	23,13	8,21	18,66
(f) Servidores (<i>Hardware</i>)	1,49	0,75	5,22	19,40	23,13	27,61	22,39
(g) <i>Software</i> aplicacional	1,49	2,99	9,70	19,40	27,61	17,91	20,90
(h) Sistemas Operativos	1,49	2,24	7,46	19,40	25,37	21,64	22,39
(i) Internet	1,49	1,49	7,46	12,69	29,85	29,10	17,91
(j) Correio electrónico	1,49	0,75	6,72	14,93	30,60	29,10	16,42
(k) Rede informática	2,24	0,00	7,46	14,18	26,87	29,85	19,40
(l) Sistema de comunicações (telefones, telefaxes, etc.)	8,21	5,97	8,96	20,90	23,13	9,70	23,13

Quadro 8.16 – Percepção dos Docentes acerca de aspectos relevantes para a segurança da informação

Os aspectos referenciados como mais importantes são os ‘Técnicos de Informática’, os ‘Utilizadores’ e o ‘Correio Electrónico’, enquanto que os menos importantes correspondem aos ‘Periféricos’ e ao ‘Sistema de comunicações’.

Deve todavia referenciar-se a grande diversidade das respostas nos diversos níveis de classificação, e ainda que existe um número apreciável de Docentes que não classificaram alguns dos aspectos.

D13) Classifique, relativamente à segurança do Sistema Informático (*6 para muito importante e 1 para pouco importante*), os seguintes aspectos:

	1	2	3	4	5	6	NR
(a) Utilizadores	0,00	3,95	17,11	23,68	26,32	15,79	13,16
(b) Técnicos de informática	1,32	0,00	7,89	15,79	31,58	30,26	13,16
(c) Leis/Políticas/Regulamentos/Procedimentos	3,95	9,21	9,21	17,11	27,63	17,11	15,79
(d) Computadores Pessoais (<i>Hardware</i>)	1,32	1,32	21,05	23,68	22,37	14,47	15,79
(e) Periféricos (Impressoras, Scanners, etc.)	1,32	9,21	19,74	28,95	21,05	7,89	11,84
(f) Servidores (<i>Hardware</i>)	0,00	3,95	11,84	19,74	22,37	27,63	14,47
(g) <i>Software</i> aplicacional	0,00	3,95	17,11	23,68	26,32	11,84	17,11
(h) Sistemas Operativos	0,00	3,95	13,16	25,00	27,63	13,16	17,11
(i) Internet	0,00	1,32	9,21	21,05	34,21	21,05	13,16
(j) Correio electrónico	0,00	3,95	7,89	18,42	27,63	31,58	10,53
(k) Rede informática	0,00	5,26	9,21	13,16	21,05	38,16	13,16
(l) Sistema de comunicações (telefones, telefaxes, etc.)	3,95	9,21	14,47	30,26	21,05	9,21	11,84

Quadro 8.17 – Percepção dos Não Docentes acerca de aspectos relevantes para a segurança da informação

Os aspectos referenciados como mais importantes são os ‘Técnicos de Informática’, a ‘Rede Informática’ e o ‘Correio Electrónico’, enquanto que os menos importantes correspondem às ‘Leis/Políticas/Regulamentos/Procedimentos’ e ao ‘Sistema de comunicações’.

Deve todavia referenciar-se a grande diversidade das respostas nos diversos níveis de classificação, e ainda que existe um número apreciável de Não Docentes que não classificaram alguns aspectos.

D23) Classifique, relativamente à segurança do Sistema Informático (6 para muito importante e 1 para pouco importante), os seguintes aspectos:							
	1	2	3	4	5	6	NR
(a) Pessoas	0,00	0,00	14,29	21,43	21,43	35,71	7,14
(b) Leis/Políticas/Regulamentos/Procedimentos	0,00	7,14	14,29	7,14	28,57	35,71	7,14
(c) Computadores Pessoais (Hardware)	0,00	7,14	14,29	7,14	28,57	35,71	7,14
(d) Periféricos (Impressoras, Scanners, etc.)	0,00	7,14	21,43	35,71	21,43	7,14	7,14
(e) Servidores (Hardware)	0,00	21,43	35,71	28,57	7,14	0,00	7,14
(f) Software aplicacional	0,00	7,14	7,14	21,43	28,57	28,57	7,14
(g) Sistemas Operativos	0,00	0,00	21,43	42,86	21,43	7,14	7,14
(h) Internet	0,00	7,14	7,14	21,43	50,00	7,14	7,14
(i) Correio electrónico	0,00	0,00	14,29	14,29	28,57	35,71	7,14
(j) Rede informática	0,00	0,00	7,14	28,57	28,57	28,57	7,14
(k) Sistema de comunicações (telefones, telefaxes, etc.)	0,00	0,00	7,14	14,29	42,86	28,57	7,14

Quadro 8.18 – Percepção dos Técnicos acerca de aspectos relevantes para a segurança da informação

Os aspectos referenciados como mais importantes são o ‘Sistema de comunicações’, as ‘Leis/Políticas/Regulamentos/Procedimentos’, os ‘Computadores Pessoais’ e o ‘Correio Electrónico’, enquanto que os menos importantes correspondem aos ‘Servidores’ e aos ‘Periféricos’.

Os quadros 8.19, 8.20 e 8.21 apresentam as respostas obtidas relativamente à classificação, em termos de importância, de diversos tipos de ameaças à segurança do Sistema Informático, agrupando as respostas em função do tipo de inquirido(a): Docentes, Não Docentes e Técnicos.

D17) Classifique, de acordo com o impacto na segurança do Sistema Informático (6 para muito importante e 1 para pouco importante), os seguintes tipos de ameaças.							
	1	2	3	4	5	6	NR
(a) Acidentes naturais (incêndios, terremotos, inundações, etc.)	3,73	4,48	12,69	17,91	15,67	23,13	22,39
(b) <i>Hackers</i> (acessos não autorizados a partir do exterior das organizações)	1,49	1,49	4,48	11,19	19,40	40,30	21,64
(c) Acessos indevidos (não autorizados) a partir do interior das organizações	1,49	1,49	4,48	12,69	23,88	34,33	21,64
(d) <i>Virus/Trojan Horses/Worms/etc.</i>	0,00	2,24	2,99	10,45	23,13	38,81	22,39
(e) Roubo de informação	1,49	1,49	5,22	15,67	20,15	34,33	21,64
(f) Destruição de informação	1,49	0,00	5,97	11,19	21,64	37,31	22,39
(g) Utilização incorrecta do sistema	0,75	1,49	16,42	18,66	22,39	16,42	23,88
(h) Definição por defeito das <i>passwords</i> iniciais (por ex. <i>Password</i> igual ao <i>UserID</i>)	2,99	4,48	13,43	17,16	23,13	15,67	23,13
(i) Intercepção de mensagens de correio electrónico e respectivos anexos	1,49	0,75	8,96	9,70	29,85	26,12	23,13
(j) Falhas no fornecimento de energia eléctrica ao sistema	1,49	2,99	12,69	15,67	22,39	22,39	22,39
(k) Configuração incorrecta da <i>firewall</i>	0,75	3,73	5,97	14,93	27,61	23,13	23,88
(l) Falhas de funcionamento do <i>software</i> do sistema	0,00	2,24	8,96	11,94	29,85	24,63	22,39
(m) Falhas de funcionamento do <i>hardware</i> do sistema	0,75	2,24	9,70	13,43	27,61	23,88	22,39

Quadro 8.19 – Percepção dos Docentes acerca dos impactos das ameaças na segurança da informação

As ameaças cujos impactos são referenciados como mais importantes são os ‘*Virus/Trojan Horses/Worms/etc.*’, os ‘*Hackers*’, a ‘Destruição de informação’ e os ‘Acessos indevidos a partir do interior das organizações’, enquanto que as menos importantes correspondem aos ‘Acidentes naturais’ e a ‘Definição por defeito das *passwords* iniciais’.

Deve ainda referenciar-se a grande diversidade das respostas nos diversos níveis de classificação, e a existência de um número apreciável de Docentes que não classificaram algumas das ameaças.

D17) Classifique, de acordo com o impacto na segurança do Sistema Informático (6 para muito importante e 1 para pouco importante), os seguintes tipos de ameaças.

	1	2	3	4	5	6	NR
(a) Acidentes naturais (incêndios, terremotos, inundações, etc.)	5,26	3,95	13,16	14,47	13,16	32,89	17,11
(b) <i>Hackers</i> (acessos não autorizados a partir do exterior das organizações)	1,32	0,00	5,26	9,21	19,74	50,00	14,47
(c) Acessos indevidos (não autorizados) a partir do interior das organizações	0,00	1,32	5,26	13,16	30,26	32,89	14,29
(d) <i>Virus/Trojan Horses/Worms/etc.</i>	0,00	1,32	6,58	3,95	22,37	50,00	15,79
(e) Roubo de informação	0,00	1,32	6,58	11,84	22,37	42,11	15,79
(f) Destruição de informação	0,00	1,32	5,26	10,53	25,00	42,11	15,79
(g) Utilização incorrecta do sistema	0,00	2,63	7,89	32,89	27,63	14,47	14,47
(h) Definição por defeito das <i>passwords</i> iniciais (por ex. <i>Password</i> igual ao <i>UserID</i>)	2,63	3,95	11,84	28,95	19,74	17,11	15,79
(i) Intercepção de mensagens de correio electrónico e respectivos anexos	0,00	2,63	10,53	22,37	30,26	18,42	15,79
(j) Falhas no fornecimento de energia eléctrica ao sistema	0,00	5,26	9,21	26,32	26,32	15,79	17,11
(k) Configuração incorrecta da <i>firewall</i>	0,00	7,89	6,58	23,68	21,05	22,37	18,42
(l) Falhas de funcionamento do <i>software</i> do sistema	0,00	1,32	10,53	31,58	21,05	19,74	15,79
(m) Falhas de funcionamento do <i>hardware</i> do sistema	0,00	1,32	14,29	14,29	23,68	19,74	15,79

Quadro 8.20 – Percepção dos Não Docentes acerca dos impactos das ameaças na segurança da informação

As ameaças cujos impactos são referenciados como mais importantes são os ‘*Virus/Trojan Horses/Worms/etc.*’, os ‘*Hackers*’, a ‘Destruição de informação’, o ‘Roubo de informação’ e os ‘Acessos indevidos a partir do interior das organizações’, enquanto que as menos importantes correspondem aos ‘Acidentes naturais’ e a ‘Definição por defeito das *passwords* iniciais’.

Deve ainda referenciar-se a grande diversidade das respostas nos diversos níveis de classificação, e a existência de um número apreciável de Não Docentes que não classificaram algumas das ameaças.

D27) Classifique, de acordo com o impacto na segurança do Sistema Informático (6 para muito importante e 1 para pouco importante), os seguintes tipos de ameaças.							
		2	3	4	5	6	NR
(a) Acidentes naturais (incêndios, terremotos, inundações, etc.)	0,00	0,00	7,14	14,29	28,57	42,86	7,14
(b) <i>Hackers</i> (acessos não autorizados a partir do exterior das organizações)	0,00	0,00	7,14	21,43	35,71	28,57	7,14
(c) Acessos indevidos (não autorizados) a partir do interior das organizações	0,00	0,00	7,14	21,43	21,43	35,71	14,29
(d) <i>Virus/Trojan Horses/Worms/etc.</i>	0,00	0,00	7,14	28,57	42,86	14,29	7,14
(e) Roubo de informação	0,00	0,00	21,43	14,29	35,71	21,43	7,14
(f) Destruição de informação	0,00	0,00	14,29	28,57	21,43	28,57	7,14
(g) Utilização incorrecta do sistema	0,00	0,00	42,86	28,57	14,29	7,14	7,14
(h) Definição por defeito das <i>passwords</i> iniciais (por ex. <i>Password</i> igual ao <i>UserID</i>)	0,00	7,14	21,43	21,43	21,43	21,43	7,14
(i) Intercepção de mensagens de correio electrónico e respectivos anexos	0,00	0,00	28,57	28,57	28,57	7,14	7,14
(j) Falhas no fornecimento de energia eléctrica ao sistema	7,14	0,00	21,43	28,57	14,29	21,43	7,14
(k) Configuração incorrecta da <i>firewall</i>	0,00	0,00	21,43	21,43	21,43	28,57	7,14
(l) Falhas de funcionamento do <i>software</i> do sistema	0,00	7,14	14,29	21,43	35,71	14,29	7,14
(m) Falhas de funcionamento do <i>hardware</i> do sistema	0,00	7,14	14,29	14,29	42,86	14,29	7,14

Quadro 8.21 – Percepção dos Técnicos acerca dos impactos das ameaças na segurança da informação

As ameaças cujos impactos são referenciados como mais importantes são os ‘Acidentes naturais’, os ‘*Hackers*’, os ‘*Virus/Trojan Horses/Worms/etc.*’, os ‘Acessos indevidos a partir do interior das organizações’, a ‘Destruição de informação’, o ‘Roubo de informação’ e as ‘Falhas de funcionamento do *hardware* do sistema’, enquanto que a menos importante corresponde às ‘Falhas no fornecimento de energia eléctrica ao sistema’.

Contrariamente aos outros grupos, verifica-se aqui uma maior convergência nas opções e que a grande maioria procedeu à classificação de todas as ameaças.

Tópicos a considerar relativamente à percepção da segurança do Sistema Informático:

- ⇒ Realizar acções de sensibilização para a problemática da segurança da informação.
- ⇒ Realizar acções de formação sobre segurança da informação.

⇒ Divulgar documento das políticas de segurança e procedimentos relacionados com a utilização dos activos do sistema.

8.5.5. Resultados do Grupo E – Usabilidade do Sistema Informático

A apreciação dos resultados deste grupo será efectuada tendo em atenção a relação directa entre as questões colocadas e não apenas e só a sequência pela qual as mesmas foram apresentadas no questionário.

Neste contexto serão abordados os seguintes temas:

- Formação na utilização do sistema;
- Facilidade de utilização e aprendizagem do sistema.

8.5.5.1. Formação na Utilização do Sistema

Esta secção agrega as questões relacionadas com a percepção das Pessoas acerca da formação na utilização do Sistema Informático, considerando a sua participação em acções formativas e a existência de documentos de apoio a essa utilização.

Questões	Doc	NDoc	Téc
Recebeu formação na utilização do Sistema Informático?	E1)	E1)	E1)
Com que frequência recebe formação necessária à utilização do Sistema Informático?	E2)	E2)	-
Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)	E3)	E3)	E2)
São proporcionadas acções de formação sobre a utilização do Sistema Informático aos utilizadores finais?	-	-	E3)
Com que frequência são realizadas essas acções?	-	-	E4)
São elaborados alguns documentos acerca da utilização do Sistema Informático para apoio aos utilizadores finais?	-	-	E5)
Existe algum(uns) documento(s) acerca da utilização do Sistema Informático?	E4)	E4)	-
Como tomou conhecimento desse(s) documento(s)?	E5)	E5)	-
Classifique a utilidade desse(s) documento(s). (6 para muito útil e 1 para pouco útil)	E6)	E6)	-

Tabela 8.34 – Questões acerca da formação na utilização do sistema

- *Recebeu formação na utilização do Sistema Informático?*
- *Com que frequência recebe formação necessária à utilização do Sistema Informático?*

No respeitante à participação em acções de formação acerca da utilização do sistema, a maioria dos Docentes (73,88%) refere não ter participado em qualquer

acção, enquanto que os Não Docentes (61,84%) e os Técnicos (64,29%) mencionam a participação nessas acções, embora nem todos o tenham feito.

Relativamente à frequência das acções, os Docentes e os Não Docentes referem que estas se realizam sempre que existem mudanças no sistema, com valores de 54,29% e de 69,39% respectivamente. Esta questão foi colocada em termos distintos aos Técnicos, avaliando-as de acordo com as respostas então proporcionadas no grupo C.

E3) Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)							
Opções	[Técnicos (C2)]	Docentes		Não Docentes		Técnicos	
		nº	%	nº	%	nº	%
1		2	5,71	0	0,00	0	0,00
2		1	2,86	0	0,00	0	0,00
3		3	8,57	6	12,24	1	11,11
4		12	34,29	2	4,08	2	22,22
5		11	31,43	15	30,61	3	33,33
6		4	11,43	22	44,90	3	33,33
Não Responderam		2	5,71	4	8,16	0	0,00
Total de Respostas		35		49		9	

Quadro 8.22 – Formação na utilização do Sistema Informático

Já acerca da classificação atribuída à relevância dessa formação, os Docentes mencionam maioritariamente os níveis 4 (34,29%) e 5 (31,43%), os Não Docentes e os Técnicos referem por seu lado maioritariamente os níveis 5 (30,61% e 33,33% respectivamente) e 6 (44,90% e 33,33% respectivamente).

- São proporcionadas acções de formação sobre a utilização do Sistema Informático aos utilizadores finais?
- Com que frequência são realizadas essas acções?
- São elaborados alguns documentos acerca da utilização do Sistema Informático para apoio aos utilizadores finais?

Face à sua especificidade, as questões desta tabela são apenas colocadas aos Técnicos. Relativamente às acções de formação para os utilizadores finais, a maioria dos Técnicos (57,14%) refere que não são proporcionadas acções de formação, e que, quando ocorrem, estas se realizam ‘Sempre que existem mudanças no sistema’.

Acerca dos documentos sobre utilização do sistema, a maioria dos Técnicos (78,57%) refere que são elaborados documentos de apoio para os utilizadores finais.

- *Existe algum(uns) documento(s) acerca da utilização do Sistema Informático?*
- *Como tomou conhecimento desse(s) documento(s)?*

Relativamente aos documentos sobre utilização do sistema, a maioria dos Docentes e dos Não Docentes refere desconhecer a sua existência ou mesmo que não existem, notando-se que apenas 32,09% dos Docentes e 25,00% dos Não Docentes confirma que existem tais documentos.

De entre estes, os Docentes referem na sua maioria que tomaram conhecimento dos documentos porque lhes foram entregues na Escola ou devido a informação dos serviços de informática, enquanto que os Não Docentes mencionam que lhes foram entregues no Serviço ou devido a informações de colegas.

E6) Classifique a utilidade desse(s) documento(s). (6 para muito útil e 1 para pouco útil)					
Opções	Docentes		Não Docentes		
	nº	%	nº	%	
1	1	2,17	0	0,00	
2	2	4,35	1	5,00	
3	3	6,52	1	5,00	
4	10	21,74	3	15,00	
5	18	39,13	10	50,00	
6	9	19,57	4	20,00	
<i>Não Responderam</i>	3	6,52	1	5,00	
Total de Respostas	46		20		

Quadro 8.23 – Documentos acerca da utilização do Sistema Informático

No respeitante à classificação da sua utilidade, a maioria dos Docentes classifica-a nos níveis 4 (21,74%) e 5 (39,13%), enquanto que a maioria dos Não Docentes a classificam nos níveis 5 (50,00%) e 6 (20,00%).

Tópicos a considerar relativamente à formação na utilização do Sistema:

- ⇒ Divulgar o documento de suporte às políticas de segurança e outros documentos relacionados.
- ⇒ Definir e implementar plano de formação para utilização do sistema.

8.5.5.2. Facilidade de Utilização e Aprendizagem do Sistema

Esta secção agrega as questões relacionadas com a percepção das Pessoas acerca da facilidade de utilização e de aprendizagem do Sistema Informático, considerando ainda a sua importância para as actividades que desenvolvem.

Os quadros 8.24, 8.25 e 8.26 apresentam as respostas obtidas relativamente à classificação, em termos de importância, de diversos aspectos relacionados com a facilidade de utilização e aprendizagem do Sistema Informático, agrupando as respostas em função do tipo de inquirido(a): Docentes, Não Docentes e Técnicos.

De forma similar são também apresentadas as respostas obtidas por cada grupo de inquiridos relativamente à importância da usabilidade para as actividades que desenvolvem.

Os quadros 8.27, 8.28 e 8.29 apresentam as respostas obtidas relativamente à classificação, em termos de importância, de diversos aspectos relativamente à relevância da usabilidade, agrupando as respostas em função do tipo de inquirido(a): Docentes, Não Docentes e Técnicos.

E7) Classifique a facilidade de utilização do Sistema Informático do Serviço/Escola. (6 para fácil de utilizar e 1 para difícil de utilizar)							
E8) Classifique a facilidade de aprendizagem do Sistema Informático do Serviço/Escola. (6 para fácil de aprender e 1 para difícil de aprender)							
E10) Classifique em que medida considera que a usabilidade do Sistema Informático do Serviço/Escola é ou pode ser importante para as suas actividades lectivas e de investigação. (6 para muito importante e 1 para pouco importante)							
Docentes	Opções	E7)		E8)		E10)	
		nº	%	nº	%	nº	%
	1	5	3,73	6	4,48	0	0,00
	2	2	1,49	4	2,99	1	0,75
	3	12	8,96	8	5,97	1	0,75
	4	24	17,91	30	22,39	20	14,93
	5	49	36,57	44	32,84	53	39,55
	6	26	19,40	22	16,42	52	38,81
	<i>Não Responderam</i>	16	11,94	20	14,93	7	5,22
Total de Respostas		134		134		134	

Quadro 8.24 – Percepção dos Docentes acerca da utilização e aprendizagem do Sistema Informático

E7) Classifique a facilidade de utilização do Sistema Informático do Serviço/Escola. (6 para fácil de utilizar e 1 para difícil de utilizar) E8) Classifique a facilidade de aprendizagem do Sistema Informático do Serviço/Escola. (6 para fácil de aprender e 1 para difícil de aprender) E10) Classifique em que medida considera que a usabilidade do Sistema Informático do Serviço/Escola é ou pode ser importante para as suas actividades lectivas e de investigação. (6 para muito importante e 1 para pouco importante)							
Não Docentes		E7)		E8)		E10)	
Opções		nº	%	nº	%	nº	%
1		0	0,00	0	0,00	1	1,32
2		0	0,00	0	0,00	0	0,00
3		9	11,84	9	11,84	2	2,63
4		21	27,63	26	34,21	10	13,16
5		33	43,42	31	40,79	23	30,26
6		13	17,11	10	13,16	39	51,32
Não Responderam		0	0,00	0	0,00	1	1,32
Total de Respostas		76		76		76	

Quadro 8.25 – Percepção dos Não Docentes acerca da utilização e aprendizagem do Sistema Informático

E7) Classifique a facilidade de utilização do Sistema Informático do Serviço/Escola. (6 para fácil de utilizar e 1 para difícil de utilizar) E8) Classifique a facilidade de aprendizagem do Sistema Informático do Serviço/Escola. (6 para fácil de aprender e 1 para difícil de aprender) E10) Classifique em que medida considera que a usabilidade do Sistema Informático do Serviço/Escola é ou pode ser importante para as suas actividades lectivas e de investigação. (6 para muito importante e 1 para pouco importante)							
Técnicos		E6)		E7)		E9)	
Opções		nº	%	nº	%	nº	%
1		0	0,00	0	0,00	0	0,00
2		0	0,00	0	0,00	0	0,00
3		1	7,14	1	7,14	1	7,14
4		2	14,29	2	14,29	1	7,14
5		6	42,86	9	64,29	5	35,71
6		5	35,71	2	14,29	7	50,00
Não Responderam		0	0,00	0	0,00	0	0,00
Total de Respostas		14		14		14	

Quadro 8.26 – Percepção dos Técnicos acerca da utilização e aprendizagem do Sistema Informático

Relativamente aos Docentes, este classificam maioritariamente a facilidade de utilização nos níveis 5 (36,57%) e 6 (19,40%), a facilidade de aprendizagem nos níveis 4 (22,39%) e 5 (33,84%), e a usabilidade nos níveis 5 (39,55%) e 6 (38,81%).

No que diz respeito aos Docentes, este classificam maioritariamente a facilidade de utilização e de aprendizagem nos níveis 4 (27,63% e 34,21%, respectivamente) e 5

(43,42% e 40,79%, respectivamente), e a usabilidade nos níveis 5 (30,26%) e 6 (51,32%).

Já no respeitante aos Técnicos, estes classificam maioritariamente a facilidade de utilização e de aprendizagem, e a usabilidade nos níveis 5 (42,86%, 64,29% e 35,71%, respectivamente) e 6 (35,71%, 14,29% e 50,00%, respectivamente).

E9) Classifique, relativamente à usabilidade do Sistema Informático do Serviço/Escola (6 para muito importante e 1 para pouco importante), a relevância dos seguintes aspectos:							
	1	2	3	4	5	6	NR
(a) Facilidade de acesso	0,00	0,00	5,97	10,45	35,07	41,04	7,46
(b) Disponibilidade	0,00	0,00	2,99	13,43	29,10	47,01	7,46
(c) Adequação às necessidades	0,00	1,49	5,97	17,16	28,36	38,06	8,96
(d) Apoio técnico à utilização	0,75	5,22	12,69	17,16	29,85	27,61	6,72
(e) Interface com o sistema	0,75	3,73	10,45	20,90	34,33	17,16	12,69
(f) Regras de utilização	0,00	0,00	16,42	27,61	31,34	15,67	8,96
(g) Conhecimento prévio do sistema	3,73	5,97	14,93	27,61	27,61	11,19	8,96
(h) Participação no desenvolvimento/implementação do sistema	8,21	11,94	20,15	21,64	11,94	13,43	12,69

Quadro 8.27 – Percepção dos Docentes acerca de aspectos relevantes para a usabilidade

Os aspectos referenciados como mais importantes são a ‘Disponibilidade’, a ‘Facilidade de acesso’ e a ‘Adequação às necessidades’, enquanto que os menos importantes correspondem à ‘Participação no desenvolvimento/implementação do sistema’ e ao ‘Conhecimento prévio do sistema’. Deve ainda referenciar-se a grande diversidade das respostas nos diversos níveis de classificação.

E9) Classifique, relativamente à usabilidade do Sistema Informático do Serviço/Escola (6 para muito importante e 1 para pouco importante), a relevância dos seguintes aspectos:							
	1	2	3	4	5	6	NR
(a) Facilidade de acesso	0,00	1,32	2,63	17,11	44,74	30,26	3,95
(b) Disponibilidade	0,00	0,00	5,26	19,74	43,42	27,63	3,95
(c) Adequação às necessidades	0,00	2,63	3,95	19,74	36,84	28,95	7,89
(d) Apoio técnico à utilização	0,00	1,32	2,63	28,95	28,95	28,95	9,21
(e) Interface com o sistema	1,32	2,63	7,89	25,00	34,21	15,79	13,16
(f) Regras de utilização	0,00	1,32	7,89	25,00	36,84	21,05	7,89
(g) Conhecimento prévio do sistema	1,32	5,26	14,47	28,95	19,74	21,05	9,21
(h) Participação no desenvolvimento/implementação do sistema	3,95	5,26	7,89	22,37	31,58	15,79	13,16

Quadro 8.28 – Percepção dos Não Docentes acerca de aspectos relevantes para a usabilidade

Os aspectos referenciados como mais importantes são a ‘Facilidade de acesso’, a ‘Disponibilidade’ e a ‘Adequação às necessidades’, enquanto que os menos importantes correspondem à ‘Participação no desenvolvimento/implementação do

sistema' e ao 'Conhecimento prévio do sistema'. Deve ainda referenciar-se a grande diversidade das respostas nos diversos níveis de classificação

E8) Classifique, relativamente à usabilidade do Sistema Informático do Serviço/Escola (6 para muito importante e 1 para pouco importante), a relevância dos seguintes aspectos:							
	1	2	3	4	5	6	NR
(a) Facilidade de acesso	0,00	0,00	7,14	14,29	50,00	28,57	0,00
(b) Disponibilidade	0,00	0,00	7,14	21,43	28,57	42,86	0,00
(c) Adequação às necessidades	0,00	0,00	7,14	21,43	42,86	28,57	0,00
(d) Apoio técnico à utilização	0,00	0,00	14,29	50,00	21,43	14,29	0,00
(e) Interface com o sistema	0,00	0,00	7,14	42,86	42,86	7,14	0,00
(f) Regras de utilização	0,00	0,00	14,29	35,71	28,57	21,43	0,00
(g) Conhecimento prévio do sistema	0,00	21,43	35,71	28,57	14,29	0,00	0,00
(h) Participação no desenvolvimento/implementação do sistema	0,00	21,43	21,43	28,57	28,57	0,00	0,00

Quadro 8.29 – Percepção dos Técnicos acerca de aspectos relevantes para a usabilidade

Os aspectos referenciados como mais importantes são a 'Facilidade de acesso', a 'Disponibilidade' e a 'Adequação às necessidades', enquanto que os menos importantes correspondem ao 'Conhecimento prévio do sistema' e à 'Participação no desenvolvimento/implementação do sistema'.

Tópicos a considerar relativamente à facilidade de utilização e aprendizagem do sistema:

⇒ Proporcionar um maior envolvimento das Pessoas nos processos de desenvolvimento e implementação de sistemas.

8.5.6. Comparação com os Resultados do Grupo de Teste

A comparação dos resultados obtidos com o grupo de teste são genericamente coincidentes com os que foram obtidos pelo conjunto dos três modelos de questionário final, não se verificando divergências dignas de registo por parte dos alunos, a não ser nas seguintes questões:

- Apresentam uma maior utilização do computador pessoal na sua residência;
- Partilham o computador pessoal com um maior número de Pessoas;
- Utilizam maioritariamente a memorização para guardar a *password*;
- Assumem uma maior utilização de *firewall* e de antivírus;
- Optam preferencialmente pelo *backup* dos ficheiros que consideram importantes, utilizando CD/DVD para essa actividade;

- Referem uma utilização quase uniforme de todas as funcionalidades do sistema;
- Apresentam uma utilização menos frequente do sistema da Escola e habitualmente não possuem endereço de correio electrónico associado a esse sistema;
- São mais assertivos nas actividades proibidas nos locais onde acedem ao Sistema Informático.

8.6. Conclusões

A metodologia identificada para suportar o trabalho, baseado numa abordagem qualitativa, foi o Estudo de Casos, considerando como métodos ou técnicas a utilizar o estudo de documentos (normas técnicas, legislação, relatórios e outros documentos organizacionais) e a realização de um questionário.

A selecção de casos de estudo para suportar o trabalho foi condicionada desde o seu início devido essencialmente à escassez da informação disponível e ao receio de divulgação de informação relativa à segurança da informação pela incerteza de eventuais impactos negativos na sua imagem e credibilidade. Perante este contexto decidiu-se que o trabalho seria suportado pelo estudo de um único caso, tentando-se que o caso a escolher fosse suficientemente abrangente para possibilitar as respostas necessárias a este trabalho.

O âmbito do estudo compreende os aspectos associados à segurança da informação, à utilização dos SI e das TIC e ao papel desempenhado pelas Pessoas no IPS e nas suas Escolas e Serviços, procurando abranger Pessoas com actividades distintas, Docentes e Não Docentes, surgindo posteriormente a separação de um novo grupo, com características muito específicas, os Técnicos de Informática.

A elaboração das questões a inserir nas versões iniciais dos questionários teve em consideração a norma ISO/IEC 17799 [ISO 2005a], que estabelece um conjunto de boas práticas no âmbito da segurança da informação, que faz parte do normativo estudado, complementarmente foi também utilizada a norma ISO/IEC 27001 [ISO 2005b], necessária para obtenção da certificação do SGSI, utilizando por isso os mesmos controlos especificados na norma ISO/IEC 17799.

As versões finais dos questionários foram construídas com base nos referenciais do MIDImOS, utilizando-se os controlos subjacentes a cada referencial em função da adequação ao problema a questionar.

O desenvolvimento dos questionários, iniciais e finais, foi suportado pelo desenho de fluxogramas, os quais foram sucessivamente alterados de acordo com os testes a que os questionários foram submetidos e à realidade da instituição alvo do estudo, procurando que as questões colocadas possibilitassem a resposta às questões de partida.

A análise dos resultados obtidos com os questionários permite constatar a existência de uma atenção especial para a problemática da segurança da informação, que, conjugada com uma abertura para maior e melhor utilização dos SI e das TIC, potenciará, através da realização de acções de formação e de um maior envolvimento das Pessoas neste tipo de actividades, um melhor desempenho organizacional e um incremento da segurança da informação institucional.

Perante os resultados obtidos com os questionários, mesmo considerando que a maioria do universo em análise não procedeu à devolução do respectivo questionário, considera-se pertinente a amostra constante deste trabalho (44,15%) do total.

Conclui-se ainda da necessidade de proceder à divulgação do documento de suporte das políticas de segurança por todos os envolvidos na utilização do Sistema Informático, independentemente do respectivo grau de utilização.

Relativamente ainda à documentação, considerando também a necessidade do estabelecimento de procedimentos específicos para as situações identificadas, importa que estes sejam objecto de idêntica divulgação. Neste sentido, a manutenção actualizada de toda a informação deve ser uma regra básica a considerar.

A análise das questões de partida possibilitou a identificação do conjunto de itens considerados pertinentes, que tiveram em conta a percepção das Pessoas acerca da segurança da informação, a classificação da segurança da informação numa perspectiva pessoal, e ainda a percepção das Pessoas acerca da utilização dos SI e das TIC.

Procedeu-se então à identificação dos itens relevantes especificados pelas Pessoas, utilizando-os para caracterizar os impactos nas suas actividades organizacionais, a

quando da implementação de SGSI, procurando assim responder à principal formulação do problema que conduziu o desenvolvimento deste trabalho.

Os itens identificados como relevantes constituirão uma componente primordial para suportar a implementação prática do SGSI no IPS, recorrendo aos referenciais definidos no MIDImOS para apoiar as actividades a desempenhar pelas Pessoas neste processo.

Referências bibliográficas

- Andrade, J. e Ferreira, L., *25 Anos a Construir Futuro*, Instituto Politécnico de Setúbal, Abril de 2004.
- ISO, *BS ISO/IEC 17799 (BS 7799-1:2005) – Information Technology - Code of practice for information security management*, British Standard Institution, 2005.
- ISO, *BS ISO/IEC 27001 (BS 7799-2:2005) – Information Technology - Security Techniques - Information Security Management Systems - Requirements*, British Standard Institution, 2005.
- Macedo, P., Zacarias, M.S. e Tribolet, J., “Técnicas e Métodos de Investigação em Engenharia Organizacional: Projecto de Investigação em Modelação de Processos de Produção”, Actas (formato digital) da 6ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade do Minho e pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança, Bragança, 26-28 de Outubro de 2005.
- Martins, M.E.G. e Cerveira, A.G., *Introdução às Probabilidades e à Estatística*, 1ª Edição-5ª Impressão, Universidade Aberta, Outubro de 2006.
- Yin, R. K., *Case Study Research: Design and Methods*, 2nd edition, Applied Social Research Methods Series. Thousand Oaks: SAGE Publications, 1994.

9

Validação do Modelo

A eficácia do Modelo definido e a sua adequação aos processos associados à segurança da informação dependem em grande medida da capacidade das Pessoas na sua utilização de acordo com as necessidades previamente identificadas.

Nesse sentido, torna-se crucial proceder à validação da sua aplicabilidade, exequibilidade e da correcção dos pressupostos e princípios que sustentaram a sua elaboração.

9.1. Princípios

O Modelo apresentado neste trabalho atende a duas componentes essenciais: as Pessoas nas suas diversas tipificações (utilizadores finais, técnicos, clientes, *stakeholders*, fornecedores) e a segurança da informação (pessoal e organizacional).

Estas duas componentes terão como base os seguintes aspectos:

- pertinência da informação;
- grau de criticidade atribuído;
- vulnerabilidades e ameaças (potenciais e identificadas);
- adequação dos SI e das TIC às necessidades das Pessoas e das organizações;
- competências e capacidades das Pessoas em utilizar adequadamente esses sistemas;
- envolvimento no processo de todos os interessados nas diversas actividades.

Salienta-se que o Modelo se suporta no normativo relacionado com os SGSI já referenciados neste trabalho, que proporcionam um enquadramento adequado a suportar a sua estrutura, permitindo assim a sua aplicação na generalidade das organizações, considerando a missão e estratégia definidas, assim como os objectivos determinados e os recursos disponibilizados para a realização das actividades necessárias.

Com as Pessoas a contituir um dos principais focos para suporte ao Modelo definido e com o diverso normativo considerado no trabalho, com os resultados obtidos através dos questionários, nomeadamente os tópicos considerados fundamentais, devem ser considerados como pertinentes os seguintes aspectos:

- ⇒ Sensibilização para a utilização dos SI e das TIC;
- ⇒ Sensibilização para a segurança da informação;
- ⇒ Participação dos utilizadores na identificação de necessidades;
- ⇒ Participação dos utilizadores na especificação dos requisitos;
- ⇒ Cumprimento das expectativas dos utilizadores;
- ⇒ Formação dos utilizadores;
- ⇒ Utilização dos sistemas de acordo com as necessidades pessoais e organizacionais;
- ⇒ Atender a propostas de melhorias.

9.2. Metodologia de Aplicação

Considerando as diversas etapas que suportaram o desenvolvimento do Modelo, entende-se que os princípios estabelecidos permitem que este possa servir como base para introdução dos SGSI na generalidade das organizações, considerando obviamente as especificidades apresentadas por cada uma delas.

A metodologia de aplicação do Modelo terá em consideração os seguintes aspectos:

- ⇒ Fase de desenvolvimento do SI;
- ⇒ Estado do SI (novo ou legado);
- ⇒ Nível de conhecimentos e competências das Pessoas;
- ⇒ Grau de envolvimento dos parceiros de negócio;
- ⇒ Normas implementadas na organização;
- ⇒ Implicações legais;
- ⇒ Cultura da organização.

Todavia, o sucesso desta metodologia e da aplicação do próprio Modelo dependerá sempre do envolvimento dos utilizadores, actuais e potenciais, assim como do apoio

inequívoco dos responsáveis organizacionais e dos recursos disponibilizados para a definição e implementação do SGSI.

Refira-se no entanto que a aplicação do Modelo não deve ser entendida como suporte único dos SGSI, papel esse a ser desempenhado pela utilização dos normativos apropriados, mas apenas como facilitador do processo, definindo um conjunto de directrizes que facilitem o envolvimento dos utilizadores em todas as etapas associadas à concepção, desenvolvimento e implementação do SGSI.

9.3. Contributos dos Questionários

O que se pretende aqui é proceder a uma análise global das respostas a cada um dos grupos de questões, procurando a obtenção de uma visão sumária da percepção das Pessoas às diversas questões colocadas.

Pretende-se ainda, de acordo com a identificação prévia do conjunto de tópicos derivados da agregação das questões interrelacionadas, realizar uma apreciação de cada um desses tópicos, no sentido de proceder à sua integração considerando a identificação dos aspectos relevantes para a validação do Modelo.

9.3.1. Contributos do Grupo A – Identificação/Caracterização do(a) Inquirido(a)

Em termos genéricos, verifica-se alguma uniformidade em termos do tempo de ligação dos inquiridos à instituição, reflectindo um conhecimento adequado dos sistemas implementados e das actividades a realizar com a sua utilização.

No que diz respeito à área de formação, constata-se que 40 dos inquiridos (17,39%) se enquadra nas áreas científicas de Informática e Sistemas de Informação.

Acerca da área de residência, a maioria dos inquiridos (123 de um total de 230) reside no concelho de Setúbal, com a maioria dos Docentes (61,31%) e dos Técnicos (57,14%) a indicarem que residem fora do concelho.

9.3.2. Contributos do Grupo B – Computador pessoal

Os contributos deste grupo foram agregados nos tópicos constantes da tabela seguinte e serão objecto de um desenvolvimento ao longo desta secção:

Temas	Tópicos
Existência e partilha de computador pessoal	– Utilização de computadores portáteis – Partilha da utilização do computador pessoal
Acesso à Internet com o computador pessoal	– Locais de acesso à Internet – Solução tecnológica adoptada – Frequência de utilização
Utilização de <i>password</i> no computador pessoal	– Reduzida utilização de <i>password</i>, associada à reduzida taxa de alterações efectuadas – Opções assumidas na escolha de novas <i>passwords</i>
Utilização de mecanismos de protecção	– Utilização de mecanismos complementares da <i>password</i>
Realização de cópias de segurança	– Opções assumidas na realização de <i>backups</i> – Escolha dos dispositivos de backup e respectivo armazenamento
Utilização do computador pessoal	– Tipo de utilização do computador pessoal – Software utilizado no computador pessoal
Percepção da segurança do computador pessoal	– Classificação atribuída aos níveis de segurança

Tabela 9.1 – Tópicos do grupo B do questionário

Relativamente ao computador pessoal constata-se que a maioria possui pelo menos um, utilizando-o para aceder à Internet, enviar e receber correio electrónico, realizando ainda uma diversidade de actividades comuns.

Os aspectos relacionados com utilização de *password* de acesso e de outros mecanismos de segurança, realização de *backups* e a frequência de utilização dos seus computadores já apresenta perspectivas diferentes entre os grupos de inquiridos.

Com os tópicos identificados através da agregação efectuada nas questões deste grupo, é pertinente uma análise genérica dos itens que os inquiridos consideraram relevantes nos diversos contextos apresentados.

Foram assim, de acordo com os aspectos identificados, desenvolvidos os tópicos anteriormente identificados:

(1) Existência e partilha de computador pessoal:

⇒ *Utilização de computadores portáteis.* Em termos globais, 135 inquiridos referem a posse de computadores pessoal, correspondente a 62,50% do total de inquiridos, o que pode, face à constatação de que 59,79% dos inquiridos refere a sua utilização também no Serviço/Escola, realçar desde logo a necessidade do

estabelecimento de procedimentos para regular a sua adequada utilização com o Sistema Informático do Serviço/Escola.

⇒ *Partilha da utilização do computador pessoal.* Em conjunto com o tópico anterior, reforçando as considerações estabelecidas, acresce o facto de 60,85% dos inquiridos referir que partilha a utilização do seu computador pessoal, contribuindo essa situação para a emergência de adoptar os procedimentos já referenciados.

(2) Acesso à Internet com o computador pessoal:

⇒ *Locais de acesso à Internet.* Constatando-se que 44,97% dos inquiridos utiliza o seu computador pessoal em espaços onde, em princípio, os mecanismos de segurança não existem ou poderão ser insuficientes e ao facto desse mesmo computador ser utilizado no Serviço/Escola, permite assumir a necessidade de ter em atenção essa situação, definindo, conjuntamente com o especificado para os tópicos anteriores, um conjunto de recomendações acerca das medidas a tomar, medidas essas tendentes a evitar intrusões e perdas desnecessárias da informação contida nesses computadores.

⇒ *Solução tecnológica adoptada.* Relativamente a este tópico, face à diversidade de soluções adoptadas, torna-se pertinente aconselhar a sua uniformização, considerando as condições de acesso ao Sistema Informático que são disponibilizadas nos diversos Serviços/Escolas.

⇒ *Frequência de utilização.* Com 86,24% (163) dos inquiridos refere um acesso diário ou quase diário à Internet com o seu computador pessoal, considera-se essencial, no mesmo âmbito referenciado no tópico anterior, encontrar uma solução que permita essa optimização, particularmente se forem tidas em conta as respostas obtidas na questão C36/38), onde 71,43% (160) dos inquiridos refere a disposição para aceder remotamente ao Sistema Informático do Serviço/Escola

(3) Utilização de *password* no computador pessoal:

⇒ *Reduzida utilização de password, associada à reduzida taxa de alterações efectuadas.* Considerando que 125 (57,87%) dos inquiridos refere a não utilização de *password* para acesso ao computador pessoal e que, uma parte dos

que a utilizam (40, ou seja 43,96%) efectua a sua partilha, torna-se pertinente a realização de acções de sensibilização para a problemática da segurança da informação. O facto de 40,66% dos inquiridos referir que nunca alterou a sua *password* contribui para reforçar a necessidade deste tipo de acção

⇒ *Opções assumidas na escolha de novas passwords*. De entre um total de 54 inquiridos que refere a actualização da sua *password*, existem 21 (38,89%) que utilizam opções consideradas de fácil descodificação, facto que contribui para realçar a necessidade de realização de acções de sensibilização para a referida problemática.

(4) Utilização de mecanismos de protecção:

⇒ *Utilização de mecanismos complementares da password*. A utilização de outros mecanismos de protecção surge com uma perspectiva distinta, constatando-se que de entre os 216 inquiridos que responderam a estas questões, 114 referem a utilização de *Firewall*, 178 a utilização de *Antivírus* e 83 utilizam aplicações de *AntiSpyware*, reflectindo assim um utilização bastante superior à que se realiza relativamente às *passwords*. Como complemento às actividades de segurança deve ser reforçada a pertinência de possuir um funcionamento integrados de todos estes mecanismos, tornando-se assim possível o alargamento da abrangência de um maior número de potenciais ameaças.

(5) Realização de cópias de segurança:

⇒ *Opções assumidas na realização de backups*. Constatando-se que a maioria dos inquiridos (61,57%) realiza *backups*, verifica-se que as periodicidades adoptadas são muito distintas e que as opções acerca da informação a salvaguardar também divergem, considera-se relevante, a exemplo do que foi anteriormente referenciado, estabelecer acções de sensibilização para este tipo de problemática.

⇒ *Escolha dos dispositivos de backup e respectivo armazenamento*. Situação similar à anterior surge quando se constata que 63,77% dos inquiridos que responderam afirmativamente à realização de *backups*, referir o seu armazenamento na mesma sala onde se encontra o computador, contrariando assim o especificado em diversos normativos aplicáveis.

(6) Utilização do computador pessoal:

⇒ *Tipo de utilização do computador pessoal.* A grande maioria dos inquiridos (84,26%) refere uma utilização diária ou quase diária do seu computador pessoal, constatando-se a sua utilização para a grande maioria das opções apresentadas, muitas das quais poderiam ser realizadas através da utilização do Sistema Informático do Serviço/Escola.

⇒ *Software utilizado no computador pessoal.* O *software* maioritariamente utilizado (Windows, Folha de Cálculo, Apresentações, Processador de Texto) permite inferir a pertinência do estabelecimento de protocolos adequados a possibilitar a utilização deste *software* a custos controlados.

(7) Percepção da segurança do computador pessoal:

⇒ *Classificação atribuída aos níveis de segurança.* Relativamente aos níveis de segurança foi solicitada a classificação de três aspectos distintos, obtendo-se como resultado classificações maioritárias nos níveis 4 e 5, com 61,38% relativamente aos acessos, 59,34% relativamente à *password* e 58,80% no respeitante ao computador pessoal. Esta situação revela uma preocupação clara com os aspectos de segurança, considerando relativamente elevados os respectivos níveis de segurança.

9.3.3. Contributos do Grupo C – Sistema Informático

Os contributos deste grupo foram agregados nos tópicos constantes da tabela seguinte e serão objecto de um desenvolvimento ao longo desta secção:

Temas	Tópicos
Funcionamento e mudanças no Sistema Informático	– <i>Aumentar a participação das Pessoas nas mudanças organizacionais</i>
Conhecimentos e formação em informática	– <i>Definir e implementar plano de formação na área de informática</i>
<i>Password</i> e mecanismos de acesso ao Sistema Informático	– <i>Definir e implementar procedimentos acerca dos acessos ao sistema e dos respectivos mecanismos de acesso</i>
Utilização do correio electrónico	– <i>Definir, implementar e divulgar procedimentos acerca da utilização do correio electrónico</i>
Acesso e utilização do Sistema Informático	– <i>Definir e implementar procedimentos de utilização dos activos do sistema</i> – <i>Publicar e divulgar o documento de suporte às políticas de segurança</i>

Tabela 9.2 – Tópicos do grupo C do questionário

No respeitante ao Sistema Informático do Serviço/Escola, constata-se um reduzido envolvimento das Pessoas nos processos de mudança no sistema, embora a sua maioria refira a participação em acções de formação na área da Informática/Sistemas de Informação e considere relevante os conhecimentos que detêm nesta área.

Constata-se ainda a utilização de *password* como mecanismo usual de acesso ao sistema, embora a sua gestão (alteração, salvaguarda e utilização) não seja efectuada da forma mais adequada.

A frequência de acesso ao sistema, o tipo de utilização e a forma como os recursos disponíveis são utilizados apresenta algumas discrepâncias, tornando-se essencial o estabelecimento dos procedimentos adequados em cada caso concreto, com estes a enquadrarem-se nas políticas de segurança da instituição.

Perante os tópicos identificados através da agregação efectuada nas questões deste grupo, é relevante uma análise genérica dos itens que os inquiridos consideraram relevantes nos diversos contextos apresentados.

Foram assim, de acordo com os aspectos identificados, desenvolvidos os seguintes tópicos:

(1) Funcionamento e mudanças no Sistema Informático:

⇒ *Aumentar a participação das Pessoas nas mudanças organizacionais.*
Constatando-se a existência de mudanças, referenciadas por 80,00% dos inquiridos, verificou-se que apenas 42,02% destes participaram nesses processos, considerando relativamente baixo o seu grau de participação, embora a sua percepção acerca das melhorias no respectivo funcionamento apontem para um grau de satisfação relativamente elevado, níveis 4 e 5 (70,75%). Neste contexto, verifica-se a pertinência de assegurar um maior envolvimento das Pessoas nestas actividades.

(2) Conhecimentos e formação em informática:

⇒ *Definir e implementar plano de formação na área de informática.* As questões deste tópico foram colocadas de forma diferenciada aos grupos de inquiridos, com a experiência prévia na área da Informática e a utilização de computadores a serem maioritariamente referidas. Relativamente à classificação dos

conhecimentos em Informática/Sistemas de Informação, constata-se a existência de classificações em níveis diferentes, para cada um dos grupos de inquiridos, o que releva a necessidade de possuir um plano de formação adequado a cada um dos grupos.

(3) Password e mecanismos de acesso ao Sistema Informático:

⇒ *Definir e implementar procedimentos acerca dos acessos ao sistema e dos respectivos mecanismos de acesso.* Com o acesso ao Sistema Informático do Serviço/Escola a ser a solução adoptada referida por 97,77% dos inquiridos que possuem acesso ao sistema. Todavia, considera-se preocupante o facto de 50,30% destes utilizar opções de escolha de novas *passwords* de fácil descodificação, quando esta é referenciada como meio único de acesso por parte de 64,64% dos inquiridos.

(4) Utilização do correio electrónico:

⇒ *Definir, implementar e divulgar procedimentos acerca da utilização do correio electrónico.* A maioria dos inquiridos refere que possui um endereço de correio nos sistemas informáticos, mencionando também que além desse possui mais um ou dois endereços. Embora a grande maioria dos inquiridos refira a utilização de um endereço associado ao Sistema Informático do Serviço/Escola, não é utilizada a mesma *password* para acesso ao sistema e ao correio electrónico. Constata-se ainda que existe implementado um sistema de filtragem de mensagens de correio electrónico.

(5) Acesso e utilização do Sistema Informático:

⇒ *Definir e implementar procedimentos de utilização dos activos do sistema.* Perante a elevada frequência de acessos ao sistema, e os tempos médios de utilização diária e tipo de actividades realizadas, considera-se essencial definir a utilização aceitável dos activos do sistema.

⇒ *Publicar e divulgar o documento de suporte às políticas de segurança.* Considerando o tipo de utilização do sistema, particularmente quando se constata a disparidade de respostas relativamente às atitudes assumidas quando se perde informação ou desaparecem documentos, impõe-se a necessidade de

proceder à divulgação dos documentos de suporte às políticas de segurança, de modo a ser possível a uniformização de procedimentos.

9.3.4. Contributos do Grupo D – Segurança da Informação

Os contributos deste grupo foram agregados nos tópicos constantes da tabela seguinte e serão objecto de um desenvolvimento ao longo desta secção:

Temas	Tópicos
Políticas de segurança da informação e do Sistema Informático	– <i>Divulgação do documento da política de segurança e outros relacionados</i> – <i>Envolvimento das Pessoas na elaboração das políticas</i>
Mecanismos de protecção do Sistema Informático	– <i>Definir gama de mecanismos de segurança a utilizar</i>
Realização de cópias de segurança	– <i>Política de backups</i>
Percepção da facilidade de acesso ao Sistema Informático	– <i>Elaborar e divulgar documento de utilização do Sistema Informático</i>
Controlo dos activos do sistema e da sua utilização	– <i>Definir e divulgar procedimentos de actuação em caso de ocorrerem violações de segurança</i> – <i>Definir e divulgar os procedimentos adequados ao controlo dos activos</i>
Percepção da segurança do Sistema Informático	– <i>Realizar acções de sensibilização para a problemática da segurança da informação</i> – <i>Realizar acções de formação sobre segurança da informação</i> – <i>Divulgar documento das políticas de segurança e procedimentos relacionados com a utilização dos activos do sistema</i>

Tabela 9.3 – Tópicos do grupo D do questionário

Em termos de segurança do Sistema Informático do Serviço/Escola, constata-se um elevado desconhecimento acerca da sua existência e dos aspectos concretos que são abrangidos, com a participação das Pessoas na sua elaboração e/ou alteração a apresentar-se bastante reduzida.

A utilização de mecanismos de segurança complementares à *password*, apresenta alguma difusão, embora não se encontrem abrangidos todos os aspectos essenciais à segurança, procurando se possível enquadrar a política de *backups* com as políticas de segurança institucionais.

A facilidade de acesso aos recursos e o controlo da utilização adequada dos activos do sistema apresenta necessidades de ser enquadrado por procedimentos englobados na

política de segurança, considerando a pertinência de publicitar e divulgar por todos os interessados a documentação de suporte dessas mesmas políticas

Perante os tópicos identificados através da agregação efectuada nas questões deste grupo, é pertinente uma análise genérica dos itens que os inquiridos consideraram relevantes nos diversos contextos apresentados.

Foram assim, de acordo com os aspectos identificados, desenvolvidos os seguintes tópicos:

(1) Políticas de segurança da informação e do Sistema Informático:

⇒ *Divulgação do documento da política de segurança e outros relacionados.*

Considerando o facto de 55,36% dos inquiridos referenciar desconhecimento ou até inexistência de políticas de segurança, existir uma grande diversidade nas respostas acerca da forma como tomaram conhecimento dessas políticas e até os aspectos abrangidos, é fundamental proceder à adequada publicitação e divulgação da documentação de suporte a essas políticas.

⇒ *Envolvimento das Pessoas na elaboração das políticas.* Acerca do envolvimento das Pessoas, verifica-se que a sua grande maioria (84,00%) não teve qualquer participação, e as que participaram referem envolvimento e níveis de participação bastante diferenciados, reforçando a perspectiva de ser útil um aumento do envolvimento das Pessoas nestas actividades.

(2) Mecanismos de protecção do Sistema Informático:

⇒ *Definir gama de mecanismos de segurança a utilizar.* Os mecanismos de segurança utilizados, além da *password*, são os mesmos referenciados pelos inquiridos relativamente aos seus computadores pessoais, ou seja, *Firewall*, *Antivirus* e *AntiSpyware*, com a utilização de outros dispositivos a ser mínima. Por outro lado, constata-se que a maioria dos inquiridos refere o desconhecimento (41,96%) ou a inexistência (34,82%) de tempo limite das sessões de trabalho, embora a maioria (50,45%) referencie a utilização de mecanismos de protecção do ecrã dos computadores utilizados. Este contexto reforça a necessidade de se proceder a uma definição clara dos mecanismos a utilizar, adequando-os às necessidades organizacionais, de acordo com as políticas definidas e implementadas.

(3) Realização de cópias de segurança:

⇒ *Política de backups.* Considerando que estas questões apenas foram colocadas aos Técnicos, constata-se a existência de uma política de *backups* que inclui regras em função da criticidade da informação, definindo-se a periodicidade com que se concretizam, referenciando-se esta como diária por parte de todos os inquiridos, que no entanto divergem relativamente a outras periodicidades. Nesta situação considera-se útil proceder a uma uniformização de procedimentos, particularmente quando 12 dos inquiridos referencia aspectos associados à realização de *backups*, contrariando o facto de apenas 9 terem referenciado que os *backups* estavam abrangidos pelas políticas de segurança (questão D3).

(4) Percepção da facilidade de acesso ao Sistema Informático:

⇒ *Elaborar e divulgar documento de utilização do Sistema Informático.* As respostas obtidas quando se solicita uma classificação para a facilidade de acesso físico ao sistema, além de apresentarem uma grande dispersão pelos diversos níveis, realça a convergência de todos os grupos de inquiridos na identificação da “sala de servidores” como o local com maior dificuldade de acesso.

(5) Controlo dos activos do sistema e da sua utilização:

⇒ *Definir e divulgar procedimentos de actuação em caso de ocorrerem violações de segurança.* Mesmo constatando-se que a maioria dos inquiridos refere nunca ter presenciado violações de segurança, verifica-se que a actuação dos que já presenciaram não segue um padrão, agindo de acordo com perspectivas individuais.

⇒ *Definir e divulgar os procedimentos adequados ao controlo dos activos.* Verificando-se a percepção de que algumas actividades efectuadas em locais de acesso ao sistema são proibidas, as respostas apresentam algumas incoerências, particularmente quando referem como proibidas algumas actividades essenciais à utilização habitual do Sistema Informático. Refira-se ainda o facto de, existindo esta consciência, ser tão diminuto o número de inquiridos que refere ter presenciado violações de segurança, quando tudo o que está proibido nestes locais de acesso poder ser considerada uma violação da segurança. Neste contexto, refira-se a existência, referida pela maioria dos Técnicos inquiridos, de

registos de *software* e *hardware* existente, embora alguns deles (30,77%) desconheçam a sua periodicidade.

(6) Percepção da segurança do Sistema Informático:

- ⇒ *Realizar acções de sensibilização para a problemática da segurança da informação.* A maioria dos inquiridos (74,11%) refere o desconhecimento da existência de qualquer acção de sensibilização para a problemática da segurança da informação, com os outros inquiridos a referirem opções distintas (não ter sido convidado(a) ou ter participado), realçando-se que a maioria dos Técnicos (64,29%) menciona ter tido conhecimento de acções deste tipo.
- ⇒ *Realizar acções de formação sobre segurança da informação.* Quando se colocou a questão de classificar, de acordo com a sua percepção, os níveis de segurança do Sistema Informático e em que medida essa segurança é importante para as suas actividades, a maioria dos inquiridos classifica a segurança nos níveis 4 (41,52%) e 5 (26,34%), enquanto que a sua importância para as actividades é classificada nos níveis 5 (33,93%) e 6 (37,50%).
- ⇒ *Divulgar documento das políticas de segurança e procedimentos relacionados com a utilização dos activos do sistema.* Relativamente à classificação de algumas facilidades e recursos do sistema, o ‘Correio electrónico’, as ‘Pessoas/Utilizadores/Técnicos’, a ‘Internet’ e a ‘Rede informática’, são os aspectos assumidos como mais importantes, considerando menos importantes os ‘Periféricos’ e o ‘Sistema de comunicações’. Já no respeitante à classificação das ameaças, os ‘Virus/Trojan Horses/Worms/etc.’, os ‘Hackers’ e a ‘Destrução de informação’ surgem como os mais importantes, sendo os ‘Acidentes naturais’ e a ‘Definição por defeito das *passwords* iniciais’ as ameaças consideradas como menos importantes.

9.3.5. Contributos do Grupo E – Usabilidade do Sistema Informático

Os contributos deste grupo foram agregados nos tópicos constantes da tabela seguinte e serão objecto de um desenvolvimento ao longo desta secção:

Temas	Tópicos
Formação na utilização do Sistema	– Definir e implementar plano de formação para utilização do sistema – Divulgar o documento de suporte às políticas de segurança e outros documentos relacionados
Facilidade de utilização e aprendizagem do sistema	– Proporcionar um maior envolvimento das Pessoas nos processos de desenvolvimento e implementação de sistemas

Tabela 9.4 – Tópicos do grupo E do questionário

A percepção dos inquiridos acerca da realização de acções de formação na utilização do sistema apresenta algumas discrepâncias em termos de cada um dos grupos de inquiridos, embora seja consensual a relevância dessa mesma formação. Considerando-se relevante, neste contexto, a existência e divulgação de informação de suporte à utilização do sistema.

A facilidade de utilização e de aprendizagem é classificada num elevado nível de relevância e consensual entre os grupos de inquiridos. No mesmo sentido emerge a elevada importância atribuída à usabilidade do Sistema Informático para as actividades desenvolvidas, com a sua utilização, pelos diversos grupos de inquiridos.

Além disso, os aspectos identificados como mais relevantes para a usabilidade do Sistema Informático, tornam cruciais, além de outras medidas, um incremento da participação das Pessoas nas actividades associadas, directa ou indirectamente, ao desenvolvimento e/ou implementação de um sistema.

Face aos tópicos identificados através da agregação efectuada nas questões deste grupo, é essencial proceder a uma análise genérica dos itens que os inquiridos consideraram relevantes nos diversos contextos apresentados.

Foram assim, de acordo com os aspectos identificados, desenvolvidos os seguintes tópicos:

(1) Formação na utilização do sistema:

⇒ *Definir e implementar plano de formação para utilização do sistema.* Das respostas obtidas ressalta a diferença entre Docentes, cuja maioria refere não ter recebido formação na utilização do Sistema Informático, e os Não Docentes e Técnicos, que referem a situação oposta. Esta situação reflecte-se na classificação da relevância dessa formação, que os Docentes enquadram maioritariamente nos níveis 4 e 5, enquanto que os Não Docentes e Técnicos

atribuem maioritariamente os níveis 5 e 6. Relativamente às acções de formação proporcionadas aos utilizadores finais, a maioria dos Técnicos refere a sua inexistência, notando-se algumas divergências no respeitante à frequência com que são realizadas.

⇒ *Divulgar o documento de suporte às políticas de segurança e outros documentos relacionados.* Embora a maioria dos Técnicos (78,54%) refira que são elaborados documentos acerca da utilização do Sistema Informático, a maioria dos Docentes (65,68%) e dos Não Docentes (73,68%) menciona o desconhecimento ou mesmo a inexistência desse tipo de documentos. De entre os que referem a sua existência, não é idêntica a forma pela qual tomaram conhecimento dos documentos, com a classificação desse documentos a ser entendida como bastante útil por qualquer destes dois grupos de inquiridos.

(2) Facilidade de utilização e aprendizagem do sistema:

⇒ *Proporcionar um maior envolvimento das Pessoas nos processos de desenvolvimento e implementação de sistemas.*

Relativamente à facilidade de utilização e aprendizagem do Sistema Informático, a maioria dos inquiridos atribui uma classificação nos níveis 4 e 5, respectivamente 60,27% e 63,39% para as referidas questões.

No respeitante à importância da usabilidade do Sistema Informático para as actividades desenvolvidas, a maioria dos inquiridos apresenta uma classificação entre os níveis 5 e 6 (79,91%).

Acerca da classificação da relevância de alguns aspectos para a usabilidade do Sistema Informático, a ‘Facilidade de acesso’, a ‘Disponibilidade’ e a ‘Adequação às necessidades’, são classificadas como as mais importantes, verificando-se que a ‘Participação no desenvolvimento/implementação do sistema’ e o ‘Conhecimento prévio do sistema’ são assumidos como os aspectos menos importantes, esta situação apresenta desde logo uma contradição pela impossibilidade de, por exemplo, proceder a uma adequação do sistema às necessidades, quando a participação das Pessoas no desenvolvimento e/ou implementação do sistema é assumida como o aspecto menos importante.

9.4. Análise das Questões de Partida na Perspectiva da Segurança

Numa apreciação global das respostas às questões relacionadas com a segurança, considerando as suas diversas inter relações, é possível constatar que existe uma preocupação clara com esta problemática, notando-se todavia a necessidade do estabelecimento de procedimentos e políticas de segurança enquadradas na missão e nas estratégias institucionais.

Em termos de segurança, as questões foram colocadas em dois contextos distintos: o primeiro engloba a percepção das Pessoas e o seu conhecimento acerca das práticas, procedimentos e políticas utilizadas, o segundo considerando os aspectos a classificar em função da percepção das Pessoas acerca de cada questão concreta.

O primeiro contexto, percepção das Pessoas acerca da segurança da informação, compreende os seguintes agrupamentos de questões:

- ⇒ Grupo B: (i) Utilização do computador pessoal; (ii) Utilização e gestão de *password*; (iii) Utilização de outros mecanismos de protecção; (iv) Realização e gestão de *backups*.
- ⇒ Grupo C: (i) Utilização e gestão de *password*; (ii) Utilização de áreas de trabalho nos servidores; (iii) Utilização de impressoras partilhadas.
- ⇒ Grupo D: (i) Conhecimento das políticas de segurança; (ii) Participação na elaboração e/ou alteração das políticas de segurança; (iii) Realização e gestão de *backups*; (iv) Utilização de outros mecanismos de protecção; (v) Acessos ao sistema.

O segundo contexto, classificação da segurança da informação numa perspectiva pessoal, engloba os seguintes agrupamentos de questões:

- ⇒ Grupo B: (i) Segurança do acesso à Internet; (ii) Grau de segurança da *password*; (iii) Grau de segurança do computador pessoal.
- ⇒ Grupo C: (i) Grau de segurança da *password*.
- ⇒ Grupo D: (i) Segurança do Sistema Informático; (ii) Importância da segurança do Sistema Informático para as actividades realizadas; (iii) Aspectos relevantes para a

segurança do Sistema Informático; (iv) Impacto de ameaças na segurança do Sistema Informático.

Além dos dois contextos anteriormente referenciados, deve ainda ser considerado um terceiro contexto, não na segurança da informação mas na utilização dos SI e das TIC por parte das Pessoas, englobando os seguintes agrupamentos de questões:

- ⇒ Grupo B: (i) Frequência de utilização do computador pessoal; (ii) Tipo de utilização do computador pessoal; (iii) *Software* utilizado no computador pessoal.
- ⇒ Grupo C: (i) Envolvimento nas mudanças dos Sistemas Informáticos; (ii) Formação na área de Informática; (iii) Frequência de utilização do Sistema Informático; (iv) Tipo de utilização do Sistema Informático; (v) *Software* utilizado.
- ⇒ Grupo D: (i) Acesso aos activos do Sistema Informático e a sua utilização.
- ⇒ Grupo E: (i) Formação na utilização do Sistema Informático; (ii) Documentos de apoio à utilização do Sistema Informático; (iii) Facilidade de utilização do Sistema Informático; (iv) Facilidade de aprendizagem do Sistema Informático; (v) Aspectos relevantes para a usabilidade do Sistema Informático; (vi) Importância da usabilidade do Sistema Informático para as actividades realizadas.

9.4.1. Percepção das Pessoas acerca da Segurança da Informação

O facto de as Pessoas utilizarem os seus computadores pessoais para aceder à Internet em locais onde, em princípio, não possuem controlo acerca da segurança dos respectivos acessos, indicia uma percepção deficitária em termos das ameaças a que se encontram sujeitos, situação esta reforçada pelo facto de terem uma elevada frequência de acesso e tempos de ligação com alguma duração.

Por outro lado, a baixa taxa de utilização de *passwords* e, para quem utiliza, não ser muito frequente proceder à sua alteração, com esta a ser feita através do recurso a opções relativamente fáceis de descodificar, contribui para realçar a necessidade de existir um controlo mais estreito sobre onde, como e quem utiliza.

Além disso, a utilização de mecanismos de protecção complementares à *password*, devido à sua elevada taxa de utilização parece ir em contra ciclo com a utilização da

própria *password*, até porque a sua utilização requer conhecimentos relevantes na área da informática, além dos custos associados a uma frequência de actualização referida como relativamente elevada.

A opção pela realização de *backups*, as periodicidades escolhidas, as opções tomadas relativamente ao que salvar e os espaços de armazenamento escolhidos realçam a diversidade de alternativas assumidas pelas Pessoas, considerando-se pertinente a existência de uma política de *backups* e a realização de acções de formação na área da segurança da informação.

Contrariamente ao que sucedia relativamente à alteração da *password* do computador pessoal, constata-se que é mais frequente proceder à sua alteração quando se trata do Sistema Informático do Serviço/Escola, continuando todavia a ser feita com recurso a opções relativamente fáceis de decodificar, reforçando a necessidade de estabelecer procedimentos para um controlo mais efectivo sobre a gestão das *passwords*.

A utilização de áreas de trabalho privadas no Sistema Informático do Serviço/Escola é efectuada por pouco mais de metade das Pessoas, guardando maioritariamente ficheiros de trabalho, constatando-se que a grande maioria nunca perdeu qualquer informação aí guardada. Já no respeitante a quem perdeu informação, não existe um padrão claro em termos de atitude tomada para a recuperar, nem um controlo eficaz sobre o que sucedeu, considerando-se por isso essencial a definição de procedimentos que permitam um controlo adequado deste tipo de problemas.

Já no respeitante à impressão de documentos através de impressoras partilhadas, constata-se uma grande diversidade de opções tomadas, quer quando não encontra os seus documentos, quer quando encontra documentos que não são seus, parecendo não existir uma percepção coerente do que fazer, como e quando fazer, realçando mais uma vez a necessidade de estabelecer e divulgar os procedimentos adequados de modo a evitar as situações que surgem com maior frequência, e que configuram violações das políticas de segurança.

Relativamente a aspectos associados com o conhecimento das políticas de segurança implementadas, considera-se preocupante o facto da maioria das Pessoas desconhecer a sua existência, referindo-se que, de entre as que conhecem, esse conhecimento ter sido

adquirido de formas bastante distintas, existindo também uma grande diversidade acerca dos aspectos abrangidos por essas mesmas políticas.

Além disso, sendo diminuta a participação das Pessoas na elaboração e/ou alteração das políticas, transparece a necessidade de um maior envolvimento neste tipo de actividades, particularmente quando se constata envolvimento muito diversificados e sem continuidade (a maioria dos que participaram classificam essa participação entre os níveis 3 e 4).

Perante a especificidade das regras relacionadas com a utilização de mecanismos de protecção complementares e com a realização de *backups*, estas situações foram colocadas apenas aos Técnicos de Informática. Neste contexto, verifica-se que os mecanismos mais referenciados coincidem exactamente com as respostas obtidas no mesmo âmbito acerca da utilização dos computadores pessoais, indo no mesmo sentido a frequência de actualização desses mecanismos.

No que se relaciona directamente com os *backups*, considerando que a situação se encontra condicionada por políticas institucionais, não existe uma similaridade com opções pessoais, constatando-se todavia alguma convergência em termos dos dispositivos adoptados e das opções de armazenamento assumidas, referindo-se assim a necessidade de se proceder à definição de procedimentos adequados a este tipo de situação.

Em termos dos acessos, nomeadamente em termos de facilidade de acesso, a sala de servidores e os serviços de informática são considerados como os que apresentam maiores dificuldades, já as zonas de circulação internas e externas surgem como as de maior facilidade de acesso. Todavia, o que transparece como aspecto a ter em atenção é o facto de existir uma grande diversidade em termos dos níveis de classificação atribuídos, transmitido algum desconhecimento relativamente às condições de acesso e utilização do sistema, o que implica a documentação adequada em termos de acesso ao sistema e da sua utilização.

9.4.2. Classificação da Segurança da Informação numa Perspectiva Pessoal

O facto de as Pessoas utilizarem os seus computadores pessoais para aceder à Internet em locais onde, em princípio, não possuem controlo acerca da segurança dos respectivos acessos, indicia uma percepção deficitária em termos das ameaças a que se encontram sujeitos, situação esta reforçada pelo facto de terem uma elevada frequência de acesso e tempos de ligação com alguma duração.

Em termos das classificações obtidas, regista-se que em qualquer das situações de segurança (acesso, *password*, computador pessoal), os inquiridos referem maioritariamente os níveis 4 e 5, constatando-se que as percentagens acumuladas nestes níveis são de 61,38% relativamente aos acessos, 59,34% relativamente à *password* e 58,80% no respeitante ao computador pessoal.

Relativamente ao grau de segurança da *password* de acesso ao sistema informático constata-se que 63,35% dos inquiridos a classifica maioritariamente nos níveis 4 e 5, constatando-se neste caso concreto que existe uma maior percentagem a atribuir estes níveis comparativamente com a *password* do computador pessoal.

A segurança do Sistema Informático é maioritariamente classificada nos níveis 4 e 5, transparecendo deste modo uma percepção bastante favorável (67,86%) perante a segurança proporcionada, com uma tendência clara para o nível 4. Já no que respeita à importância dessa segurança para as actividades realizadas no sistema, verifica-se um aumento substancial na percepção favorável assumida pelos inquiridos, com os níveis 5 e 6, correspondentes a um total de 71,43%, a serem maioritariamente referidos, registando-se uma tendência para o nível 6. Esta situação indicia uma preocupação nítida com a segurança realçando a sua importância para as diversas actividades dos inquiridos.

Como aspectos com maior relevância para a segurança da informação identificam-se o ‘Correio Electrónico’ (59,82%), as ‘Pessoas’ (58,04%), a ‘Rede Informática’ (57,59%), e a ‘Internet’ (57,59%), enquanto que em termos de impacto das ameaças na segurança do Sistema Informático, se constata que os ‘*Virus/Trojan Horses/Worms/etc.*’ (65,18%), os ‘*Hackers*’ (63,39%), a ‘Destruição da Informação’ (61,16%), os ‘Acessos indevidos

a partir do interior' (59,82%), e o 'Roubo da Informação' (58,04%), constituem as ameaças com maior impacto no sistema.

Na perspectiva oposta, os aspectos com menor relevância para a segurança da informação são os 'Periféricos' (14,29%), o 'Sistema de Comunicações' (12,95%), as 'Leis/Políticas/Regulamentos/Procedimentos' (7,59%), e os 'Computadores Pessoais' (5,36%). As ameaças com menor impacto na segurança do Sistema Informático são os 'Acidentes Naturais' (8,04%), a 'Definição por defeito das *passwords* iniciais' (7,14%), a 'Configuração incorrecta da *firewall*' (5,36%), e as 'Falhas no fornecimento de energia eléctrica ao sistema' (4,91%).

Neste contexto de percepção das Pessoas acerca da segurança da informação, deve referenciar-se o facto de as 'Leis/Políticas/Regulamentos/Procedimentos' serem consideradas como um dos aspectos menos relevantes para a segurança da informação, contrastando com o facto da segurança do Sistema Informático ser considerado muito importante para as suas actividades, 71,43% das respostas, e com a identificação das ameaças com maior impacto na segurança, quando as que foram identificadas são as que dependem mais directamente de políticas, procedimentos e regulamentos. Situação similar ocorre com o 'Sistema de Comunicações', quando a maioria dos inquiridos menciona ter encontrado documentos que não são seus, ou não encontra documentos que mandou imprimir.

9.4.3. Percepção das Pessoas acerca da Utilização dos SI e das TIC

Os resultados obtidos permitem constatar que a grande maioria das Pessoas utiliza o seu computador diariamente ou quase diariamente, e quando o fazem, essa utilização é efectuada durante uma a três horas (48,15%) ou por mais de três horas (33,33%).

Em termos de utilização, as actividades mais frequentes são a 'Elaboração de relatórios e outros trabalhos', as 'Pesquisas na Internet' e o 'Envio/Recepção de correio electrónico', qualquer delas com valores superiores a 80%.

Verifica-se ainda que o sistema operativo mais utilizado é o Windows (91,67%), enquanto que as aplicações mais utilizadas são a folha de cálculo e o processador de texto, qualquer delas com valores superiores a 85%.

Relativamente ao envolvimento das Pessoas nas mudanças, verifica-se que essa participação é insatisfatória (cerca de 42%), sendo bastante diversas as actividades em que participam. Todavia, as Pessoas que participam nessas actividades atribuem uma classificação centrada nos níveis 3 e 4, com uma tendência para o nível 2. Constatase no entanto que a maioria das Pessoas (níveis 4 e 5) refere a sua satisfação com as mudanças efectuadas, mencionando ainda a sua percepção de que o funcionamento do Sistema Informático melhorou (níveis 4 e 5), com um valor de 70% em qualquer destas situações.

A questão dos conhecimentos prévios em informática apenas foi colocada aos Não Docentes, constatando-se que a sua maioria já tinha efectuado formação na área da informática, possuindo também conhecimentos acerca da utilização de computadores.

Relativamente às questões de formação dos Técnicos, a sua maioria refere frequentar uma média anual de uma a duas acções, classificando essas acções nos níveis 5 e 6 (78,57%). Por outro lado, quando se questionam os inquiridos acerca dos conhecimentos em Informática/Sistemas de Informação, a sua maioria classifica esses conhecimentos nos níveis 3 e 4 (64,52%).

No que diz respeito à frequência de utilização, a grande maioria das Pessoas refere que utiliza o sistema informático diariamente ou quase diariamente (92,86%), e quando o fazem, essa utilização é efectuada durante três a cinco horas (25,00%) ou por mais de cinco horas (33,48%).

Em termos de utilização, as actividades mais frequentes são o ‘Envio/Recepção de correio electrónico’, as ‘Pesquisas na Internet’ e a ‘Impressão de documentos’, qualquer delas com valores superiores a 85%.

Verifica-se ainda que o sistema operativo mais utilizado é o Windows (91,07%), enquanto que as aplicações mais utilizadas são a folha de cálculo e o processador de texto, qualquer delas com valores de 75%.

Como locais com maior dificuldade de acesso físico ao Sistema Informático identificam-se a ‘Sala de servidores’ (49,98%) e os ‘Serviços de Informática’ (29,02%), constatando-se todavia uma grande diversidade nas respostas. Na perspectiva oposta os locais com menor dificuldade de acesso físico ao Sistema Informático são os ‘Átrios/Corredores’ (33,48%) e as ‘Salas de informática para alunos’ (315,34%).

As actividades proibidas nos locais de acesso ao Sistema Informático, maioritariamente referidas, são ‘Fumar’, ‘Movimentar computadores instalados’ e ‘Instalar/Desinstalar *software*’, verificando-se que 9,38% dos inquiridos refere a ‘Realização de cópias dos trabalhos’ como uma actividade proibida, quando o pressuposto de instalação destas salas é precisamente o contrário.

Quando questionados(as) acerca da existência de políticas de segurança do Sistema Informático, a maioria dos inquiridos menciona a sua não existência ou desconhecimento acerca disso. Acerca dos aspectos abrangidos por essas políticas, os mais referenciados são a ‘Definição de acessos ao sistema’ (80,00%), a ‘Utilização do correio electrónico’ (62,00%) e o ‘Acesso aos servidores’ (46,00%), constatando-se também que a sua maioria não teve qualquer participação na elaboração/alteração dessas políticas.

No respeitante à formação na utilização do Sistema Informático, constata-se que a maioria dos inquiridos (58,48%) não recebeu qualquer formação. De entre os que responderam afirmativamente constata-se que a maioria (63,10%, correspondente a 23,66% do total de inquiridos) refere que recebem formação ‘sempre que existem mudanças no sistema’, com a relevância dessa formação a ser maioritariamente classificada nos níveis 5 e 6 (62,36%). Relativamente às respostas dos Técnicos sobre as acções de formação e a sua frequência, verifica-se que as tendências mencionadas são idênticas.

A existência de documentos de apoio à utilização do Sistema Informático é desconhecida ou considerada inexistente pela maioria dos inquiridos (68,54%). O modo como tomaram conhecimento desses documentos foi através de documento entregue no Serviço/Escola (53,03%) ou através de informação dos Serviços de Informática (45,45%), com a sua relevância a ser classificada nos níveis 3, 4 e 5 (81,82%). Acerca da existência de documentos de apoio à utilização do Sistema Informático, os Técnicos referem maioritariamente (78,57%) a sua existência, o que apresenta uma situação contrária ao mencionado pelos Docentes e Não Docentes.

Quer a facilidade de utilização quer a facilidade de aprendizagem do Sistema Informático, são maioritariamente (60,27% e 63,39% respectivamente) classificadas pelos inquiridos nos níveis 4 e 5.

Como aspectos mais relevantes para a usabilidade do Sistema Informático, referem-se a ‘Facilidade de acesso’, a ‘Disponibilidade’ e a ‘Adequação às necessidades’, enquanto que os menos importantes correspondem à ‘Participação no desenvolvimento/implementação do sistema’ e ao ‘Conhecimento prévio do sistema’. Deve ainda referenciar-se a grande diversidade das respostas nos diversos níveis de classificação.

Acerca da importância da usabilidade do Sistema Informático para as actividades realizadas pelos inquiridos, verifica-se que esta é maioritariamente classificada nos níveis 5 e 6, com um valor total de 79,91%.

9.4.4. Impactos dos SGSI nas Actividades das Pessoas

Face à principal questão a que importa responder ‘Qual o impacto na actividade das pessoas quando se implementa um SGSI?’, pode inferir-se dos contextos anteriores um conjunto de itens relevantes, directamente associados com as atitudes e com os comportamentos das Pessoas no contexto dos SGSI.

Neste âmbito, embora se considere que os resultados do grupo B dos questionários são importantes para um entendimento mais alargado da percepção das Pessoas, serão apenas considerados aqui os itens mais relevantes abordados nos grupos C, D e E dos questionários, com estes a serem obtidos através dos tópicos especificados em função dos contributos dos grupos constantes dos questionários.

Para se chegar à principal questão a responder, importa em primeiro lugar perceber as respostas às questões parciais, obtidas através dos itens considerados mais relevantes, de acordo com a percepção das Pessoas acerca de cada uma dessas questões parciais.

A(s) resposta(s) à Questão 1 (Qual a percepção dos utilizadores acerca da segurança da informação existente no Sistema de Informação?) pode(m) ser obtida(s) através dos seguintes itens:

- Utilização e gestão das *passwords*;
- Utilização de áreas de trabalho nos servidores;
- Utilização de impressoras partilhadas;
- Conhecimento das políticas de segurança;
- Participação na elaboração e/ou alteração das políticas de segurança;

- Realização e gestão de *backups*;
- Utilização de mecanismos de protecção;
- Acessos ao sistema.

Itens relevantes na Questão 1	Impactos nas actividades das Pessoas
Utilização e gestão das <i>passwords</i>	<i>Cumprir as políticas definidas para as passwords</i>
Utilização de áreas de trabalho nos servidores	<i>Cumprir as políticas de utilização dos activos</i>
Utilização de impressoras partilhadas	<i>Cumprir as políticas de utilização dos activos</i>
Conhecimento das políticas de segurança	<i>Manter actualizado o documento da política de segurança</i>
Participação na elaboração e/ou alteração das políticas de segurança	<i>Colaborar nas actividades a desenvolver</i>
Realização e gestão de <i>backups</i>	<i>Cumprir as políticas de utilização e protecção dos activos</i>
Utilização de mecanismos de protecção	<i>Respeitar os procedimentos definidos para estes mecanismos</i>
Acessos ao sistema	<i>Cumprir as políticas de controlo e gestão de acessos</i>

Tabela 9.5 – Itens relevantes na Questão 1 *versus* Impactos na actividade das Pessoas

Por seu lado, a(s) resposta(s) à Questão 2 (Que indicadores possibilitam a avaliação da segurança de um Sistema de Informação e a avaliação de um Sistema de Gestão da Segurança da Informação?) pode(m) ser obtida(s) através dos seguintes itens:

- Grau de segurança da *password*;
- Segurança do Sistema Informático;
- Importância da segurança do Sistema Informático para as actividades realizadas;
- Aspectos relevantes para a segurança do Sistema Informático;
- Impacto de ameaças na segurança do Sistema Informático.

Itens relevantes na Questão 2	Impactos nas actividades das Pessoas
Grau de segurança da <i>password</i>	<i>Cumprir as políticas definidas para as passwords</i>
Segurança do Sistema Informático	<i>Cumprir as políticas de segurança implementadas</i>
Importância da segurança do Sistema Informático para as actividades realizadas	<i>Cumprir as políticas de segurança implementadas</i>
Aspectos relevantes para a segurança do Sistema Informático	<i>Cumprir as políticas de segurança implementadas</i>
Impacto de ameaças na segurança do Sistema Informático	<i>Cumprir as políticas de segurança implementadas</i>

Tabela 9.6 – Itens relevantes na Questão 2 *versus* Impactos na actividade das Pessoas

Por último, a(s) resposta(s) à Questão 3 (Como são aceites pelas pessoas as mudanças tecnológicas e organizacionais motivadas pela implementação do Sistema de Gestão da Segurança da Informação?) pode(m) ser obtida(s) através dos seguintes itens:

- Envolvimento nas mudanças dos Sistemas Informáticos;
- Formação na área de Informática;
- Frequência de utilização do Sistema Informático;
- Tipo de utilização do Sistema Informático;
- *Software* utilizado;
- Acesso aos activos do Sistema Informático e a sua utilização
- Formação na utilização do Sistema Informático;
- Documentos de apoio à utilização do Sistema Informático;
- Facilidade de utilização do Sistema Informático;
- Facilidade de aprendizagem do Sistema Informático;
- Aspectos relevantes para a usabilidade do Sistema Informático;
- Importância da usabilidade do Sistema Informático para as actividades realizadas.

Itens relevantes na Questão 3	Impactos nas actividades das Pessoas
Envolvimento nas mudanças dos Sistemas Informáticos	<i>Participar nas actividades de acordo com as suas competências e necessidades</i>
Formação na área de Informática	<i>Participar nas acções de acordo com os planos</i>
Frequência de utilização do Sistema Informático	<i>Cumprir as políticas de utilização dos activos</i>
Tipo de utilização do Sistema Informático	<i>Cumprir as políticas de utilização dos activos</i>
<i>Software</i> utilizado	<i>Cumprir as políticas de utilização dos activos</i>
Acesso aos activos do Sistema Informático e a sua utilização	<i>Cumprir as políticas de utilização dos activos</i>
Formação na utilização do Sistema Informático	<i>Participar nas acções de acordo com os planos estabelecidos</i>
Documentos de apoio à utilização do Sistema Informático	<i>Respeitar as regras definidas pelo documento</i>
Facilidade de utilização do Sistema Informático	<i>Garantir que são cumpridos os requisitos dos utilizadores</i>
Facilidade de aprendizagem do Sistema Informático	<i>Garantir que são cumpridos os requisitos dos utilizadores</i>
Aspectos relevantes para a usabilidade do Sistema Informático	<i>Garantir que os novos ou a alterar respeitam estes aspectos</i>
Importância da usabilidade do Sistema Informático para as actividades realizadas	<i>Garantir que são cumpridos os requisitos dos utilizadores</i>

Tabela 9.7 – Itens relevantes na Questão 3 *versus* Impactos na actividade das Pessoas

Pode assim procurar-se a identificação dos potenciais impactos na actividade das Pessoas, que conduz a situação para a questão de partida do trabalho (Qual o impacto na actividade das pessoas quando se implementa um SGSI?), tendo em conta as respostas às questões parciais, ou seja, considerando-as como os ‘itens relevantes’.

Refira-se ainda que, sempre que se verificou a existência de uma sobreposição entre os itens identificados, se optou por considerar apenas o que for entendido como mais relevante para o contexto.

Esta identificação permite caracterizar os principais impactos a que as Pessoas podem ficar sujeitas a quando da implementação de SGSI, possibilitando a tomada de medidas adequadas a minimizar ou atenuar esses mesmos impactos, de forma a potenciar o desempenho das Pessoas nas organizações, contribuindo para a aquisição de vantagens competitivas, e simultaneamente para facilitar os processos de adopção dos SI e das TIC, e aderir aos SGSI implementados.

Os itens considerados relevantes nas respostas às questões de partida deste trabalho, nomeadamente os constantes das tabelas 9.5 (Itens relevantes na Questão 1 *versus* Impactos na actividade das Pessoas), 9.6 (Itens relevantes na Questão 2 *versus* Impactos na actividade das Pessoas) e 9.7 (Itens relevantes na Questão 3 *versus* Impactos na actividade das Pessoas).

Neste mesmo âmbito, devem ser também considerados os temas e tópicos referenciados nas tabelas 9.1 (Tópicos do grupo B do questionário), 9.2 (Tópicos do grupo C do questionário), 9.3 (Tópicos do grupo D do questionário) e 9.4 (Tópicos do grupo E do questionário).

Os dois contextos anteriores deverão ser utilizados como base de sustentação da implementação de um SGSI do IPS, permitindo que as Pessoas contribuam para o sucesso deste sistema através da aplicação do MIDImOS como referência fundamental para a plena utilização dos referidos itens, obtidos da análise e apreciação dos resultados dos questionários.

9.5. Validação do MIDImOS

A validação é assegurada pelo cumprimento dos aspectos da segurança aos quais foi dada maior relevância nas respostas aos questionários e que foram utilizados para enquadrar as respostas às questões de partida do trabalho.

A outra componente da validação é assegurada pelo cumprimento da legislação em vigor e do normativo aplicável que foi seleccionado para suportar a definição da política de segurança da informação e a implementação do respectivo SGSI.

Considera-se ainda que o processo de validação deverá ser apoiado pelas métricas definidas especificamente para cada caso concreto, salientando-se a importância da análise das especificações no que concerne às questões subjacentes à cultura, estratégia e objectivos de negócio.

Como principais resultados da avaliação dos impactos registados em função das respostas dos questionários referem-se:

- ⇒ A Questão 1 possibilitará a inclusão nos processos de validação do Modelo, as actividades relacionadas com a Gestão de Acessos e com a Utilização dos Activos do Sistema.
- ⇒ Relativamente aos aspectos associados à Questão 2 são relevados dois contextos fundamentais: Políticas de Segurança e Monitorização da Utilização do Sistema.
- ⇒ No que diz respeito à Questão 3, utilização dos SI e das TIC, nomeadamente a percepção das Pessoas e os impactos nas suas actividades, são realçados genericamente os seguintes aspectos: Controlo das Alterações, Formação, Utilização dos Activos do Sistema, Gestão de Acessos.

9.5.1. Análise dos Resultados

Recorde-se todavia, que a Questão 1 diz respeito à percepção que as Pessoas possuem acerca da segurança da informação, enquanto que a Questão 2 tem a ver com a avaliação dessa mesma segurança. Já a Questão 3, está associada à aceitação por parte das Pessoas, das mudanças tecnológicas e organizacionais, forçadas pela implementação de um SGSI.

A identificação dos itens relevantes para obtenção das respostas às questões, decorrente da análise das respostas aos questionários e da especificação dos seus principais contributos para os diversos temas, permitiu a especificação dos potenciais impactos que podem afectar a actividade das Pessoas.

Desta actividade resultou a necessidade de proceder ao enquadramento desses potenciais impactos com referenciais do MIDImOS, de modo a ser possível eliminar ou reduzir eventuais dados, resultantes dos referidos impactos, que pudessem condicionar ou mesmo impedir as Pessoas de desempenhar eficaz e eficientemente as suas normais actividades na organização.

As tabelas que a seguir se apresentam resultam da agregação, às tabelas 9.5, 9.6 e 9.7, relacionadas com as Questões 1, 2 e 3 respectivamente, de referenciais constantes do MIDImOS. Refira-se aliás que os aspectos anteriormente especificados relativos à Questão 1, são directamente aplicáveis às Questões 2 e 3.

Itens relevantes na Questão 1	Impactos nas actividades das Pessoas	Referenciais do MIDImOS aplicáveis
Utilização e gestão das <i>passwords</i>	<i>Cumprir as políticas definidas para as passwords</i>	$\alpha 4$, $\alpha 10$, $\alpha 11$, $\beta 8$, $\gamma 5$
Utilização de áreas de trabalho nos servidores	<i>Cumprir as políticas de utilização dos activos</i>	$\alpha 5$, $\beta 4$, $\gamma 3$, $\gamma 7$
Utilização de impressoras partilhadas	<i>Cumprir as políticas de utilização dos activos</i>	$\alpha 5$, $\beta 1$, $\beta 4$, $\gamma 3$, $\gamma 7$
Conhecimento das políticas de segurança	<i>Manter actualizado o documento da política de segurança</i>	$\alpha 3$, $\alpha 10$, $\beta 8$, $\gamma 5$
Participação na elaboração e/ou alteração das políticas de segurança	<i>Colaborar nas actividades a desenvolver</i>	$\alpha 10$, $\beta 8$, $\gamma 5$
Realização e gestão de <i>backups</i>	<i>Cumprir as políticas de utilização e protecção dos activos</i>	$\alpha 5$, $\alpha 10$, $\alpha 11$, $\beta 5$, $\beta 4$, $\gamma 3$, $\gamma 4$
Utilização de mecanismos de protecção	<i>Respeitar os procedimentos definidos para estes mecanismos</i>	$\alpha 10$, $\alpha 11$, $\beta 5$, $\beta 4$,
Acessos ao sistema	<i>Cumprir as políticas de controlo e gestão de acessos</i>	$\alpha 4$, $\beta 5$, $\gamma 3$

Tabela 9.8 – Aplicação dos referenciais MIDImOS na Questão 1

A aplicação dos referenciais MIDImOS aos impactos nas actividades das Pessoas, identificados relativamente à Questão 1, proporcionam um enquadramento que possibilitará a sua inclusão nos processos de validação do Modelo, relacionando-se essencialmente com a Gestão de Acessos e com a Utilização dos Activos do Sistema.

Itens relevantes na Questão 2	Impactos nas actividades das Pessoas	Referenciais do MIDImOS aplicáveis
Grau de segurança da <i>password</i>	<i>Cumprir as políticas definidas para as passwords</i>	$\alpha 5, \alpha 10, \beta 8, \gamma 5$
Segurança do Sistema Informático	<i>Cumprir as políticas de segurança implementadas</i>	$\alpha 10, \beta 8, \gamma 5$
Importância da segurança do Sistema Informático para as actividades realizadas	<i>Cumprir as políticas de segurança implementadas</i>	$\alpha 7, \alpha 8, \alpha 10, \beta 1, \beta 3, \beta 8, \gamma 4, \gamma 5$
Aspectos relevantes para a segurança do Sistema Informático	<i>Cumprir as políticas de segurança implementadas</i>	$\alpha 10, \beta 3, \beta 8, \gamma 1, \gamma 5$
Impacto de ameaças na segurança do Sistema Informático	<i>Cumprir as políticas de segurança implementadas</i>	$\alpha 2, \alpha 7, \alpha 8, \alpha 10, \beta 3, \beta 8, \gamma 1, \gamma 2, \gamma 5$

Tabela 9.9 – Aplicação dos referenciais MIDImOS na Questão 2

Relativamente aos aspectos associados à Questão 2, os impactos identificados e a relação estabelecida com os referenciais MIDImOS releva dois contextos fundamentais: Políticas de Segurança e Monitorização da Utilização do Sistema.

Itens relevantes na Questão 3	Impactos nas actividades das Pessoas	Referenciais do MIDImOS aplicáveis
Envolvimento nas mudanças dos Sistemas Informáticos	<i>Participar nas actividades de acordo com as suas competências e necessidades</i>	$\alpha 9, \alpha 10, \beta 1$
Formação na área de Informática	<i>Participar nas acções de acordo com os planos</i>	$\alpha 12, \beta 6, \gamma 6$
Frequência de utilização do Sistema Informático	<i>Cumprir as políticas de utilização dos activos</i>	$\alpha 5, \alpha 10, \beta 8, \gamma 4$
Tipo de utilização do Sistema Informático	<i>Cumprir as políticas de utilização dos activos</i>	$\alpha 5, \alpha 6, \beta 8, \beta 9, \gamma 4$
<i>Software</i> utilizado	<i>Cumprir as políticas de utilização dos activos</i>	$\alpha 5, \beta 8, \gamma 4$
Acesso aos activos do Sistema Informático e a sua utilização	<i>Cumprir as políticas de utilização dos activos</i>	$\alpha 5, \alpha 6, \beta 8, \gamma 4, \gamma 7$
Formação na utilização do Sistema Informático	<i>Participar nas acções de acordo com os planos estabelecidos</i>	$\alpha 12, \beta 6, \gamma 6,$
Documentos de apoio à utilização do Sistema Informático	<i>Respeitar as regras definidas pelo documento</i>	$\alpha 3, \alpha 6, \alpha 10, \beta 2, \gamma 5$
Facilidade de utilização do Sistema Informático	<i>Garantir que são cumpridos os requisitos dos utilizadores</i>	$\alpha 1, \alpha 12, \beta 9, \gamma 7$
Facilidade de aprendizagem do Sistema Informático	<i>Garantir que são cumpridos os requisitos dos utilizadores</i>	$\alpha 1, \alpha 12, \beta 6, \beta 9, \gamma 6$
Aspectos relevantes para a usabilidade do Sistema Informático	<i>Garantir que os novos ou a alterar respeitam estes aspectos</i>	$\alpha 1, \alpha 12, \beta 2, \beta 9$
Importância da usabilidade do Sistema Informático para as actividades realizadas	<i>Garantir que são cumpridos os requisitos dos utilizadores</i>	$\alpha 1, \alpha 6, \alpha 10, \beta 2, \beta 9$

Tabela 9.10 – Aplicação dos referenciais MIDImOS na Questão 3

No que diz respeito à Questão 3, utilização dos SI e das TIC, nomeadamente a percepção das Pessoas e os impactos nas suas actividades, a aplicação dos referenciais MIDImOS aos impactos identificados, realça genericamente os seguintes aspectos: Controlo das Alterações, Formação, Utilização dos Activos do Sistema, Gestão de Activos.

9.5.2. Definição e Aplicação de Métricas

As métricas a aplicar consideram os princípios referenciados no capítulo 6 (Métricas de Segurança), sendo derivadas essencialmente dos resultados dos questionários, da sua apreciação e também do diverso normativo aplicável.

Com esse objectivo e a título de exemplo, definem-se as seguintes métricas:

Métrica 1: Frequência de acesso ao Sistema Informático.

Métrica 2: Grau de envolvimento na elaboração/alteração das políticas de segurança.

Métrica 3: Classificação do nível de segurança da *password* (podendo ser, por exemplo quantitativo ou qualitativo).

Métrica 4: Tempos de paralisação do Sistema Informático devido a quebras de segurança.

...

Métrica x-1: Número/Horas de acções de formação frequentadas.

Métrica x: Classificação da disponibilidade do Sistema Informático.

A definição destas métricas é efectuada apelas a título exemplificativo, devendo ser definidas as métricas necessárias e apropriadas a cada caso concreto, utilizando tantas vezes quanto as necessárias os referenciais constantes do MIDImOS.

9.6 Vantagens do Modelo

Como vantagem genérica da criação do Modelo surge a maior facilidade de percepção de um problema complexo, onde a visão do conjunto é fundamental, não deixando obviamente de parte a possibilidade de uma análise a níveis de maior detalhe, enquadrados precisamente pela referida visão global.

A possibilidade de utilizar a percepção das Pessoas para suportar os processos associados ao desenvolvimento, implementação e teste dos SGSI apresenta-se como uma vantagem capaz de facilitar e simplificar as referidas actividades.

Nesta situação particular será considerada como vantagem relevante a participação das Pessoas nos aspectos associados à segurança da informação e a sua relevância nos SGSI.

Outra das vantagens reside na possibilidade de inserir o processo de definição e implementação de políticas de segurança da informação, qualquer que seja o estágio de desenvolvimento/renovação do SI.

Com esta solução é possível proceder a um desenvolvimento e implementação integrada, evitando-se a opção por SI e TIC que possam condicionar as necessidades em termos dos SGSI.

Todavia, considera-se fundamental que a implementação de um SGSI, com a definição dos seus requisitos, dos activos a proteger, dos recursos afectados, deve ser suportada por uma norma adequada à missão e objectivos de negócio, e sempre que possível ser integrada no próprio processo de planeamento, desenvolvimento, implementação e operação do SI nos aspectos considerados relevantes num processo desta natureza, contando com a participação das Pessoas de acordo com as suas competências e motivações.

Como vantagem emerge o facto de o MIDImOS ter sido definido com base numa metodologia suportada em modelos *standard*, onde a facilidade de utilização, de aplicação e de optimização, possibilita a sua adequação às necessidades de qualquer organização.

Outra das vantagens de aplicação a qualquer organização, dada a diversidade de métricas que permita, perante a especificidade da organização, o seu modelo de negócio, a sua estratégia e a sua missão, adopta o subconjunto de métricas que considera adequado para aferir a segurança de informação implementada.

O sucesso da componente Iniciação e Planeamento do MIDImOS está implicitamente ligado ao grau de comprometimento dos decisores hierárquicos da organização e à definição adequada do seu propósito, no que se refere à componente Concepção e

Desenvolvimento, salienta-se a importância da implementação e operação da política do SGSI, dos seus controlos, processos e procedimentos. Por outro lado, a componente Implementação e Avaliação, encontra-se dependente das medições realizadas aos processos, considerando como padrão os objectivos definidos e a experiência prática acumulada, já a componente Operação, Manutenção e Optimização, depende das auditorias e da revisão do SGSI por parte da gestão de topo para atingir a melhoria contínua do SGSI [Avison and Fitzgerald 2003, Grance *et al* 2003, ISO 2005a, ISO 2005b].

9.7. Conclusões

Perante os princípios explanados, pode concluir-se que o MIDImOS corresponde às necessidades organizacionais de segurança da informação.

Pode ainda concluir-se que o MIDImOS permite um maior envolvimento das Pessoas em todas as etapas de concepção do SGSI, facilitando a implementação e utilização do SGSI, garantindo um aumento do seu sucesso no contexto das actividades que desenvolvem.

Além disso, a metodologia de aplicação do MIDImOS depende do envolvimento das Pessoas e da utilização do normativo adequado a suportar o SGSI na organização, considerando a possibilidade de se proceder ao seu alinhamento com outros *standards* implementados na organização.

Neste aspecto pode concluir-se que além de ser essencial o envolvimento das Pessoas, é igualmente relevante o suporte por parte da gestão de topo, particularmente no apoio claro inequívoco à aplicação do Modelo para simplificação dos processos associados à problemática da segurança.

Os principais contributos dos questionários residem na possibilidade que proporcionaram na identificação de tópicos e ter em atenção nas actividades das Pessoas durante a utilização da Informação organizacional, dos SI que suportam os seus fluxos e das TIC que suportam esses sistemas.

Tornou-se assim possível realizar uma apreciação crítica dos resultados dos questionários em função dos temas que agruparam os referidos tópicos, considerando os contributos de cada um dos grupos dos questionários.

A análise dos contributos dos questionários em confronto com as questões de partida do trabalho foi efectuada segundo três perspectivas distintas relacionadas com as questões de partida. As perspectivas analisadas foram: Percepção das Pessoas acerca da segurança da informação; Classificação da segurança da informação numa perspectiva pessoal; Utilização dos SI e das TIC por parte das Pessoas.

Como resultado destas análises obtiveram-se, para cada uma das questões de partida, conjuntos de itens relevantes relacionados com os impactos nas actividades das Pessoas concluindo-se a utilização destes resultados pode ser importante para se actuar nos SGSI.

A validação do MIDImOS depende da sua adequação à organização em causa, das métricas apropriadas a cada caso concreto e, fundamentalmente, das Pessoas que vão realizar as medições necessárias.

Utilizando-se os itens identificados na análise dos resultados torna-se possível associar a cada um desses itens os referenciais aplicáveis, constatando-se que a utilização dos referenciais adequados a cada caso concreto permite actuar no sentido de minimizar ou mesmo eliminar todos os impactos mencionados.

Com base nos itens, impactos e referenciais relativos a cada uma das questões de partida pode proceder-se à definição e aplicação de métricas que demonstram a validade do MIDImOS para uma identificação prévia dos aspectos críticos para a organização no respeitante à segurança da informação e ao envolvimento das Pessoas.

Perante o Modelo apresentado, conclui-se da sua facilidade de utilização e aplicação a situações diversas que envolvam as Pessoas e a utilização que fazem dos recursos de SI e TIC num contexto de garantia de segurança da informação enquadrada pelas políticas de segurança definidas e pelos SGSI implementados.

Referências bibliográficas

- Avison, D. and Fitzgerald, G., *Information Systems Development: Methodologies, Techniques and Tools*, 3rd Edition, McGraw-Hill, 2003.
- Grance, T., Hash, J. and Stevens, M., *Security Considerations in the Information System Development Life Cycle*, Special Publication 800-64, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2003.

ISO, *BS ISO/IEC 17799 (BS 7799-1:2005) – Information Technology - Code of practice for information security management*, British Standard Institution, 2005.

ISO, *BS ISO/IEC 27001 (BS 7799-2:2005) – Information Technology - Security Techniques - Information Security Management Systems - Requirements*, British Standard Institution, 2005.

10

Conclusões

Considerada conjuntamente com as Pessoas um dos mais relevantes activos das organizações, a informação requer protecção adequada de modo a assegurar que se mantenha no âmbito para o qual foi criada/adquirida, emergindo uma situação que implica a necessidade de garantir que a segurança dessa informação era adequada aos objectivos organizacionais.

Neste contexto é comum a referência às Pessoas que utilizam a informação no seio da organização como o seu elo mais fraco, o que desde logo reflectia alguma insatisfação em termos dos objectivos fundamentais para os quais as organizações foram criadas.

O desafio torna-se então perceber o entendimento que as Pessoas possuem acerca da segurança da informação e como será possível a implementação e utilização de SGSI sem que as Pessoas sejam entendidas e assumidas como um entrave sério à segurança das informações pessoais e organizacionais, mesmo quando as utilizam nas suas actividades pessoais e profissionais.

10.1. Resultados

Actualmente a informação é assumida por um grande número de organizações como um importante activo, a par das Pessoas, das TIC e dos recursos financeiros, a segurança da informação, simultaneamente com a segurança dos SI que possibilitam os fluxos de informação e das TIC que suportam esses sistemas, emerge como um factor fundamental para assegurar as suas actividades.

Nesta envolvente, assume-se importante definir como podiam ser avaliados os aspectos de maior relevância no contexto e como, sem afectar a actividade das organizações, podiam esses aspectos ser optimizados de modo a suportar adequadamente as actividades organizacionais, sem colocar em causa o futuro das organizações.

Procurou-se assim estabelecer em primeiro lugar um enquadramento teórico que se considerar adequado ao trabalho a desenvolver, considerando as diversas vertentes a analisar.

De um modo genérico, os resultados obtidos permitiram reforçar a percepção inicial da importância do envolvimento das Pessoas nas actividades relacionadas com os SI e as TIC e com a sua facilidade de utilização e aprendizagem, particularmente no actual contexto de globalização que permitiu a aceção de uma Sociedade da Informação omnipresente no seu dia-a-dia, principalmente quando a informação, base crucial nesta sociedade, está sujeita a uma diversidade de ameaças, tornando obrigatória a garantia da sua segurança.

Neste sentido a utilização das diversas normas, *standards*, regulamentos, leis, políticas, que de forma directa ou indirecta a nível nacional e internacional, se relacionam com a informação e a sua segurança, como base inicial do trabalho a desenvolver consideram-se determinantes para a obtenção de uma visão mais largada acerca das diversas vertentes de evolução e desenvolvimento da problemática da segurança da informação.

Contexto no qual, a utilização das normas ISO/IEC 17799:2005 e ISO/IEC 17799:2005 [ISO 2005a, ISO 2005b] (guia de boas práticas e SGSI, respectivamente), contribuiu para assegurar que a organização é bem sucedida na implementação do SGSI e que a informação de negócio que utiliza se encontra protegida de forma adequada, permitindo suportar a fase inicial do trabalho.

O subsequente desenvolvimento do trabalho permitiu a criação de um Modelo, o MIDImOS, que suportou a continuidade das actividades e a finalização dos questionário, que por sua vez contribuíram para a validação do próprio Modelo.

A necessidade do desenvolvimento de acções de sensibilização e de formação na área da segurança da informação, assim como dos SI e das TIC que permitem a partilha dessa informação, surge claramente reforçada perante os desafios colocados actualmente pelos novos mercados impulsionados maioritariamente pelos desenvolvimentos verificados em termos das TIC.

Definir um questionário que atendendo ao normativo abordado permita aferir a perspectiva e percepção das Pessoas acerca da utilização dos SI e das TIC, como suportes essenciais da informação organizacional, considerando a pertinência da

facilidade de utilização dos referidos sistemas e da políticas e SGSI implementados, a componente da própria informação apresentou-se como essencial para o alargamento dos diversos aspectos directamente associados à problemática da segurança da informação e do envolvimento das Pessoas nesse mesmo âmbito.

A realização do questionário acerca da percepção das Pessoas relativamente à segurança da informação e dos SI e das TIC que suportam a aquisição, tratamento, armazenamento e partilha de informação, constituiu um desafio, quer pela sua dimensão e diversidade das questões colocadas, quer pela necessidade de utilizar normativos relativos à segurança da informação para propiciar o enquadramento adequado à definição dessas questões.

10.2. Contributos Organizacionais do Modelo

Actualmente, no seu dia a dia, as Pessoas e as organizações são frequentemente confrontadas com ameaças à sua segurança. Estas ameaças revestem-se de formas diversas e implicam cuidados redobrados em função da especificidade de cada evento concreto que tanto pode ameaçar a sua integridade física como a sua propriedade.

Se a segurança física e ambiental se encontram razoavelmente controladas, particularmente pelo facto de serem os aspectos sobre os quais recaem as primeiras abordagens por parte da organização à problemática da segurança, o mesmo não se poderá dizer da segurança da informação pessoal, sobre a qual as ameaças têm aumentado em diversidade e quantidade.

As preocupações com a segurança dos SI cresceram exponencialmente com os efeitos da globalização nas sociedades, comportando riscos acrescidos para as organizações que, ao apostarem nos mercados surgidos com a utilização ampla das vias de comunicação digitais, se confrontam com a necessidade de assegurar a confidencialidade e fiabilidade da informação resultante dos contactos com os seus diversos parceiros.

Com as normas associadas à problemática da segurança da informação a deixarem frequentemente de fora o envolvimento das Pessoas na maioria dos processos relacionados com os SI e as TIC que os suportam, a utilização do MIDImOS, desenvolvido com uma forte base da percepção das Pessoas acerca, dos SI, das TIC, da

sua usabilidade e também da segurança da informação pessoal e organizacional, permitirá proporcionar desde logo um forte envolvimento das Pessoas em todos os processos relacionados com estas actividades.

Entende-se que um dos principais contributos organizacionais do MIDImOS consistiu na demonstração da possibilidade de utilizar os diversos normativos como suporte essencial para congregar as Pessoas e as organizações num rumo comum, onde a importância de todos os interessados nas actividades organizacionais é indispensável, quer para atingir os objectivos delineados pelas estratégias definidas para a concretização da missão da organização, quer para responder de forma adequada e eficaz aos desafios da actual sociedade, que relewa o papel das Pessoas, seja nas organizações seja nas sociedades em geral.

10.3. Tendências de Evolução e Trabalhos Futuros

O potencial de evolução da segurança da informação num contexto de globalização dos mercados, marcadamente vincado pela emergência de novas TIC e por um aumento de exigências de rapidez e qualidade por parte dos consumidores, contribui para realçar as Pessoas como activo organizacional capaz de potenciar o desempenho da organização recorrendo às suas competências e conhecimentos.

Considera-se que o presente trabalho, centrado essencialmente nas Pessoas e no uso que fazem dos SI, das TIC e dos SGSI, pode constituir o ponto de partida para o estudo de aspectos complementares quer da problemática da segurança da informação, quer do ou dos papéis a desempenhar pelas Pessoas, um dos mais importantes activos organizacionais.

10.3.1. Tendências de Evolução da Segurança da Informação

A dificuldade em enumerar tendências de evolução é patente, no entanto considera-se que a principal tendência que actualmente se verifica em termos de segurança da informação se apresenta como uma crescente consciencialização das Pessoas acerca da segurança, pessoal e organizacional, entendendo este aspecto como omnipresente nas suas actividades, mesmo quando essa percepção não é entendida de forma similar por todas as Pessoas que partilham uma mesma informação.

As ameaças que as organizações enfrentam actualmente deixaram o âmbito local e encontram-se actualmente numa escala global, abrangendo uma diversidade de aspectos que Zúquete [2006:1] identifica como catástrofes ambientais (terramotos, inundações, tempestades, entre muitas outras situações), políticas (ataques terroristas, motins) e materiais (degradação física dos equipamentos, roubo ou adulteração dos mesmos), com qualquer delas com potencial para causar danos irreparáveis que afectarão a actividade das Pessoas e das organizações.

Um plano de segurança eficaz incorpora, segundo Greenberg [2003:29], três componentes principais. Estes elementos da segurança são: um modelo de negócio centrado na segurança (considerando três componentes: Informação, Infraestrutura e Pessoas); uma abordagem à gestão do ciclo de vida da segurança (comportando a selecção das tecnologias, a implementação, a operação e a resposta a incidentes); uma visão completa das tecnologias relacionadas com a segurança (englobando componentes físicos, de rede, de aplicações e do sistema operativo).

Esta situação realça a necessidade de um acompanhamento frequente do desenvolvimento dos modelos de negócio, das TIC, procurando em simultâneo que as Pessoas se envolvam nestas actividades onde o seu contributo pode fazer a diferença entre o sucesso e o fracasso.

A simplicidade actual no acesso aos SI, e a facilidade de obtenção de instrumentos capazes de ultrapassar as defesas da segurança organizacional surgem em diversas vertentes que podem ir desde falhas previsíveis até às actividades não autorizadas, com os consequentes impactos negativos sobre a propriedade organizacional [Zúquete 2006:4].

Perante o anteriormente referenciado e no actual contexto de globalização, têm-se constatado aumentos em termos do número de ameaças e da frequência com que as Pessoas e as organizações são afectadas, tornando imprescindível uma atenção constante sobre sua evolução e um clara e ampla percepção dos seus potenciais impactos.

Nesta envolvente, Whitman and Mattord [2004:42] apresentam um modelo que consiste em doze categorias representativas dos perigos actuais para informação organizacional e para os seus SI. As categorias especificadas são as seguintes:

1. Actos de erros ou falhas humanas (acidentes, enganos dos funcionários);
2. Comprometimento da propriedade intelectual (infrações à privacidade e ao direito de cópia);
3. Actos deliberados de espionagem (acessos não autorizados e recolha de dados);
4. Actos deliberados de extorsão de informação (utilização indevida dos recursos);
5. Actos deliberados de vandalismo ou sabotagem (destruição da informação ou dos sistemas);
6. Actos deliberados de roubo (confiscação ilegal de equipamento ou informações);
7. Ataques deliberados ao *software* (vírus, *worms*, negação de serviço);
8. Alteração da qualidade dos serviços por parte dos fornecedores (serviços de rede ou de energia);
9. Forças da natureza (incêndios, aluimentos, terremotos);
10. Erros ou falhas técnicas do *hardware* (falhas do equipamento);
11. Erros ou falhas técnicas do *software* (*bugs*, erros de código);
12. Obsolescência técnica (tecnologias antiquadas ou ultrapassadas).

Desta caracterização podem inferir-se tendências para um crescimento das categorias de perigos e das respectivas ameaças, exigindo por isso um acompanhamento adequado da sua evolução, pressupondo deste modo um aumento da relevância das Pessoas como activo organizacional e elemento fundamental nas actividades relacionadas com a segurança da informação.

10.3.2. Trabalhos Futuros

A dificuldade de delimitação dos trabalhos futuros encontra-se estreitamente relacionada com a temática da segurança da informação, com uma infinidade de contextos estudados de forma deficitária, particularmente aqueles que envolvem as Pessoas e as suas actividades no âmbito da segurança da informação.

A importância deste novo contexto é reforçada por Dinis [2005:39] quando menciona as actuais facilidades de actuar sobre os SI e as TIC que os suportam, onde não são necessárias grandes competências técnicas na actuar no que considera como uma sociedade centrada em rede, com todos a possuírem um acesso quase global,

Embora se considere a impossibilidade de definir todas as tendências futuras, considera-se que é possível definir algumas propostas de evolução de investigação a partir do presente trabalho.

Os trabalhos futuros podem então ser considerados em quatro vertentes distintas: (i) ligação do MIDImOS ao Planeamento e Gestão da Continuidade de Negócio; (ii) implementação de um SGSI no IPS tendo como base o Modelo definido; (iii) alargamento da base de abrangência do MIDImOS, para a gestão dos serviços de TIC; (iv) integração da Gestão do Risco no MIDImOS.

Constata-se que estes trabalhos futuros serão sempre alicerçados no pressuposto do envolvimento das Pessoas nas actividades relativas às linhas de investigação seguidamente explicitadas.

- ⇒ Continuidade do Negócio – A introdução da componente de continuidade de negócio pretende proporcionar a ligação a um dos principais aspectos que se apresenta crítico nas actividades organizacionais, procurando garantir a minimização dos danos causados por eventuais falhas de funcionamento dos SI e das TIC que suportam o negócio. Considera-se deste modo fundamental que esta via seja suportada por normas adequadas e devidamente testadas nesta área, nomeadamente as normas BS 25999-1:2006, *Business Continuity Management – Part 1: Code of practice*, BS 22599-2:2007, *Business Continuity Management – Part 2: Requirements*, e NIST SP800-34, *Contingency Planning Guide for Information Technology Systems*.
- ⇒ Concepção e Implementação de um SGSI – A importância para o IPS da implementação de um SGSI terá como base fundamental os resultados práticos obtidos no questionário, sendo nesta vertente, necessária a identificação dos diversos aspectos directamente relacionados com a segurança física e tecnológica, que tendo sido abordados neste trabalho não o foram com a profundidade suficiente para abranger todas as componentes tecnológicas necessárias para englobar toda a instituição.
- ⇒ Gestão dos Recursos e Serviços de TIC – O alargamento do Modelo para abranger as componentes relacionadas com a gestão dos recursos de TIC pode ser entendido como uma opção de complementaridade face aos actual contexto

de globalização económica e social, onde a Sociedade da Informação impõe claramente as suas regras, forçando de certa forma a necessidade de maiores e melhores competências na utilização dos SI e das TIC como fontes potenciais de aquisição de vantagens competitivas, onde a informação e as Pessoas assumem claramente o papel principal. Neste contexto, a utilização de normativo adequado, como por exemplo as normas BS ISO/IEC 20000-1:2005, *Information Technology - Service Management – Specification*, BS ISO/IEC 20000-2:2005, *Information Technology - Service Management - Code of practice*, e COBIT, *Control Objectives for Information and related Technology* (Version 4.0), 2005, podem contribuir em grande parte para o sucesso dessa tarefa.

⇒ Gestão do Risco – A integração da Gestão do Risco no Modelo permitirá considerar a classificação da informação, a especificação e valorização das ameaças a que essa informação poderá ser sujeita, a identificação das vulnerabilidades, de forma a proceder a uma adequada avaliação das probabilidades associadas à exploração das vulnerabilidades por parte das ameaças que poderão causar danos ou perdas à organização. Como normativo a utilizar neste contexto referenciam-se as normas BS 7799-3:2006, *Guidelines for Information Security Risk Management* e NIST SP800-30, *Risk Management Guide for Information Technology Systems*.

Assume-se que os trabalhos futuros a desenvolver terão sempre em atenção o envolvimento das Pessoas nas actividades associadas aos SI e aos SGSI, considerando a pertinência destes sistemas para a prossecução dos objectivos organizacionais.

10.4. Conclusões Finais

O trabalho desenvolvido e que se apresenta nesta forma escrita, envolveu uma diversidade de temáticas com uma extensão que tornou impossível a apreciação pormenorizada de cada uma delas.

Para atingir os objectivos identificados tornou-se necessário considerar as implicações da implementação de SGSI na utilização dos SI e consequentemente no desempenho das organizações, atendendo em especial aos efeitos da globalização e à emergência das

TIC, com relevância particular para a sua utilização no âmbito das actividades pessoais e organizacionais.

Todavia, podem realçar-se como fundamentais seis aspectos distintos mas complementares, aspectos estes com fortes interacções que impõe a sua apreciação integrada sem impedir o estudo individual de qualquer deles. Os aspectos relevados são: Sociedade da Informação; Pessoas; SI e TIC; Segurança da Informação; Políticas e SGSI; MIDImOS.

A actual Sociedade da Informação estabeleceu um factor de instabilidade, desafiando os Estados, as organizações e as Pessoas a encararem novas perspetivas de actuação nas suas vertentes de actuação, exigindo novas e melhores competências para responder adequada e prontamente às exigências identificadas.

Objectiva-se então que seja incrementado o papel das Pessoas nos aspectos organizacionais, procurando-se que essa participação se faça de forma clara e abrangente, de modo a otimizar o seu desempenho no interior das organizações e o consequente incremento das actividades organizacionais, permitindo que estas respondam adequadamente aos desafios dos mercados e da Sociedade da Informação e do Conhecimento com que actualmente se confrontam.

A actual difusão dos SI e das TIC que os suportam, tem conduzido a dependências crescentes por parte das organizações, não apenas porque a sua utilização pode simplificar e acelerar as actividades do dia-a-dia das organizações, mas também se adequadamente seleccionadas, integradas na estratégia organizacional e aplicadas nas actividades de negócio, podem constituir um factor competitivo fundamental para otimizar o desempenho das organizações e potenciar a utilização dos outros activos organizacionais.

Neste contexto evolutivo, onde os SI, as TIC e as Pessoas, assumem crescente relevância, é necessário assegurar que a informação que utilizam e partilham com os parceiros de negócio é adequadamente protegida. Esta protecção não é competência exclusiva das políticas de segurança da informação mas sim uma actividade e responsabilidade permanente das Pessoas que utilizam os SI e a informação que os mesmos suportam.

Mas é também uma competência e um compromisso da gestão de topo, cujo comprometimento se deve manter e até reforçar para além do mero processo de concepção, desenvolvimento e implementação das políticas de segurança e dos SGSI, mantendo-se ao longo do tempo e acompanhando as actividades relativas a alterações que se venham a revelar imprescindíveis para a continuidade das actividades de negócio da organização.

Os SGSI desempenham aqui um papel crucial ao possibilitarem processos e controlos apropriados à concepção, implementação, utilização e revisão das políticas de segurança, procurando o cumprimento da legislação e vigor, do normativo aplicado e das estratégias organizacionais, envolvendo forçosamente as Pessoas nas diversas actividades a realizar, incentivando os seus contributos para a segurança da informação e para as necessárias mudanças nos SI e nas TIC.

Os contributos organizacionais derivados do MIDImOS residem essencialmente na facilitação das actividades das Pessoas e da potencialização da sua maior envolvimento nas actividades de implementação, utilização e substituição de SI e de TIC, considerando os contextos da necessária segurança da informação organizacional e pessoal, e ainda a possibilidade de aplicar SI e TIC mais fáceis de aprender e utilizar, potenciando por isso mesmo o seu desempenho nas organizações.

Os trabalhos futuros consideram algumas das diversas alternativas de desenvolvimento deste trabalho, tendo sempre presente que qualquer eixo de evolução do trabalho tem como pressuposto a participação das Pessoas na análise das diversas vertentes apresentadas nas opções de caminhos futuros deste estudo.

Neste enquadramento onde a concepção e implementação de um SGSI emerge como um dos factores essenciais ao desenvolvimento organizacional alicerçado nas competências e no desempenho das Pessoas, a evolução do presente estudo incorporará desde o planeamento e continuidade do negócio até à gestão do risco, passando pela gestão dos serviços de TIC e pela continuação do projecto no IPS, cumprindo neste caso específico as etapas seguintes, ou seja, concepção e implementação do SGSI, a sua utilização, manutenção e optimização recorrendo aos dados obtidos através do Estudo de Caso e ao MIDImOS como padrão de orientação para as diversas actividades associadas.

Referências bibliográficas

- Dinis, J.A., *Guerra de Informação – Perspectivas de Segurança e Competitividade*, Edições Sílabo, 2005.
- Greenberg, E., *Mission-Critical Planner: Creating Customized Strategies*, Wiley Publishing, Inc, 2003.
- ISO, *BS ISO/IEC 17799 (BS 7799-1:2005) – Information Technology - Code of practice for information security management*, British Standard Institution, 2005.
- ISO, *BS ISO/IEC 27001 (BS 7799-2:2005) – Information Technology - Security Techniques - Information Security Management Systems - Requirements*, British Standard Institution, 2005.
- Whitman, M.E. and Mattord, H.J., *Management of Information Security*, Thomson Course Technology, 2004.
- Zúquete, A., *Segurança em Redes Informáticas*, FCA, 2006.

Bibliografia

--- A ---

- Almeida, J.M.G., “Controlar o Futuro”, in José Dias Coelho (Coordenador), *Sociedade da Informação – O percurso Português*, Edições Sílabo, 2007, p.189-199.
- Alter, S., *Information Systems: A Management Perspective*, 3rd Edition, Addison-Wesley Publishing Company, 1998.
- Amaral, L.M., “A Sociedade da Informação”, in José Dias Coelho (Coordenador), *Sociedade da Informação – O percurso Português*, Edições Sílabo, 2007, p.85-92.
- Andrade, J. e Ferreira, L., *25 Anos a Construir Futuro*, Instituto Politécnico de Setúbal, Abril de 2004.
- Antunes, I., “A Problemática da Avaliação e da Maturidade nos Processos de Desenvolvimento de Aplicações Informáticas”, *Informação & Informática*, 26, 2001, p.45-52.
- Anunciação, P. e Zorrinho, C., *Urbanismo Organizacional – Como gerir o choque tecnológico nas empresas*, Edições Sílabo, 2006.
- APDSI, *Glossário da Sociedade da Informação*, José Palma Fernandes (Coordenador), Associação para a Promoção e Desenvolvimento da Sociedade da Informação (APDSI), Outubro de 2005.
- Assembleia da República, “Lei da Criminalidade Informática”, Lei n.º109/91, de 17 de Agosto, Diário da República nº188, I Série-A.
- Assembleia da República, “Lei da Protecção Jurídica de Programas de Computador”, Lei n.º 252/94, de 20 de Outubro, Diário da República nº243, I Série-A.
- Assembleia da República, “Lei da Protecção de Dados Pessoais”, Lei n.º67/98, de 26 de Outubro, Diário da República nº247, I Série-A.
- Assembleia da República, “Lei das Comunicações Electrónicas”, Lei n.º5/2004, de 10 de Fevereiro, Diário da República nº34, I Série-A.

Assembleia da República, “Lei da Protecção da Privacidade no Sector das Comunicações Electrónicas”, Lei n.º41/2004, de 18 de Agosto, Diário da República n.º194, I Série-A.

Avison, D. and Fitzgerald, G., *Information Systems Development: Methodologies, Techniques and Tools*, 3rd Edition, McGraw-Hill, 2003.

--- B ---

Barman, S., *Writing Information Security Policies*, New Riders Publishing, 2002.

Berti, J. and Rogers, M., “Social Engineering: The Forgotten Risk”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 3, 4th Edition, Auerbach Publications, 2002, p.51-63.

Bevan, N., Kirakowski, J. and Maissel, J., “What is usability?”, Proceedings of the 4th International Conference on HCI, September 1991.

Bias, R.G. and Mayhew, D.J., *Cost-Justifying Usability*, Morgan Kaufmann Publishers, 1994.

Bishop, M., *Computer Security: Art and Science*, Addison-Wesley Professional, 2002.

Bosworth, S. and Jacobson, R., “Brief History and Mission of Information System Security”, in S. Bosworth and M.E. Kabay, (Editors), *Computer Security Handbook*, 4th Edition, John Wiley & Sons, 2002.

Bowen, P., Hash, J. and Wilson, M., *Information Security Handbook: A Guide for Managers*, Special Publication 800-100, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2006.

BS, *BS ISO/IEC 20000-1 – Information Technology - Service Management – Specification*, British Standard Institution, 2005.

BS, *BS ISO/IEC 20000-2 – Information Technology - Service Management - Code of practice*, British Standard Institution, 2005.

BS, *BS 7799-3 – Information - Management Systems - Guidelines for Information Security Risk Management*, British Standard Institution, 2006.

BSI, *IT Baseline Protection Manual*, Bundesamt für Sicherheit in der Informationstechnik (BSI, Federal Office for Information Security), 2004.

--- C ---

Caldeira, M. e Romão, M., “Estratégias de Investigação em Sistemas de Informação Organizacionais – A utilização de métodos qualitativos”, *Estudos de Gestão – Portuguese Journal of Management Studies*, 3 (1), 2002, p.77-97.

Caldeira, M. e Romão, M., “Porque falham os sistemas e tecnologias de informação nas PMEs Portuguesas”, Actas (formato digital) da 3ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.

Carneiro, A., *Introdução à Segurança dos Sistemas de Informação*, FCA, 2002.

Carvalho, J.Á. e Amaral, L., “Matriz de Actividades: Um Enquadramento Conceptual para as Actividades de Planeamento e Desenvolvimento de Sistemas de Informação”, *Revista da Associação Portuguesa de Sistemas de Informação*, 1 (1993), p.37-48.

Castells, M., *A Galáxia Internet: Reflexões sobre Internet, Negócios e Sociedade*, Fundação Calouste Gulbenkian, 2004.

Cerveira, A.G., “Informática e Mecanografia”, *Associação Internacional de Estudos sobre Mecanografia*, IV Encontro Internacional de Mecanografia e Informática, Outubro de 1967, p.45-50.

Chew, E., Clay, A., Hash, J., Bartol, N. and Brown, A., *Guide for Developing Performance Metrics for Information Security*, Special Publication 800-80 (Initial Public Draft), National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2006.

Choo, C.W., *Gestão da Informação para a Organização Inteligente*, Editorial Caminho, 2003.

Ciborra, C. and Andreu, R., “Organizational Learning and Core Capabilities Development: The Role of IT”, in Robert D. Galliers and Walter R. J. Baets (Organization), *Information Technology and Organizational Transformation:*

Innovation for the 21st Century Organization, London, John Wiley & Sons, 1998, p.87-106.

CISP, *Cardholder Information Security Program (CISP)*, Visa U.S.A. Inc., 2004.

COBIT, *Control Objectives for Information and related Technology (Version 4.0)*, IT Governance Institute, 2005.

Coelho, J., “Arquitectura da Empresa Centrada nos Processos: O Factor determinante para o Alinhamento Estratégico dos SI”, in Luís Amaral, Rodrigo Magalhães, Carlos Campos Morais, António Serrano e Carlos Zorrinho (Editores), *Sistemas de Informação Organizacionais*, Edições Sílabo, 2005, p.141-197.

Comissão Nacional de Protecção de Dados, “Princípios sobre a privacidade no local de trabalho”, 29 de Outubro de 2002, <http://www.cnpd.pt/bin/orientacoes/principiostrabalho.htm> (10-05-2005).

Comissão Nacional de Protecção de Dados, “Princípios sobre a utilização de dados biométricos”, 26 de Fevereiro de 2004, <http://www.cnpd.pt/bin/orientacoes/principiosbiometricos.htm> (10-05-2005).

Comissão Nacional de Protecção de Dados, “Princípios sobre o tratamento de dados por videovigilância”, 19 de Abril de 2004, <http://www.cnpd.pt/bin/orientacoes/principiosvideo.htm> (10-05-2005).

Correia, E., *Novas Tecnologias – Presente e Futuro*, volume 2, Edições Sílabo, 2006.

Cunha, P.R., Figueiredo, A.D., “Information Systems Planning for Emerging Challenges”, in Luís Valadares Tavares e Manuel João Pereira (Organizadores), *Nova Economia e Tecnologias de Informação: Desafios para Portugal*, Universidade Católica Editora, 2000, p.22-29.

--- D ---

Daly-Jones, O., Bevan, N. and Thomas, C., “Handbook of User-Centred Design – INUSE 6.2”, Version 1.2, Serco Usability Services – National Physical Laboratory, 12 February 1999, <http://www.ejeisa.com/nectar/inuse/6.2/index.htm> (15-11-2002).

Daniels, C., *Estratégias Empresariais e Tecnologias de Informação*, Biblioteca de Economia e Gestão – Editorial Caminho, 1997.

- Dark, M.J., “Security Education, Training, and Awareness from a Human Performance Technology Point of View”, in Michael E. Whitman and Herbert J. Mattord (Editors), *Readings and Cases in The Management Information Security*, Thomson Course Technology, 2006, p.86-104.
- Davis, F.D., “Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology”, *MIS Quarterly*, September 1989, p.319-339.
- Dicionário Houaiss da Língua Portuguesa, Tomo III, Instituto António Houaiss, Temas e Debates, 2003.
- Dicionário da Língua Portuguesa, Porto Editora, 2006.
- Dinis, J.A., *Guerra de Informação – Perspectivas de Segurança e Competitividade*, Edições Sílabo, 2005.
- Directiva 91/250/CEE do Conselho, 14 de Maio de 1991, “Protecção jurídica dos programas de computador”, Jornal Oficial das Comunidades Europeias n.º L 122 de 17 de Maio de 1991.
- Directiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de Outubro de 1995, “Protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados”, Jornal Oficial das Comunidades Europeias n.º L 281 de 23 de Novembro de 1995.
- Directiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de Julho de 2002, “Privacidade e comunicações electrónicas”, Jornal Oficial das Comunidades Europeias n.º L 201/37 de 31 de Julho de 2002.
- Drucker, P., “The Coming of the New Organization”, *Harvard Business Review*, Jan.-Feb. 1988, p.45-53.
- Drucker, P., *Gerindo para o Futuro*, Difusão Cultural, 1993.
- Drucker, P., *Peter Drucker sobre a Profissão de Gestão*, Publicações Dom Quixote, 1999.
- Drucker, P., *Desafios da Gestão para o Século XXI*, Editora Civilização Livraria, 2000.
- Dumas, J.S. and Redish, J.C., *A Practical Guide to Usability Testing*, Intellect, 1999.

--- E ---

- Earl, M., “Todas as empresas são empresas de informação”, *O Domínio da Informação*, Diário Económico, 2000, p.12-15.
- Earl, M. and Feeny, D., “How To Be a CEO for the Information Age”, *Sloan Management Review*, Winter 2000, p.11-23.
- Edwards, C., Ward, J. and Bytheway, A., *The Essence of Information Systems*, 2nd Edition, Prentice Hall, 1995.
- ENSI, *Carta de Segurança da Informação (Versão 1.0)*, Estrutura Nacional de Segurança da Informação (ENSI), Unidade de Missão Inovação e Conhecimento (UMIC), Fevereiro de 2005.
- ENSI, *Política Nacional de Segurança da Informação (Versão 1.0)*, Estrutura Nacional de Segurança da Informação (ENSI), Unidade de Missão Inovação e Conhecimento (UMIC), Fevereiro de 2005.

--- F ---

- Falkenberg, E., Hesse, W., Lindgreen, P., Nilssen B., Oei, J., Rolland, C., Stamper, R., Van Assche, F., Verrijn-Stuart, A. and Voss, K., *FRISCO: A Framework of Information Systems Concepts*, IFIP WG 8.1 Task Group FRISCO, 1998.
- Faria, L. e Amaral, L., “Planeamento da Contingência e Recuperação”, *Revista da Associação Portuguesa de Sistemas de Informação*, 8, 1998, p.43-51.
- Fenton, J.H. and Wolfe, J.M., “Organizing for Success: Some Human Resources Issues in Information Security”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 4, 4th Edition, Auerbach Publications, 2003, p.313-324.
- Fernandes, J.P., Correia, M. e Antunes, M., “A Terminologia e a Sociedade da Informação”, in José Dias Coelho (Coordenador), *Sociedade da Informação – O percurso Português*, Edições Sílabo, 2007, p.457-472.

Ferreira, J.M.C., “Teoria Geral dos Sistemas e Abordagem Sociotécnica”, in J.M. Carvalho Ferreira, José Neves e António Caetano (Editores), *Manual de Psicossociologia das Organizações*, McGrawHill, 2001.

Ferreira, J.M.C., Neves, J. e Caetano, A., *Manual de Psicossociologia das Organizações*, McGrawHill, 2001.

FISMA, *Federal Information Security Management Act*, Senate and House of Representatives of the United States of America, 2002.

Fraser, B. (Editor), *RFC 2196 The Site Security Handbook*, Software Engineering Institute - Carnegie Mellon University, 1997.

--- G ---

GAISP, *Generally Accepted Information Security Principles (Version 3.0)*, Information Systems Security Association (ISSA), 2003.

Garcia, C., “A Notável Intangibilidade das Organizações: O Capital Intelectual e os Sistemas de Informação”, in Luís Amaral, Rodrigo Magalhães, Carlos Campos Morais, António Serrano e Carlos Zorrinho (Editores), *Sistemas de Informação Organizacionais*, Edições Sílabo, 2005, p.199-222.

Giddens, A., *O mundo na era da globalização*, Editorial Presença, 2000.

Grance, T., Hash, J. and Stevens, M., *Security Considerations in the Information System Development Life Cycle*, Special Publication 800-64, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2003.

Grance, T., Kent, K. and Kim, B., *Computer Security Incident Handling Guide*, Special Publication 800-61, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2004.

Greenberg, E., *Mission-Critical Planner: Creating Customized Strategies*, Wiley Publishing, Inc, 2003.

--- H ---

- Haag, S., *Cummings, M. and Dawkins, J., Management Information Systems for the Information Age*, Irwin/McGraw-Hill, 1998.
- Hansche, S.D., “Making Security Awareness Happen”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 3, 4th Edition, Auerbach Publications, 2002, p.317-335.
- Hare, C., “Policy Development”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 3, 4th Edition, Auerbach Publications, 2002, p.353-383.
- Hash, J., Bowen, P., Johnson, A., Smith, C.D. and Steinberg, D.I., *An Introductory Resource Guide for Implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule*, Special Publication 800-66, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2005.
- Henning, R. (editor), *Workshop on Information Security Scoring and Ranking – Information System Security Attribute Quantification or Ordering* (Commonly but Improperly Known as “Security Metrics”), Applied Computer Security Associates, 2001.
- Henry, K., “Risk Management and Analysis”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 3, 4th Edition, Auerbach Publications, 2002, p.407-418.
- Henry, K., “The Human Side of Information Security”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 4, 4th Edition, Auerbach Publications, 2003, p.239-261.
- Herrmann, D.S., *A Practical Guide to Security Engineering and Information Assurance*, CRC Press, 2002.
- Herrmann, D.S., *Using the Common Criteria for IT Security Evaluation*, Auerbach Publications, 2003.

Herold, R., “Information Protection: Organization, Roles, and Separation of Duties”, in H.F. Tipton and M. Krause, (Editors), *Information Security Management Handbook*, volume 4, 4th Edition, Auerbach Publications, 2003, p.415-439.

HIPAA, *Health Insurance Portability and Accountability Act*, Public Law 104-191, Senate and House of Representatives of the United States of America, 1996.

Hoffer, J., George, J. and Valacich, J., *Modern Systems Analysis & Design*, 3rd Edition, Addison-Wesley Longman, 2001.

--- I ---

IEEE, *Standard Glossary of Software Engineering Terminology*, STD610.12-1990, September 28, 1990.

ISF, *The Standard of Good Practice for Information Security (Version 4.1)*, Information Security Forum (ISF), 2005.

ISO, *ISO/IEC 21827 – Information Technology - Systems Security Engineering - Capability Maturity Model (SSE-CMM)*, International Standard Organization, 2002.

ISO, *ISO/IEC FDIS 13335-1 – Information technology - Guidelines for the management of IT security - Concepts and models for information and communications technology security*, International Standard Organization, 2004.

ISO, *BS ISO/IEC 17799 (BS 7799-1:2005) – Information Technology - Code of practice for information security management*, British Standard Institution, 2005.

ISO, *BS ISO/IEC 27001 (BS 7799-2:2005) – Information Technology - Security Techniques - Information Security Management Systems - Requirements*, British Standard Institution, 2005.

ISSAF, *Information Systems Security Assessment Framework (draft 0.2)*, Open Information Systems Security Group, 2005.

ITIL, *Information Technology Infrastructure Library (Version 2.0)*, Office of Government Commerce of United Kingdom Government, 2001.

--- K ---

- Kabay, M.E., “Developing Security Policies”, in S. Bosworth and M.E. Kabay, (Editors), *Computer Security Handbook*, 4th Edition, John Wiley & Sons, 2002.
- Kajava, J. and Savola, R., “Towards Better Information Security Management by Understanding Security Metrics and Measuring Processes”, VTT Technical Research Centre of Finland, 2005.
- Katzke, S., “Security Metrics”, National Security Agency, 2001.
- King, C.M., Dalton, C.E. and Osmanoglu, T.E., *Security Architecture: Design, Deployment & Operations*, Osborne/McGraw-Hill, 2001.
- Kirakowski, J., “The use of Questionnaire methods for usability assessment”, SUMI background reading, <http://www.ucc.ie/hfrg/questionnaires/sumi/sumipapp.html> (25-10-2002).
- Kovács, I., “Trabalho, Qualificações e Aprendizagem ao longo da vida: Ilusões e problemas da sociedade de informação”, in VII Encontro Nacional da APSIOT, *Formação, Trabalho e Tecnologia: Para uma Nova Cultura Organizacional*, Celta Editora, 1998, p.69-84.

--- L ---

- Laudon, K. and Laudon, J., *Management Information Systems: Organization and Technology in the Networked Enterprise*, 6th Edition, Prentice-Hall, 2000.
- Llufríu, M., “Impacte das Tecnologias de Informação e Comunicação na Sociedade do Conhecimento”, in Luís Amaral, Rodrigo Magalhães, Carlos Campos Morais, António Serrano e Carlos Zorrinho (Editores), *Sistemas de Informação Organizacionais*, Edições Sílabo, 2005, p.95-112.
- Lindley, R.M., “Economias Baseadas no Conhecimento”, in Maria João Rodrigues (Coordenadora), *Para Uma Europa da Inovação e do Conhecimento*, Celta Editora, 2000, p.33-78.
- Lopes, F.C. e Amaral, L.A., “Actividades de Intervenção de Sistemas de Informação”, Actas (formato digital) da 1ª Conferência da Associação Portuguesa de Sistemas de

Informação (APSI), organizada pela Universidade do Minho, Guimarães, 25-27 de Outubro de 2000.

Lopes, F. C., Morais, M. P. e Carvalho, A. J., *Desenvolvimento de Sistemas de Informação*, FCA, 2005.

Lourenço, R.T. e O'Neill, H., “As Tecnologias de Informação e Comunicação na Gestão Empresarial e o papel dos Recursos Humanos na sua Potenciação”, Actas (formato digital) da 3ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.

Luz, N., “Impacto da Internet sobre a Estratégia de Internacionalização das Empresas”, in Luís Valadares Tavares e Manuel João Pereira (Organizadores), *Nova Economia e Tecnologias de Informação: Desafios para Portugal*, Universidade Católica Editora, 2000, p.378-397.

--- M ---

Macedo, P., Zacarias, M.S. e Tribolet, J., “Técnicas e Métodos de Investigação em Engenharia Organizacional: Projecto de Investigação em Modelação de Processos de Produção”, Actas (formato digital) da 6ª Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade do Minho e pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança, Bragança, 26-28 de Outubro de 2005.

Maguire, M.C., “User-Centred Requirements Handbook”, version 3.2, HUSAT Research Institute - Telematics Applications Programme RESPECT project (TE 2010), June 29, 1998, <http://www.ejeisa.com/nectar/respect/5.3/index.htm> (15-11-2002).

Mamede, H.S., *Segurança Informática nas Organizações*, FCA, 2006.

Marcelino, H., “Potencialidades e limites das Tecnologias de Informação” in *Dossier: Gestão da Informação, Pequena e Média Empresa*, 12, (1994), IAPMEI, p.53-61.

Martin, E.W., Brown, C.V., DeHayes, D.W., Hoffer, J.A. and Perkins, W.C., *Managing Information Technology*, 4th Edition, Prentice Hall, 2002.

- Martins, M.E.G. e Cerveira, A.G., *Introdução às Probabilidades e à Estatística*, 1ª Edição-5ª Impressão, Universidade Aberta, Outubro de 2006.
- Maslow, A., *Motivation and Personality*, Harper and Row, 1954.
- Michaelis: *Moderno Dicionário da Língua Portuguesa*, Companhia Melhoramentos, 1998.
- Misiolek, N., Zakaria, N. and Zhang, P., “Trust in Organizational Acceptance of Information Technology: A Conceptual Model and Preliminary Evidence”, *Proceedings of the Decision Sciences Institute 33rd Annual Meeting*, November 2002.
- Myers, M., “Qualitative Research in Information Systems”, *MISQ Discovery*, updated version, April 22, 2003, <http://www.qual.auckland.ac.nz> (16-05-2003).

--- N ---

- National Institute of Standards and Technology (NIST), *An Introduction to Computer Security: The NIST Handbook*, Technology Administration - U.S. Department of Commerce, Special Publication 800-12, 1998.
- Neves, J., “Personalidade, Percepção e Aprendizagem”, in J.M. Carvalho Ferreira, José Neves e António Caetano (Editores), *Manual de Psicossociologia das Organizações*, McGrawHill, 2001.
- Nielsen, J., *Usability Engineering*, Morgan Kaufmann – Academic Press, 1993.
- Nielsen, J., *Designing Web Usability*. New Riders Publishing, Indianapolis, USA, 2000.

--- O ---

- OECD, *Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security*, Organisation for Economic Co-operation and Development, 2002.
- Oliveira, J. e Amaral, L., “O Papel da Qualidade da Informação nos Sistemas de Informação”, in Luís Valadares Tavares e Manuel João Pereira (Organizadores), *Nova Economia e Tecnologias de Informação: Desafios para Portugal*, Universidade Católica Editora, 2000, p.168-184.

--- P ---

- Parker, D., “Toward a new Framework for Information Security”, in S. Bosworth and M.E. Kabay, (Editors), *Computer Security Handbook*, 4th Edition, John Wiley & Sons, 2002.
- Parkinson, D. (Editor), *Oxford Business English Dictionary*, Oxford University Press, 2005.
- Payne, S., “A Guide to Security Metrics”, SANS Institute, Inc., June 19, 2006.
- Peltier, T.R., *Information Security Risk Analysis*, Auerbach Publications, 2001.
- Peltier, T.R., *Information Security Policies, Procedures, and Standards*, CRC Press, 2002.
- Pfleeger, C.P. and Pfleeger S.L., *Security in Computing*, 3rd edition, Prentice Hall, 2003.
- Pinto, M.P., Lopes, F.C. e Morais, M.P., “Integração da Medição do Capital nos Sistemas de Gestão do Conhecimento: Uma Proposta de Modelo”, Actas (formato digital) da 6^a Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade do Minho e pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança, Bragança, 26-28 de Outubro de 2005.
- PIPEDA, *Personal Information Protection and Electronic Documents Act*, House of Commons of Canada, 2000.
- Pipkin, D.L., “Linking Business Objectives and Security Directions”, in Michael E. Whitman and Herbert J. Mattord (Editors), *Readings and Cases in The Management Information Security*, Thomson Course Technology, 2006, p.8-16.
- Plano Tecnológico, Presidência do Conselho de Ministros, *Resolução do Conselho de Ministros n.º190/2005*, <http://www.portugal.gov.pt/Portal> (10-02-2006).

--- R ---

- Reponen, T., “The Role of Learning in Information Systems Planning and Implementation”, in R.D. Galliers and R.J. Baets (Editors), *Information Technology*

- and Organizational Transformation: Innovation for the 21st Century Organization*, John Wiley & Sons, 1998, p.133-149.
- Reis, C., *Planeamento Estratégico de Sistemas de Informação*, Editorial Presença, 1993.
- Reis, L., *Planeamento de Sistemas de Informação e da Contingência e da Recuperação*, Tese de Doutoramento, Universidade do Minho, 2000.
- Reis, L., “Manual Electrónico de Apoio ao Desenvolvimento de Planos de Contingência e Recuperação em Sistemas de Informação para PME”, in Armando Pires (Organizador), *Projectos de Investigação IPS*, Instituto Politécnico de Setúbal, 2001, p.89-101.
- Reis, L. e Amaral, L., “Gestão de Riscos num contexto de Planeamento da Contingência e Recuperação”, Actas (formato digital) da 3^a Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade de Coimbra, Coimbra, 20-22 de Novembro de 2002.
- Rivas, F., *Estruturas Organizativas e Informação na Empresa*, Editorial Domingos Barreira, 1989.
- Rodrigues, L.S., *Arquitecturas dos Sistemas de Informação*, FCA, 2002.
- Ross, R., Katzke, S., Johnson, A., Swanson, M., Stoneburner, G., Rogers, G. and Lee, A., *Recommended Security Controls for Federal Information Systems*, Special Publication 800-53, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2005.
- Ross, S., “Computer Security: A practical definition”, 1999, <http://www.albion.com/security> (31-10-2003).
- Rudd, C., *An Introductory Overview of ITIL*, IT Service Management Forum (itSMF), 2004.

--- S ---

- Santana, S. e Dias, A., “Condicionantes da introdução de TIC em instituições prestadoras de cuidados”, Actas (formato digital) da 6^a Conferência da Associação Portuguesa de Sistemas de Informação (APSI), organizada pela Universidade do

- Minho e pela Escola Superior de Tecnologia e Gestão do Instituto Politécnico de Bragança, Bragança, 26-28 de Outubro de 2005.
- Santos, M.Y. e Ramos, I., *Business Intelligence – Tecnologias da Informação na Gestão de Conhecimento*, FCA, 2006.
- Serra, H., “Tecnologias da Informação, Emprego e Organização do Trabalho: A Sociedade da Informação como problemática teórica”, in VII Encontro Nacional da APSIOT, *Formação, Trabalho e Tecnologia: Para uma Nova Cultura Organizacional*, Celta Editora, 1998, p.39-50.
- Serrano, A., *Sistemas de Informação de Potencial Estratégico – Modelo Referencial para Exploração em PME*, Tese de Doutoramento, Universidade de Évora, 1997.
- Serrano, A. e Caldeira, M., “Gestão de Investimentos em Sistemas e Tecnologias de Informação – uma revisão crítica”, *Revista da Associação Portuguesa de Sistemas de Informação*, 15, 2001, p.99-107.
- Serrano, A., Caldeira, M. e Guerreiro, A., *Gestão de Sistemas e Tecnologias de Informação*, FCA, 2004.
- Serrano, A. e Fialho, C., *Gestão do Conhecimento – O novo paradigma das organizações*, FCA, 2003.
- Silberschatz, A., Galvin, P. and Gagne, G., *Operating Systems Concepts*, 6th edition, John Wiley & Sons, 2003.
- Smith, C. and Dinn, A., “User Centered Design: The Key to a ‘User-Friendly’ Information Society”, *European Journal of Engineering for Information Society Applications*, 2 (1) September, 1999.
- Soete, L., “A Economia Baseada no Conhecimento num Mundo Globalizado: Desafios e Potencial”, in Maria João Rodrigues (Coordenadora), *Para Uma Europa da Inovação e do Conhecimento*, Celta Editora, 2000, p.3-31.
- SOX, *Sarbanes-Oxley Act*, Senate and House of Representatives of the United States of America, 2002.
- Stake, R.E., *The Art of Case Study Research*, Sage Publications, 1995.

- Stoddard, M., Bodeau, D., Carlson, R., Glantz, C., Haimes, Y., Lian, C., Santos, J. and Shaw, J., “Process Control System Security Metrics – State of Practice”, Research Report, 1, Institute for Information Infrastructure Protection (I3P), Dartmouth College, August 2005.
- Stoneburner, G., *Underlying Technical Models for Information Technology Security*, Special Publication 800-33, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2001.
- Stoneburner, G., Goguen, A. and Feringa, A., *Risk Management Guide for Information Technology Systems*, Special Publication 800-30, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2001.
- Stoneburner, G., Hayden, C. and Feringa, A., *Engineering Principles for Information Technology Security (A Baseline for Achieving Security)*, Special Publication 800-27, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2001.
- Swanson, M., *Guide for Developing Security Plans for Information Technology Systems*, Special Publication 800-18, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 1998.
- Swanson, M., *Security Self-Assessment Guide for Information Technology Systems*, Special Publication 800-26, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2001.
- Swanson, M., Bartol, N., Sabato, J., Hash, J. and Graffo, L., *Security Metrics Guide for Information Technology Systems*, Special Publication 800-55, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2003.
- Swanson, M. and Guttman, B., *Generally Accepted Principles and Practices for Securing Information Technology Systems*, Special Publication 800-14, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 1996.

Swanson, M., Wohl, A., Pope, L., Grance, T., Hash, J. and Thomas, R., *Contingency Planning Guide for Information Technology Systems*, Special Publication 800-34, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 2002.

--- T ---

Tavares, L.V., Pereira, M.J., “The Value of an Information Systems”, in Luís Valadares Tavares e Manuel João Pereira (Organizadores), *Nova Economia e Tecnologias de Informação: Desafios para Portugal*, Universidade Católica Editora, 2000, p.4-21.

Toffler, A., *A Terceira Vaga*, Edição Livros do Brasil, 1984.

Tudor, J.K., *Information Security Architecture: An Integrated Approach to Security in the Organization*, Auerbach Publications, 2001.

--- U ---

Ulrich, D., “Intellectual Capital = Competence x Commitment”, *Sloan Management Review*, Winter, 1998, p.15-26.

UMIC, Unidade de Missão Inovação e Conhecimento, Presidência do Conselho de Ministros, *Resolução do Conselho de Ministros nº135/2002*, <http://www.umic.gov.pt> (22-01-2004).

UMIC, Unidade de Missão Inovação e Conhecimento, Presidência do Conselho de Ministros, “Plano de Acção para a Sociedade da Informação”, 2003.

UMIC, Unidade de Missão Inovação e Conhecimento, Presidência do Conselho de Ministros, 2003, <http://www.e-u.pt> (22-01-2004).

--- V ---

Veiga, A., *Legislação de Direito da Informática*, Coimbra Editora, 2004.

Veiga, P., “Prefácio”, in Alberto Carneiro, *Introdução à Segurança dos Sistemas de Informação*, FCA, 2002.

--- W ---

- Ward, J., *Principles of Information Systems Management*, Routedledge, 1995.
- Weiß, S., Weissmann, O., and Dressler, F., “A Comprehensive and Comparative Metric for Information Security”, IFIP International Conference on Telecommunication Systems, Modeling and Analysis 2005 (ICTSM2005), Dallas, TX, USA, November, 18, 2005.
- Whitman, M.E. and Mattord, H.J., *Management of Information Security*, Thomson Course Technology, 2004.
- Whitman, M.E. and Mattord, H.J., *Principles of Information Security*, 2nd Edition, Thomson Course Technology, 2005.
- Whitten, A. and Tygar, J.D., “Usability of Security: A Case Study”, 18 December 1998.
- Wilson, M. (ed.), Zafra, D., Pitcher, S., Tressler, J. and Ippolito, J., “Information Technology Security Training Requirements: A Role -and Performance- Based Model”, Special Publication 800-16, National Institute of Standards and Technology (NIST), Technology Administration - U.S. Department of Commerce, 1998.
- World Summit on the Information Society, “Declaration of Principles”, WSIS-03/Geneva/Doc/4-e, 12 December, 2003.
- World Summit on the Information Society, “Plan of Action”, WSIS-03/Geneva/Doc/5-e, 12 December, 2003.

--- Y ---

- Yin, R. K., *Case Study Research: Design and Methods*, 2nd edition, Applied Social Research Methods Series. Thousand Oaks: SAGE Publications, 1994.

--- Z ---

- Zorrinho, C., *Gestão da Informação*, Editorial Presença, 1991.
- Zorrinho, C., “O Mundo Virtual”, *Cadernos de Gestão de Sistemas e Tecnologias da Informação Henrique Marcelino*, Instituto de Informática, 1999, p.27-35.

Zorrinho, C., *Ordem, Caos e Utopia – Contributos para a História do Século XXI*, Editorial Presença, 2001.

Zúquete, A., *Segurança em Redes Informáticas*, FCA, 2006.

Zwass, V., *Foundations of Information Systems*, Irwin/McGraw-Hill, 1998.

Índice Remissivo

A

Abordagem · 15, 110, 206, 212, 358

Acessos · 38, 39, 50, 52, 54, 55, 62, 76, 176, 177, 181, 194, 196, 203, 204, 205, 207, 208, 210, 216, 292, 293, 294, 320, 324, 329, 332, 333

Activos · 62, 190, 193, 195, 196, 203, 205, 208, 211, 216, 252, 285, 332, 333, 335

Aprendizagem · 23, 163, 164, 191, 231, 232, 253, 298, 361, 363

B

BSI · 28, 30, 34, 35, 65, 83, 354

C

CISP · 27, 55, 83, 355

CNPD · 76, 77

COBIT · 27, 58, 59, 83, 177, 183, 202, 206, 209, 210, 211, 212, 213, 214, 215, 216, 230, 347, 355

Competências · 206, 214

Confidencialidade · 121, 203, 213, 214

Conformidade · 29, 60, 206, 210, 211

Conhecimento · 7, 11, 23, 24, 97, 98, 111, 112, 117, 163, 164, 165, 181, 231, 300, 301, 319, 320, 328, 329, 333, 348, 357, 361, 364, 366, 368

Contingência · 23, 52, 62, 111, 112, 136, 176, 177, 232, 357, 365

Controlos de Segurança · 176, 177, 194, 206, 212, 218

Cópias de Segurança · 251, 263, 282

D

Disponibilidade · 121, 300, 301, 319, 328

F

FISMA · 177, 183, 194, 195, 196, 230, 358

Formação · 163, 164, 190, 191, 193, 231, 248, 253, 271, 295, 296, 306, 318, 321, 330, 332, 334, 335, 361, 366

Framework · 27, 64, 85, 97, 110, 136, 163, 202, 207, 213, 231, 357, 360, 364

G

GAISP · 27, 60, 63, 84, 202, 207, 210, 211, 212, 213, 214, 215, 216, 230, 358

Globalização · 87, 91, 117

I

Informática · 66, 67, 82, 86, 101, 105, 109, 112, 135, 165, 239, 243, 248, 255, 257, 271, 272, 284, 285, 290, 291, 302, 307, 312, 321, 323, 324, 326, 327, 330, 334, 352, 354, 368, 369

Integridade · 53, 121, 176, 177, 194, 206, 212

Investigação · 12, 15, 22, 23, 112, 304, 354, 362, 365

IPS · 112, 237, 238, 239, 248, 254, 256, 257, 271, 302, 304, 331, 346, 350, 365

ISO/IEC 17799 · 26, 28, 30, 31, 84, 119, 120, 126, 136, 201, 203, 209, 210, 211, 212, 213, 214, 215, 216, 231, 240, 302, 304, 339, 341, 350, 360

ISO/IEC 27001 · 26, 30, 31, 85, 201, 204, 209, 210, 211, 212, 213, 214, 215, 216, 228, 231, 302, 304, 339, 350, 360

ISSAF · 27, 64, 85, 202, 207, 209, 212, 213, 214, 215, 216, 231, 360

ITIL · 27, 34, 35, 56, 85, 360, 365

M

Métricas · 19, 21, 50, 167, 169, 170, 173, 178, 193, 205, 207, 212, 216, 226, 335

Métricas de Segurança · 19, 21, 167, 169, 335

MIDIImOS · 220, 221, 222, 223, 224, 225, 226, 228, 229, 240, 247, 248, 249, 250, 251, 252, 253, 255, 303, 304, 331, 332, 333, 334, 335, 336, 337, 338, 341, 343, 346, 348, 349, 350

Missão · 7, 9, 23, 24, 39, 357, 368

Modelo · 2, 3, 6, 17, 18, 19, 21, 22, 30, 33, 112, 142, 143, 164, 177, 187, 193, 196, 197, 199, 200, 201, 215, 216, 217, 218, 219, 221, 222, 225, 226, 228, 229, 236, 255, 305, 306, 307, 332, 333, 335, 337, 338, 341, 342, 346, 347, 364, 366

N

NIST · 26, 27, 36, 37, 38, 40, 41, 42, 43, 45, 46, 47, 49, 50, 51, 52, 53, 83, 84, 85, 86, 176, 178, 183, 184, 194, 195, 196, 197, 201, 202, 204, 205, 206, 209, 210, 211, 212, 213, 214, 215, 216, 230, 232, 233, 338, 346, 347, 353, 354, 358, 359, 363, 365, 367, 368, 369

Norma · 194, 195, 209, 210, 211, 212, 213, 214, 215

O

OECD · 27, 57, 85, 175, 184, 202, 207, 209, 212, 214, 215, 216, 232, 363

P

Password · 249, 261, 268, 272, 292, 293, 294, 311, 313

PDCA · 30, 216, 217, 218, 219, 221, 228

Percepção · 23, 164, 191, 192, 232, 251, 252, 258, 265, 279, 283, 284, 285, 286, 288, 289, 290, 291, 292, 293, 294, 298, 299, 300, 301, 308, 311, 314, 316, 317, 321, 325, 338, 363

Pessoas · 1, 2, 3, 4, 5, 6, 7, 9, 11, 12, 13, 14, 15, 16, 17, 18, 19, 21, 25, 37, 40, 42, 47, 60, 68, 71, 78, 80, 81, 88, 89, 90, 91, 92, 93, 95, 97, 98, 99, 100, 102, 105, 106, 108, 113, 114, 115, 118, 119, 120, 121, 122, 123, 124, 125, 127, 129, 130, 133, 134, 137, 138, 139, 140, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 152, 153, 155, 156, 157, 158, 159, 160, 161, 168, 170, 172, 173, 176, 179, 180, 181, 182, 183, 187, 188, 189, 190, 191, 192, 193, 197, 199, 200, 217, 219, 221, 222, 226, 228, 229, 235, 236, 237, 240, 242, 254, 255, 263, 264, 268, 271, 272, 273, 275, 279, 280, 281, 283, 285, 286, 291, 295, 298, 301, 302, 303, 304, 305, 306, 307, 311, 312, 314, 315, 317, 318, 319, 320, 321, 322, 323, 324, 325, 326, 328, 329, 330, 331, 332, 333, 334, 335, 336, 337, 338, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 350

Planeamento · 23, 29, 36, 37, 39, 51, 52, 53, 57, 62, 64, 109, 111, 112, 136, 176, 177, 195, 196, 218, 219, 222, 223, 227, 228, 232, 336, 346, 354, 357, 365

Políticas de Segurança · 125, 209, 216, 250, 279, 332, 334

Privacidade · 47, 66, 68, 82, 84, 353, 356

R

Regulamentos · 76, 206, 211, 216, 290, 291, 325

Requisitos de Segurança · 54, 203, 204, 213

Responsabilidade · 10, 29, 30, 58, 60, 92, 175, 190, 191, 207, 209, 214

S

SDLC · 196, 197, 199, 216, 217, 218, 219, 221, 222, 223, 224, 225, 228

Segurança da Informação · 2, 8, 9, 10, 21, 23, 56, 61, 63, 69, 113, 119, 130, 151, 192, 193, 195, 196, 203, 207, 209, 211, 212, 213, 214, 215, 216, 221, 243, 250, 251, 252, 279, 314, 321, 324, 329, 330, 344, 348, 357

Segurança das Pessoas · 53, 176, 177, 195

Segurança de Computadores · 37, 38, 39, 204, 213

Segurança do Sistema Informático · 252, 286, 320, 329, 334

Segurança dos Sistemas de Informação · 135, 136, 162, 165, 229, 233, 354, 368

Segurança Física · 38, 39, 176, 195

Segurança Informática · 136, 163, 232, 362

Sensibilização · 38, 39, 40, 52, 58, 60, 61, 175, 176, 177, 195, 196, 203, 204, 205, 206, 207, 208, 215, 216, 306

SGSI · 2, 3, 16, 17, 18, 19, 30, 31, 32, 82, 119, 131, 132, 134, 143, 172, 173, 182, 187, 189, 190, 193, 194, 195, 196, 198, 199, 200, 202, 204, 209, 210, 211, 212, 213, 215, 216, 217,

218, 219, 222, 223, 224, 225, 227, 228, 236, 247, 254, 302, 304, 305, 306, 307, 328, 331, 332, 336, 337, 338, 340, 341, 342, 343, 346, 347, 348, 349, 350

SI · 1, 2, 3, 5, 6, 8, 9, 11, 13, 14, 15, 16, 17, 18, 19, 25, 34, 35, 36, 41, 43, 45, 46, 47, 51, 54, 56, 57, 58, 60, 61, 63, 64, 69, 87, 90, 91, 92, 93, 97, 98, 100, 101, 102, 103, 104, 105, 106, 107, 108, 109, 113, 115, 118, 119, 122, 123, 124, 125, 126, 127, 128, 129, 130, 131, 132, 133, 134, 137, 138, 139, 141, 142, 143, 144, 145, 146, 147, 148, 149, 150, 151, 153, 154, 155, 156, 157, 158, 159, 160, 161, 167, 169, 170, 172, 173, 175, 179, 180, 181, 187, 188, 189, 190, 191, 192, 193, 194, 196, 198, 199, 200, 202, 203, 209, 213, 216, 217, 219, 227, 228, 230, 236, 239, 254, 255, 302, 303, 305, 306, 321, 325, 331, 332, 335, 336, 337, 338, 340, 341, 342, 343, 344, 345, 346, 347, 348, 349, 355

SIBC · 101, 129, 144

Sistema Informático · 237, 238, 239, 241, 242, 243, 247, 248, 249, 250, 251, 252, 253, 268, 269, 270, 271, 272, 273, 274, 275, 276, 277, 278, 279, 280, 281, 282, 283, 284, 285, 286, 287, 288, 289, 290, 291, 292, 293, 294, 295, 296, 297, 298, 299, 300, 301, 302, 303, 309, 311, 312, 313, 314, 315, 316, 317, 318, 319, 320, 321, 322, 324, 325, 326, 327, 328, 329, 330, 334, 335

Sociedade da Informação · 7, 8, 9, 10, 11, 12, 13, 14, 22, 24, 79, 87, 109, 117, 124, 133, 134, 135, 147, 148, 156, 164, 173, 222, 229, 341, 347, 348, 352, 357, 366, 368

Standard · 27, 28, 54, 83, 84, 85, 136, 169, 184, 202, 208, 209, 210, 211, 212, 213, 214, 215, 216, 231, 304, 339, 350, 353, 360

T

The Standard · 27, 54, 84, 202, 208, 231, 360

TI · 11, 34, 35, 36, 38, 40, 41, 42, 43, 46, 47, 48, 49, 56, 57, 58, 59, 60, 62, 63, 65, 78, 80, 101, 102, 103, 105, 106, 107, 108, 144, 145, 177, 178, 191, 192

TIC · 2, 3, 4, 5, 6, 11, 12, 13, 14, 15, 16, 17, 18, 19, 25, 32, 37, 45, 56, 57, 69, 77, 82, 87, 88, 89, 90, 91, 97, 98, 100, 102, 103, 105, 106, 107, 108, 113, 114, 115, 117, 118, 119, 120, 123, 124, 125, 129, 130, 131, 132, 133, 134, 137, 138, 139, 141, 142, 143, 144, 145, 146, 147, 149, 150, 151, 154, 155, 156, 157, 158, 161, 164, 169, 170, 172, 173, 180, 181, 187, 188, 189, 190, 191, 192, 193, 199, 200, 217, 221, 222, 223, 228, 233, 236, 239, 254, 255, 302, 303, 305, 306, 321, 325, 331, 332, 335, 336, 337, 338, 340, 341, 342, 343, 344, 346, 347, 348, 349, 350, 365

U

UMIC · 7, 8, 23, 24, 357, 368

Usabilidade · 154, 158, 192, 193, 243, 253, 295, 317

Utilizadores · 54, 59, 146, 203, 204, 205, 207, 208, 210, 211, 214, 290, 317



As Pessoas nos Sistemas de Gestão da
Segurança da Informação
(ANEXOS)

José Manuel Gaivéo

UNIVERSIDADE ABERTA

2008

UNIVERSIDADE ABERTA

Doutoramento em Informática

As Pessoas nos Sistemas de Gestão da Segurança da Informação

- ANEXOS -

José Manuel Gaivéo

Orientação:

Professor Doutor Alexandre Gomes Cerveira (DCET/UAb)

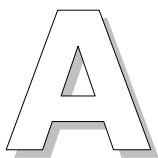
Professora Doutora Maria Leonilde dos Reis (DSI/ESCE/IPS)

2008

Índice de Anexos

Anexo A – Normativo de Segurança.....	A.1
BS ISO/IEC 17799:2005 Code of practice for information security management	A.2
BS ISO/IEC 27001:2005 – Information Security Management Systems – Requirements	A.19
ISO/IEC 21827:2002 – Systems Security Engineering - Capability Maturity Model (SSE-CMM)	A.24
SP800-12 – An Introduction to Computer Security: The NIST Handbook	A.40
SP800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems	A.85
SP800-18 – Guide for Developing Security Plans for Information Technology Systems	A.95
The Standard of Good Practice for Information Security	A.105
OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security	A.125
Control Objectives for Information and related Technology (COBIT)	A.127
Generally Accepted Information Security Principles (GAISP)	A.150
Information Systems Security Assessment Framework (ISSAF)	A.157
Anexo B – Modelo do Questionário	B.1
Questionário – Docentes	B.2
Questionário – Não Docentes	B.9
Questionário – Técnicos de Informática	B.16
Anexo C – Modelo das instruções de entrega dos questionários	C.1
Anexo D – Resultados do Questionário – Grupo de Teste	D.1
Grupo A – Identificação/Caracterização do(a) inquirido(a)	D.1
Grupo B – Computador pessoal	D.2
Grupo C – Sistema Informático da Escola	D.9
Grupo D – Segurança da Informação no Sistema Informático da Escola	D.18
Grupo E – Usabilidade do Sistema Informático da Escola	D.23

Anexo E – Resultados do Questionário tipos A, B e C	E.1
Grupo A – Identificação/Caracterização do(a) inquirido(a)	E.1
Grupo B – Computador pessoal	E.5
Grupo C – Sistema Informático do Serviço/Escola	E.13
Grupo D – Segurança da Informação no Sistema Informático do Serviço/Escola	E.24
Grupo E – Usabilidade do Sistema Informático do Serviço/Escola	E.40



Normativo de Segurança

O conjunto de normas que seguidamente se apresenta, num total de 11, previamente identificadas como essenciais para o Modelo a desenvolver, são apresentadas neste anexo, referenciando-se todos componentes da sua estrutura e um breve resumo, essencial para um entendimento da estrutura da norma, de cada um desses componentes.

Deve todavia notar-se que o propósito e objectivos de cada uma das normas previamente analisadas, um total de 30, constam do texto da tese, não se considerando por isso necessária a sua duplicação no anexo A.

As referências constantes dos diversos títulos que expressam a estrutura de cada norma correspondem exactamente aos respectivos capítulos e subdivisões dos mesmos. Todas as referências aos conteúdos apresentados devem ser feitas através das respectivas normas, de acordo com a bibliografia constante da tese.

Refira-se ainda que neste anexo o que é apresentado por cada uma das normas dele constantes é apenas um breve resumo, na língua de origem das normas, entendido como suficiente para uma compreensão das mesmas.

BS ISO/IEC 17799:2005 Code of practice for information security management

This standard (BS ISO/IEC 17799:2005) contains 11 security controls clauses collectively containing a total of 39 main security categories and one introductory clause introducing risk assessment and treatment [ISO 2005a].

Each clause contains a number of main security categories. The eleven clauses (accompanied with the number of main security categories included within each clause) are:

- a) Security Policy (1);
- b) Organizing Information security (2);
- c) Asset Management (2);
- d) Human Resources Security (3);
- e) Physical and Environmental Security (2);
- f) Communications and Operations Management (10);
- g) Access Control (7);
- h) Information Systems Acquisition, Development and Maintenance (6);
- i) Information Security Incident Management (2);
- j) Business Continuity Management (1);
- k) Compliance (3).

5. Security Policy

5.1 Information security policy

To provide management direction and support for information security in accordance with business requirements and relevant laws and regulations.

- Management should set a clear policy direction in line with business objectives and demonstrate support for, and commitment to, information security through the issue and maintenance of an information security policy across the organization.

5.1.1 information security policy document

An information security policy document should be approved by management, and published and communicated to all employees and relevant external parties.

5.1.2 review of the information security policy

The information security policy should be reviewed at planned intervals or if significant changes occur to ensure its continuing suitability, adequacy, and effectiveness.

6. Organizing Information Security

6.1 Internal organization

To manage information security within the organization.

- A management framework should be established to initiate and control the implementation of information security within the organization.
- Management should approve the information security policy, assign security roles and coordinate and review the implementation of security across the organization.
- If necessary, a source of specialist information security advice should be established and made available within the organization. Contacts with external security specialists or groups, including relevant authorities, should be developed to keep up with industrial trends, monitor standards and assessment methods and provide suitable liaison points when handling information security incidents. A multi-disciplinary approach to information security should be encouraged.

6.1.1 management commitment of information security

Management should actively support security within the organization through clear direction, demonstrated commitment, explicit assignment, and acknowledgment of information security responsibilities.

6.1.2 information security co-ordination

Information security activities should be co-ordinated by representatives from different parts of the organization with relevant roles and job functions.

6.1.3 allocation of information security responsibilities

All information security responsibilities should be clearly defined.

6.1.4 authorization process for information processing facilities

A management authorization process for new information processing facilities should be defined and implemented.

6.1.5 confidentiality agreements

Requirements for confidentiality or non-disclosure agreements reflecting the organization's needs for the protection of information should be identified and regularly reviewed.

6.1.6 contact with authorities

Appropriate contacts with relevant authorities should be maintained.

6.1.7 contact with special interest groups

Appropriate contacts with special interest groups or other specialist security forums and professional associations should be maintained.

6.1.8 independent review of information security

The organization's approach to managing information security and its implementation (i.e. Control objectives, controls, policies, processes, and procedures for information security) should be reviewed independently at planned intervals, or when significant changes to the security implementation occur.

6.2 External parties

To maintain the security of the organization's information and information processing facilities that are accessed, processed, communicated to, or managed by external parties.

- The security of the organization's information and information processing facilities should not be reduced by the introduction of external party products or services.
- Any access to the organization's information processing facilities and processing and communication of information by external parties should be controlled.
- Where there is a business need for working with external parties that may require access to the organization's information and information processing facilities, or in obtaining or providing a product or service from or to an external party, a risk assessment should be carried out to determine security implications and control requirements. Controls should be agreed and defined in an agreement with the external party.

6.2.1 identification of risks related to external parties

The risks to the organization's information and processing facilities from business processes involving external parties should be identified and appropriate controls implemented before granting access.

6.2.2 addressing security when dealing with customers

All identified security requirements should be addressed before giving customers access to the organization's information or assets.

6.2.3 addressing security in third party agreements

Agreements with third parties involving accessing, processing, communicating or managing the organization's information or information processing facilities, or adding products or services to information processing facilities should cover all relevant security requirements.

7. Asset Management

7.1 Responsibility for assets

To achieve and maintain appropriate protection of organizational assets.

- All assets should be accounted for and have a nominated owner.
- Owners should be identified for all assets and the responsibility for the maintenance of appropriate controls should be assigned. The implementation of specific controls may be delegated by the owner as appropriate but the owner remains responsible for the proper protection of the assets.

7.1.1 inventory of assets

All assets should be clearly identified and an inventory of all important assets drawn up and maintained.

7.1.2 ownership of assets

All information and assets associated with information processing facilities should be owned by a designated part of the organization.

7.1.3 acceptable use of assets

Rules for the acceptable use of information and assets associated with information processing facilities should be identified, documented, and implemented.

7.2 Information classification

To ensure that information receives an appropriate level of protection.

- Information should be classified to indicate the need, priorities, and expected degree of protection when handling the information.
- Information has varying degrees of sensitivity and criticality. Some items may require an additional level of protection or special handling. An information classification scheme should be used to define an appropriate set of protection levels and communicate the need for special handling measures.

7.2.1 classification guidelines

Information should be classified in terms of its value, legal requirements, sensitivity, and criticality to the organization.

7.2.2 information labeling and handling

An appropriate set of procedures for information labelling and handling should be developed and implemented in accordance with the classification scheme adopted by the organization.

8. Human Resources Security

8.1 Prior to employment

To ensure that employees, contractors and third party users understand their responsibilities, and are suitable for the roles they are considered for, and reduce the risk of theft, fraud or misuse of facilities.

- Security responsibilities should be addressed prior to employment in adequate job descriptions and in terms and conditions of employment.

- All candidates for employment, contractors and third party users should be adequately screened, especially for sensitive jobs.
- Employees, contractors and third party users of information processing facilities should sign an agreement on their security roles and responsibilities.

8.1.1 roles and responsibilities

Security roles and responsibilities of employees, contractors and third party users should be defined and documented in accordance with the organization's information security policy.

8.1.2 screening

Background verification checks on all candidates for employment, contractors, and third party users should be carried out in accordance with relevant laws, regulations and ethics, and proportional to the business requirements, the classification of the information to be accessed, and the perceived risks.

8.1.3 terms and conditions of employment

As part of their contractual obligation, employees, contractors and third party users should agree and sign the terms and conditions of their employment contract, which should state their and the organization's responsibilities for information security.

8.2 During employment

To ensure that employees, contractors and third party users are aware of information security threats and concerns, their responsibilities and liabilities, and are equipped to support organizational security policy in the course of their normal work, and to reduce the risk of human error.

- Management responsibilities should be defined to ensure that security is applied throughout an individual's employment within the organization.
- An adequate level of awareness, education, and training in security procedures and the correct use of information processing facilities should be provided to all employees, contractors and third party users to minimize possible security risks. A formal disciplinary process for handling security breaches should be established.

8.2.1 management responsibilities

Management should require employees, contractors, and third party users to apply security in accordance with established policies and procedures of the organization.

8.2.2 information security awareness, education, and training

All employees of the organization and, where relevant, contractors and third party users should receive appropriate awareness training and regular updates in organizational policies and procedures, as relevant for their job function.

8.2.3 disciplinary process

There should be a formal disciplinary process for employees who have committed a security breach.

8.3 Termination or change of employment

To ensure that employees, contractors and third party users exit an organization or change employment in an orderly manner.

- Responsibilities should be in place to ensure an employee's, contractor's or third party user's exit from organization is managed, and that the return of all equipment and the removal of all access rights are completed.
- Change of responsibilities and employments within an organization should be managed as the termination of the respective responsibility or employment in line with this section, and any new employments should be managed as described in section 8.1.

8.3.1 termination responsibilities

Responsibilities for performing employment termination or change of employment should be clearly defined and assigned.

8.3.2 return of assets

All employees, contractors and third party users should return all of the organization's assets in their possession upon termination of their employment, contract or agreement.

8.3.3 removal of access rights

The access rights of all employees, contractors and third party users to information and information processing facilities should be removed upon termination of their employment, contract or agreement, or adjusted upon change.

9. Physical and Environmental Security

9.1 Secure areas

To prevent unauthorized physical access, damage, and interference to the organization's premises and information.

- Critical or sensitive information processing facilities should be housed in secure areas, protected by defined perimeters, with appropriate security barriers and entry controls. They should be physically protected from unauthorized access, damage, and interference.
- The protection provided should be commensurate with the identified risks.

9.1.1 physical security perimeter

Security perimeters (barriers such as walls, card controlled entry gates or manned reception desks) should be used to protect areas that contain information and information processing facilities.

9.1.2 physical entry controls

Secure areas should be protected by appropriate entry controls to ensure that only authorized personnel are allowed access.

9.1.3 securing offices, rooms, and facilities

Physical security for offices, rooms, and facilities should be designed and applied.

9.1.4 protecting against external and environmental threats

Physical protection against damage from fire, flood, earthquake, explosion, civil unrest, and other forms of natural or man-made disaster should be designed and applied.

9.1.5 working in secure areas

Physical protection and guidelines for working in secure areas should be designed and applied.

9.1.6 public access, delivery, and loading areas

Access points as delivery and loading areas and other points where unauthorized persons may enter the premises should be controlled and, if possible, isolated from information processing facilities to avoid unauthorized access.

9.2 Equipment security

To prevent loss, damage, theft or compromise of assets and interruption to the organization's activities.

- Equipment should be protected from physical and environmental threats.
- Protection of equipment (including that used off-site, and the removal of property) is necessary to reduce the risk of unauthorized access to information and to protect against loss or damage. This should also consider equipment siting and disposal. Special controls may be required to protect against threats, and to safeguard supporting facilities, such as the electrical supply and cabling infrastructure.

9.2.1 equipment siting and protection

Equipment should be sited or protected to reduce the risks from environmental threats and hazards, and opportunities for unauthorized access.

9.2.2 supporting facilities

Equipment should be protected from power failures and other disruptions caused by failures in supporting utilities.

9.2.3 cabling security

Power and telecommunications cabling carrying data or supporting information services should be protected from interception or damage.

9.2.4 equipment maintenance

Equipment should be correctly maintained to ensure its continued availability and integrity.

9.2.5 security of equipment off-permises

Security should be applied to off-site equipment taking into account the different risks of working outside the organization's premises.

9.2.6 secure disposal or re-use of equipment

All items of equipment containing storage media should be checked to ensure that any sensitive data and licensed software has been removed or securely overwritten prior to disposal.

9.2.7 removal of property

Equipment, information or software should not be taken off-site without prior authorization.

10. Communications and Operations Management

10.1 Operational procedures and responsibilities

To ensure the correct and secure operation of information processing facilities.

- Responsibilities and procedures for the management and operation of all information processing facilities should be established. This includes the development of appropriate operating procedures.
- Segregation of duties should be implemented, where appropriate, to reduce the risk of negligent or deliberate system misuse.

10.1.1 documented operating procedures

Operating procedures should be documented, maintained, and made available to all users who need them.

10.1.2 change management

Changes to information processing facilities and systems should be controlled.

10.1.3 segregation of duties

Duties and areas of responsibility should be segregated to reduce opportunities for unauthorized or unintentional modification or misuse of the organization's assets.

10.1.4 separation of development, test, and operational facilities

Development, test, and operational facilities should be separated to reduce the risks of unauthorized access or changes to the operational system.

10.2 Third party service delivery management

To implement and maintain the appropriate level of information security and service delivery in line third party service delivery agreements.

- The organization should check the implementation of agreements, monitor compliance with the agreements and manage changes to ensure that the services delivered meet all requirements agreed with the third party.

10.2.1 service delivery

It should be ensured that the security controls, service definitions and delivery levels included in the third party service agreement are implemented, operated, and maintained by the third party.

10.2.2 monitoring and review of third party services

The services, reports and records provided by the third party should be regularly monitored and reviewed, and audits should be carried out regularly.

10.2.3 managing changes to third party services

Changes to the provision of services, including maintaining and improving existing information security policies, procedures and controls, should be managed, taking account of the criticality of business systems and processes involved and re-assessment of risks.

10.3 System planning and acceptance

To minimize the risk of systems failures.

- Advance planning and preparation are required to ensure the availability of adequate capacity and resources to deliver the required system performance.
- Projections of future capacity requirements should be made, to reduce the risk of system overload.
- The operational requirements of new systems should be established, documented, and tested prior to their acceptance and use.

10.3.1 capacity management

The use of resources should be monitored, tuned, and projections made of future capacity requirements to ensure the required system performance.

10.3.2 system acceptance

Acceptance criteria for new information systems, upgrades, and new versions should be established and suitable tests of the system(s) carried out during development and prior to acceptance.

10.4 Protection against malicious and mobile code

To protect the integrity of software and information.

- Precautions are required to prevent and detect the introduction of malicious code and unauthorized mobile code.
- Software and information facilities are vulnerable to the introduction of malicious code, such as computer viruses, network worms, Trojan horses, and logic bombs. Users should be made aware of the dangers of malicious code. Managers should, where appropriate, introduce controls to prevent, detect, and remove malicious code and control mobile code.

10.4.1 controls against malicious code

Detection, prevention, and recovery controls to protect against malicious code and appropriate user awareness procedures should be implemented.

10.4.2 controls against mobile code

Where the use of mobile code is authorised, the configuration should ensure that the authorised mobile code operates according to a clearly defined security policy, and unauthorised mobile code should be prevented from executing.

10.5 Back-up

To maintain the integrity and availability of information and information processing facilities.

- Routine procedures should be established to implement the agreed back-up policy and strategy (see also 14.1) for taking back-up copies of data and rehearsing their timely restoration.

10.5.1 information back-up

Back-up copies of information and software should be taken and tested regularly in accordance with the agreed backup policy.

10.6 Network security management

To ensure the protection of information in networks and the protection of the supporting infrastructure.

- The secure management of networks, which may span organizational boundaries, requires careful consideration to dataflow, legal implications, monitoring, and protection.
- Additional controls may also be required to protect sensitive information passing over public networks.

10.6.1 network controls

Networks should be adequately managed and controlled, in order to be protected from threats, and to maintain security for the systems and applications using the network, including information in transit.

10.6.2 security of network services

Security features, service levels, and management requirements of all network services should be identified and included in any network services agreement, whether these services are provided in-house or outsourced.

10.7 Media handling

To prevent unauthorized disclosure, modification, removal or destruction of assets, and interruption to business activities.

- Media should be controlled and physically protected.
- Appropriate operating procedures should be established to protect documents, computer media (e.g. Tapes, disks), input/output data and system documentation from unauthorized disclosure, modification, removal, and destruction.

10.7.1 management of removal media

There should be procedures in place for the management of removable media.

10.7.2 disposal of media

Media should be disposed of securely and safely when no longer required, using formal procedures.

10.7.3 information handling procedures

Procedures for the handling and storage of information should be established to protect this information from unauthorized disclosure or misuse.

10.7.4 security of system documentation

System documentation should be protected against unauthorized access.

10.8 Exchange of information

To maintain the security of information and software exchanged within a organization and with any external entity.

- Exchanges of information and software between organizations should be based on a formal exchange policy, carried out in line with exchange agreements, and should be compliant with any relevant legislation (see clause 15).

- Procedures and standards should be established to protect information and physical media containing information in transit.

10.8.1 information exchange policies and procedures

Formal exchange policies, procedures, and controls should be in place to protect the exchange of information through the use of all types of communication facilities.

10.8.2 exchange agreements

Agreements should be established for the exchange of information and software between the organization and external parties.

10.8.3 physical media in transit

Media containing information should be protected against unauthorized access, misuse or corruption during transportation beyond an organization's physical boundaries.

10.8.4 electronic messaging

Information involved in electronic messaging should be appropriately protected.

10.8.5 business information systems

Policies and procedures should be developed and implemented to protect information associated with the interconnection of business information systems.

10.9 Electronic commerce services

To ensure the security of electronic commerce services, and their secure use.

- The security implications associated with using electronic commerce services, including on-line transactions, and the requirements for controls, should be considered. The integrity and availability of information electronically published through publicly available systems should be also considered.

10.9.1 electronic commerce

Information involved in electronic commerce passing over public networks should be protected from fraudulent activity, contract dispute, and unauthorized disclosure and modification.

10.9.2 on-line transactions

Information involved in on-line transactions should be protected to prevent incomplete transmission, mis-routing, unauthorized message alteration, unauthorized disclosure, unauthorized message duplication or replay.

10.9.3 publicly available information

The integrity of information being made available on a publicly available system should be protected to prevent unauthorized modification.

10.10 Monitoring

To detect unauthorized information processing activities.

- Systems should be monitored and information security events should be recorded. Operators logs and fault logging should be used to ensure information system problems are identified.
- An organization should comply with all relevant legal requirements applicable to its monitoring and logging activities.
- System monitoring should be used to check the effectiveness of controls adopted and to verify conformity to an access policy model.

10.10.1 Audit logging

Audit logs recording user activities, exceptions, and information security events should be produced and kept for an agreed period to assist in future investigations and access control monitoring.

10.10.2 monitoring system use

Procedures for monitoring use of information processing facilities should be established and the results of the monitoring activities reviewed regularly.

10.10.3 protection of log information

Logging facilities and log information should be protected against tampering and unauthorized access.

10.10.4 administrator and operator logs

System administrator and system operator activities should be logged.

10.10.5 fault logging

Faults should be logged, analysed, and appropriate action taken.

10.10.6 clock synchronization

The clocks of all relevant information processing systems within an organization or security domain should be synchronized with an agreed accurate time source.

11. Access Control

11.1 Business requirement for access control

To control access to information

- Access to information, information processing facilities, and business processes should be controlled on the basis of business and security requirements
- Access control rules should take account of policies for information dissemination and authorization.

11.1.1 access control policy

An access control policy should be established, documented, and reviewed based on business and security requirements for access.

11.2 User access management

To ensure authorized user access and to prevent unauthorized access to information systems.

- Formal procedures should be in place to control the allocation of access rights to information systems and services.
- The procedures should cover all stages in the life-cycle of users access, from the initial registration of new users to the final de-registration of users who no longer require access to information systems and services. Special attention should be given, where appropriate, to the need to control the allocation of privileged access rights, which allow users to override system controls.

11.2.1 user registration

There should be a formal user registration and de-registration procedure in place for granting and revoking access to all information systems and services.

11.2.2 privilege management

The allocation and use of privileges should be restricted and controlled.

11.2.3 user password management

The allocation of passwords should be controlled through a formal management process.

11.2.4 review of user access rights

Management should review users' access rights at regular intervals using a formal process.

11.3 User responsibilities

To prevent unauthorized user access, and compromise or theft of information and information processing facilities.

- The co-operation of unauthorized users is essential for effective security.

- Users should be made aware of their responsibilities for maintaining effective access controls, particularly regarding the use of passwords and the security of user equipment.
- A clear desk and clear screen policy should be implemented to reduce the risk of unauthorized access or damage to papers, media, and information processing facilities.

11.3.1 password use

Users should be required to follow good security practices in the selection and use of passwords.

11.3.2 unattended user equipment

Users should ensure that unattended equipment has appropriate protection.

11.3.3 clear desk and clear screen policy

A clear desk policy for papers and removable storage media and a clear screen policy for information processing facilities should be adopted.

11.4 Network access control

To prevent unauthorized access to networked services.

- Access to both internal and external networked services should be controlled.
- User access to networks and network services should not compromise the security of the network services by ensuring:
 - a) appropriate interfaces are in place between the organization's network and networks owned by other organizations, and public networks;
 - b) appropriate authentication mechanisms are applied for users and equipment;
 - c) control of user access to information services is enforced.

11.4.1 policy on use of network services

Users should only be provided with access to the services that they have been specifically authorized to use.

11.4.2 user authentication for external connections

Appropriate authentication methods should be used to control access by remote users.

11.4.3 equipment identification in networks

Automatic equipment identification should be considered as a means to authenticate connections from specific locations and equipment.

11.4.4 remote diagnostic and configuration port protection

Physical and logical access to diagnostic and configuration ports should be controlled.

11.4.5 segregation in networks

Groups of information services, users, and information systems should be segregated on networks.

11.4.6 network connection control

For shared networks, especially those extending across the organization's boundaries, the capability of users to connect to the network should be restricted, in line with the access control policy and requirements of the business applications (see 11.1.1).

11.4.7 network routing control

Routing controls should be implemented for networks to ensure that computer connections and information flows do not breach the access control policy of the business applications.

11.5 Operating system access control

To prevent unauthorized access to operating systems.

- Security facilities should be used to restrict access to operating systems to authorized users. The facilities should be capable of the following:

- a) authenticating authorized users, in accordance with a defined access control policy;
- b) recording successful and failed system authentication attempts;
- c) recording the use of special system privileges;
- d) issuing alarms when system security policies are breached;
- e) providing appropriate means for authentication;
- f) where appropriate, restricting the connection time of users.

11.5.1 secure log-on procedures

Access to operating systems should be controlled by a secure log-on procedure.

11.5.2 user identification and authentication

All users should have a unique identifier (user ID) for their personal use only, and a suitable authentication technique should be chosen to substantiate the claimed identity of a user.

11.5.3 password management system

Systems for managing passwords should be interactive and should ensure quality passwords.

11.5.4 use of system utilities

The use of utility programs that might be capable of overriding system and application controls should be restricted and tightly controlled.

11.5.5 session time-out

Inactive sessions should shut down after a defined period of inactivity.

11.5.6 limitation of connection time

Restrictions on connection times should be used to provide additional security for high-risk applications.

11.6.1 Information access restriction

To prevent unauthorized access to information held in application systems.

- Security facilities should be used to restrict access to and within application systems.
- Logical access to application software and information should be restricted to authorized users. Application systems should:
 - a) control user access to information and application system functions, in accordance with a defined access control policy;
 - b) provide protection from unauthorized access by any utility, operating system software, and malicious software that is capable of overriding or by passing system or application controls;
 - c) not compromise other systems with which information resources are shared.

11.6.1 information access restriction

Access to information and application system functions by users and support personnel should be restricted in accordance with the defined access control policy.

11.6.2 sensitive system isolation

Sensitive systems should have a dedicated (isolated) computing environment..

11.7 Mobile computing and teleworking

To ensure information security when using mobile computing and teleworking facilities.

The protection required should be commensurate with the risks these specific ways of working cause. When using mobile computing the risks of working in an unprotected environment should be considered and appropriate protection applied. In the case of teleworking the organization should apply protection to the teleworking site and ensure that suitable arrangements are in place for this way of working.

11.7.1 mobile computing and communications

A formal policy should be in place, and appropriate security measures should be adopted to protect against the risks of using mobile computing and communication facilities.

11.7.2 teleworking

A policy, operational plans and procedures should be developed and implemented for teleworking activities.

12. Information Systems Acquisition, Development and Maintenance

12.1 Security requirements of information systems

To ensure that security is an integral part of information systems.

- Information systems include operating systems, infrastructure, business applications, off-the-shelf products, services, and user-developed applications. The design and implementation of the information system supporting the business process can be crucial for security. Security requirements should be identified and agreed prior to the development and/or implementation of information systems.
- All security requirements should be identified at the requirements phase of a project and justified, agreed, and documented as part of the overall business case for an information system.

12.1.1 security requirements analysis and specification

Statements of business requirements for new information systems, or enhancements to existing information systems should specify the requirements for security controls.

12.2 Correct processing in applications

To prevent errors, loss, unauthorized modification or misuse of information in applications.

- Appropriate controls should be designed into applications, including user developed applications to ensure correct processing. These controls should include the validation of input data, internal processing and output data.
- Additional controls may be required for systems that process, or have an impact on, sensitive, valuable or critical information. Such controls should be determined on the basis of security requirements and risk assessment.

12.2.1 input data validation

Data input to applications should be validated to ensure that this data is correct and appropriate.

12.2.2 control of internal processing

Validation checks should be incorporated into applications to detect any corruption of information through processing errors or deliberate acts.

12.2.3 message integrity

Requirements for ensuring authenticity and protecting message integrity in applications should be identified, and appropriate controls identified and implemented.

12.2.4 output data validation

Data output from an application should be validated to ensure that the processing of stored information is correct and appropriate to the circumstances.

12.3 Cryptographic controls

To protect the confidentiality, authenticity or integrity of information by cryptographic means.

- A policy should be developed on the use of cryptographic controls. Key management should be in place to support the use of cryptographic techniques.

12.3.1 policy on the use of cryptographic controls

A policy on the use of cryptographic controls for protection of information should be developed and implemented.

12.3.2 key management

Key management should be in place to support the organization's use of cryptographic techniques.

12.4 Security of system files

To ensure the security of system files.

- Access to system files and program source code should be controlled, and IT projects and support activities conducted in a secure manner. Care should be taken to avoid exposure of sensitive data in test environments.

12.4.1 control of operational software

There should be procedures in place to control the installation of software on operational systems.

12.4.2 protection of system test data

Test data should be selected carefully, and protected and controlled.

12.4.3 access control to program source code

Access to program source code should be restricted.

12.5 Security in development and support processes

To maintain the security of application system software and information.

- Project and support environments should be strictly controlled.
- Managers responsible for application systems should also be responsible for the security of the project or support environment. They should ensure that all proposed system changes are reviewed to check that they do not comprise the security of either the system or the operating environment.

12.5.1 change control procedures

The implementation of changes should be controlled by the use of formal change control procedures.

12.5.2 technical review of applications after operating system changes

When operating systems are changed, business critical applications should be reviewed and tested to ensure there is no adverse impact on organizational operations or security.

12.5.3 restrictions on changes to software packages

Modifications to software packages should be discouraged, limited to necessary changes, and all changes should be strictly controlled.

12.5.4 information leakage

Opportunities for information leakage should be prevented.

12.5.5 outsourced software development

Outsourced software development should be supervised and monitored by the organization.

12.6 Technical vulnerability management

To reduce risks resulting from exploitation of published technical vulnerabilities.

- Technical vulnerability management should be implemented in an effective, systematic, and repeatable way with measurements taken to confirm its effectiveness. These considerations should include operating systems, and any other applications in use.

12.6.1 control of technical vulnerabilities

Timely information about technical vulnerabilities of information systems being used should be obtained, the organization's exposure to such vulnerabilities evaluated, and appropriate measures taken to address the associated risk.

13. Information Security Incident Management

13.1 Reporting information security events and weaknesses

To ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken.

- Formal event reporting and escalation procedures should be in place. All employees, contractors and third party users should be made aware of the procedures for reporting the different types of event and weakness that might have an impact on the security of organizational assets. They should be required to report any information security events and weakness as quickly as possible to the designated point of contact.

13.1.1 reporting information security events

Information security events should be reported through appropriate management channels as quickly as possible.

13.1.2 reporting security weakness

All employees, contractors and third party users of information systems and services should be required to not and report any observed or suspected security weakness in systems or services.

13.2 Management of information security incidents and improvements

To ensure a consistent and effective approach is applied to the management of information security incidents.

- Responsibilities and procedures should be in place to handle information security events and weakness effectively once they have been reported. A process of continual improvement should be applied to the response to, monitoring, evaluating, and overall management of information security incidents.
- Where evidence is required, it should be collected to ensure compliance with legal requirements.

13.2.1 responsibilities and procedures

Management responsibilities and procedures should be established to ensure a quick, effective, and orderly response to information security incidents.

13.2.2 learning from information security incidents

There should be mechanisms in place to enable the types, volumes, and costs of information security incidents to be quantified and monitored.

13.2.3 collection of evidence

Where a follow-up action against a person or organization after an information security incident involves legal action (either civil or criminal), evidence should be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s).

14. Business Continuity Management

14.1 Information security aspects of business continuity management

To counteract interruptions of business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption.

- A business continuity management process should be implemented to minimize the impact on the organization and recover from loss of information assets (which may be the result of, for example, natural disasters, accidents, equipment failures, and deliberate actions) to an acceptable level through a combination of preventive and recovery controls. This process should identify the critical business processes and integrate the information security management requirements of business continuity with other continuity requirements relating to such aspects as operations, staffing, materials, transport and facilities.
- The consequences of disasters, security failures, loss of service, and service availability should be subject to a business impact analysis. Business continuity plans should be developed and implemented to ensure timely resumption of essential operations. Information security should be an integral part of the overall business continuity process, and other management processes within the organization.
- Business continuity management should include controls to identify and reduce risks, in addition to the general risks assessment process, limit the consequences of damaging incidents, and ensure that information required for business processes is readily available.

14.1.1 including information security in the business continuity management process

A managed process should be developed and maintained for business continuity throughout the organization that addresses the information security requirements needed for the organization's business continuity.

14.1.2 business continuity and risk assessment

Events that can cause interruptions to business processes should be identified, along with the probability and impact of such interruptions and their consequences for information security.

14.1.3 developing and implementing continuity plans including information security

Plans should be developed and implemented to maintain or restore operations and ensure availability of information at the required level and in the required time scales following interruption to, or failure of, critical business processes.

14.1.4 business continuity planning framework

A single framework of business continuity plans should be maintained to ensure all plans are consistent, to consistently address information security requirements, and to identify priorities for testing and maintenance.

14.1.5 testing, maintaining and re-assessing business continuity plans

Business continuity plans should be tested and updated regularly to ensure that they are up to date and effective.

15. Compliance

15.1 compliance with legal requirements

To avoid breaches of any law, statutory, regulatory or contractual obligations, and of any security requirements.

- The design, operation, use, and management of information systems may be subject to statutory, regulatory, and contractual security requirements.
- Advice on specific legal requirements should be sought from the organization's legal advisers, or suitably qualified legal practitioners. Legislative requirements vary from country to country and may vary for information created in one country that is transmitted to another country (i.e. trans-border data flow).

15.1.1 identification of applicable legislation

All relevant statutory, regulatory, and contractual requirements and the organization's approach to meet these requirements should be explicitly defined, documented, and kept up to date for each information system and the organization.

15.1.2 intellectual property rights (IPR)

Appropriate procedures should be implemented to ensure compliance with legislative, regulatory, and contractual requirements on the use of material in respect of which there may be intellectual property rights and on the use of proprietary software products.

15.1.3 protection of organizational records

Important records should be protected from loss, destruction, and falsification, in accordance with statutory, regulatory, contractual, and business requirements.

15.1.4 data protection and privacy of personal information

Data protection and privacy should be ensured as required in relevant legislation, regulations, and, if applicable, contractual clauses.

15.1.5 prevention of misuse of information processing facilities

Users should be deterred from using information processing facilities for unauthorized purposes.

15.1.6 regulation of cryptographic controls

Cryptographic controls should be used in compliance with all relevant agreements, laws, and regulations.

15.2 Compliance with security policies and standards, and technical compliance

To ensure compliance of systems with organizational security policies and standards.

- The security of information systems should be regularly reviewed.
- Such reviews should be performed against the appropriate security policies and the technical platforms and information systems should be audited for compliance with applicable security implementation standards and documented security controls.

15.2.1 compliance with security policies and standards

Managers should ensure that all security procedures within their area of responsibility are carried out correctly to achieve compliance with security policies and standards.

15.2.2 technical compliance checking

Information systems should be regularly checked for compliance with security implementation standards.

15.3 Information systems audit considerations

To maximize the effectiveness of and to minimize interference to/from the information systems audit process.

- There should be controls to safeguard operational systems and audit tools during information systems audits
- Protection is also required to safeguard the integrity and prevent misuse of audit tools.

15.3.1 information systems audit controls

Audit requirements and activities involving checks on operational systems should be carefully planned and agreed to minimize the risk of disruptions to business processes.

15.3.2 protection of information systems audit tools

Access to information systems audit tools should be protected to prevent any possible misuse or compromise.

BS ISO/IEC 27001:2005 – Information Security Management Systems – Requirements

4. Information security management system

4.1 General requirements

The organization shall establish, implement, operate, monitor, review, maintain and improve a documented ISMS within the context of the organization's overall business activities and the risks it faces. For the purposes of this International Standard the process used is based on the PDCA model.

4.2 Establish and managing the ISMS

4.2.1 Establish the ISMS

- a) Define the scope and boundaries of the ISMS in terms of the characteristics of the business, the organization, its location, assets and technology, and including details of and justification for any exclusions from the scope (see 1.2).
- b) Define an ISMS policy in terms of the characteristics of the business, the organization, its location, assets and technology.
- c) Define the risk assessment approach of the organization.
- d) Identify the risks.
- e) Analyse and evaluate the risks.
- f) Identify and evaluate options for the treatment of risks.
- g) Select control objectives and controls for the treatment of risks.
- h) Obtain management approval of the proposed residual risks.
- i) Obtain management authorization to implement and operate the ISMS.
- j) Prepare a Statement of Applicability.

4.2.2 Implement and operate the ISMS

- a) Formulate a risk treatment plan that identifies the appropriate management action, resources, responsibilities and priorities for managing information security risks (see 5).
- b) Implement the risk treatment plan in order to achieve the identified control objectives, which includes consideration of funding and allocation of roles and responsibilities.
- c) Implement controls selected in 4.2.1 g) to meet the control objectives.
- d) define how to measure the effectiveness of the selected controls or groups of controls and specify how these measurements are to be used to assess control effectiveness to produce comparable and reproducible results (see 4.2.3 c)).
- e) Implement training and awareness programmes (see 5.2.2).
- f) Manage operation of the ISMS.
- g) Manage resources for the ISMS (see 5.2).
- h) Implement procedures and other controls capable of enabling prompt detection of security events and response to security incidents (see 4.2.3 a)).

4.2.3 Monitor and review the ISMS

- a) Execute monitoring and reviewing procedures and other controls.
- b) Undertake regular reviews of the effectiveness of the ISMS (including meeting ISMS policy and objectives, and review of security controls) taking into account results of security audits, incidents, results from effectiveness measurements, suggestions and feedback from all interested parties.
- c) Measure the effectiveness of controls to verify that security requirements have been met.
- d) Review risk assessments at planned intervals and review the residual risks and the identified acceptable levels of risks, taking into account changes.
- e) Conduct internal ISMS audits at planned intervals (see 6).

- f) Undertake a management review of the ISMS on a regular basis to ensure that the scope remains adequate and improvements in the ISMS process are identified (see 7.1).
- g) Update security plans to take into account the findings of monitoring and reviewing activities.
- h) Record actions and events that could have an impact on the effectiveness or performance of the ISMS (see 4.3.3).

4.2.4 *Maintain and improve the ISMS*

- a) Implement the identified improvements in the ISMS.
- b) Take appropriate corrective and preventive actions in accordance with 8.2 and 8.3. Apply the lessons learnt from the security experiences of other organizations and those of the organization itself.
- c) Communicate the actions and improvements to all interested parties with a level of detail appropriate to the circumstances and, as relevant, agree on how to proceed.
- d) Ensure that the improvements achieve their intended objectives.

4.3 Documentation requirements

4.3.1 *General*

Documentation shall include records of management decisions, ensure that actions are traceable to management decisions and policies, and ensure that the recorded results are reproducible.

It is important to be able to demonstrate the relationship from the selected controls back to the results of the risk assessments and risk treatment process, and subsequently back to the ISMS policy and objectives.

The ISMS documentation shall include:

- a) documented statements of the ISMS policy (see 4.2.1 b)) and objectives;
- b) the scope of the ISMS (see 4.2.1 a));
- c) procedures and controls in support of the ISMS;
- d) a description of the risk assessment methodology (see 4.2.1 c));
- e) the risk assessment report (see 4.2.1 c) to 4.2.1 g));
- f) the risk treatment plan (see 4.2.2 b));
- g) documented procedures needed by the organization to ensure the effective planning, operation and control of its information security processes and describe how to measure the effectiveness of controls (see 4.2.3 c));
- h) records required by this International Standard (see 4.3.3);
- i) the Statement of Applicability.

4.3.2 *Control of documents*

Documents required by the ISMS shall be protected and controlled. A documented procedure shall be established to define the management actions needed to:

- a) approve documents for adequacy prior to issue;
- b) review and update documents as necessary and re-approve documents;
- c) ensure that changes and the current revision status of documents are identified;
- d) ensure that relevant versions of applicable documents are available at points of use;
- e) ensure that documents remain legible and readily identifiable;
- f) ensure that documents are available to those who need them, and are transferred, stored and ultimately disposed of in accordance with the procedures applicable to their classification;
- g) ensure that documents of external origin are identified;
- h) ensure that the distribution of documents is controlled;
- i) prevent the unintended use of obsolete documents;
- j) apply suitable identification to them if they are retained for any purpose.

4.3.3 Control of records

Records shall be established and maintained to provide evidence of conformity to requirements and the effective operation of the ISMS. They shall be protected and controlled. The ISMS shall take account of any relevant legal or regulatory requirements and contractual obligations. records shall remain legible, readily identifiable and retrievable. The controls needed for the identification, storage, protection, retrieval, retention time and disposition of records shall be documented and implemented.

Records shall be kept of the performance of the process as outlined in 4.2 and of all occurrences of significant security incidents related to the ISMS. devem ser mantidos afastados do desempenho dos processos, como definido em 4.2 e de todas as ocorrências de incidentes de segurança significativos, relacionados com o SGSI.

5. Management responsibility

5.1 Management commitment

Management shall provide evidence of its commitment to the establishment, implementation, operation, monitoring, review, maintenance and improvement of the ISMS by:

- a) establish an ISMS policy;
- b) ensuring that ISMS objectives and plans are established;
- c) establishing roles and responsibilities for information security;
- d) communicating to the organization the importance of meeting information security objectives and conforming to the information security policy, its responsibilities under the law and the need for continual improvement;
- e) providing sufficient resources to establish, implement, operate, monitor, review, maintain and improve the ISMS (see 5.2.1);
- f) deciding the criteria for accepting risks and the acceptable levels of risk;
- g) ensuring that internal ISMS audits are conducted (see 6);
- h) conducting management reviews of the ISMS (see 7).

5.2 Resource management

5.2.1 Provision of resources

The organization shall determine and provide the resources needed to:

- a) establish, implement, operate, monitor, review, maintain and improve an ISMS;
- b) ensure that information security procedures support the business requirements;
- c) identify and address legal and regulatory requirements and contractual security obligations;
- d) maintain adequate security by correct application of all implemented controls;
- e) carry out reviews when necessary, and to react appropriately to the results of these reviews;
- f) where required, improve the effectiveness of the ISMS.

5.2.2 Training, awareness and competence

The organization shall ensure that all personnel who are assigned responsibilities defined in the ISMS are competent to perform the required tasks by:

- a) determining the necessary competencies for personnel performing work effecting the ISMS;
- b) providing training or taking other actions (e.g. employing competent personnel) to satisfy these needs;
- c) evaluating the effectiveness of the actions taken;
- d) maintaining records of education, training, skills, experience and qualifications (see 4.3.3).

The organization shall also ensure that all relevant personnel are aware of the relevance and importance of their information security activities and how they contribute to the achievement of the ISMS objectives.

6. Internal ISMS audits

The organization shall conduct internal ISMS audits at planned intervals to determine whether the control objectives, controls, processes and procedures of its ISMS:

- a) conform to the requirements of this International Standard and relevant legislation or regulations;
- b) conform to the identified information security requirements;
- c) are effectively implemented and maintained;
- d) perform as expected.

7. Management review of the ISMS

7.1 General

Management shall review the organization's ISMS at planned intervals (at least once a year) to ensure its continuing suitability, adequacy and effectiveness. This review shall include assessing opportunities for improvement and the need for changes to the ISMS, including the information security policy and information security objectives. The results of the reviews shall be clearly documented and records shall be maintained (see 4.3.3).

7.2 Review input

The input to a management review shall include:

- a) results of ISMS audits and reviews;
- b) feedback from interested parties;
- c) techniques, products or procedures, which could be used in the organization to improve the ISMS performance and effectiveness;
- d) status of preventive and corrective actions;
- e) vulnerabilities or threats not adequately addressed in the previous risk assessment;
- f) results from effectiveness measurements;
- g) follow-up actions from previous management reviews;
- h) any changes that could affect the ISMS;
- i) recommendations for improvement.

7.3 Review output

The output from management review shall include any decisions and actions related to the following.

- a) Improvement of the effectiveness of the ISMS.
- b) Update of the risk assessment and risk treatment plan.
- c) Modification of procedures and controls that affect information security, as necessary, to respond to internal or external events that may impact on the ISMS.
- d) Resource needs.
- e) Improvement to how the effectiveness of controls is being measured.

8. ISMS improvement

8.1 Continual improvement

The organization shall continually improve the effectiveness of the ISMS through the use of the information security policy, information security objectives, audit results, analysis of monitored events, corrective and preventive actions and management review (see 7).

8.2 Corrective action

The organization shall take action to eliminate the cause of nonconformities with the ISMS requirements in order to prevent recurrence. The documented procedure for corrective action shall define requirements for:

- a) identifying nonconformities;
- b) determining the causes of nonconformities;
- c) evaluating the need for actions to ensure that nonconformities do not recur;
- d) determining and implementing the corrective action needed;
- e) recording results of action taken (see 4.3.3);
- f) reviewing of corrective action taken.

8.3 Preventive action

The organization shall determine action to eliminate the cause of potential nonconformities with the ISMS requirements in order to prevent their occurrence. Preventive actions taken shall be appropriate to the impact of the potential problems. The documented procedure for preventive action shall define requirements for:

- a) identifying potential nonconformities and their causes;
- b) evaluating the need for action to prevent occurrence of nonconformities;
- c) determining and implementing preventive action needed;
- d) recording results of action taken (see 4.3.3);
- e) reviewing of preventive action taken.

The organization shall identify changed risks and identify preventive action requirements focusing attention on significantly changed risks.

The priority of preventive actions shall be determined based on the results of the risk assessment.

ISO/IEC 21827:2002 – Systems Security Engineering - Capability Maturity Model (SSE-CMM)

6 Model Architecture

The SSE-CMM® is a compilation of the best-known security engineering practices. To understand this model, some background in security engineering is required. This section provides a high level description of security engineering, and then describes how the architecture of the model reflects this basic understanding.

6.1 Security Engineering

6.1.1 What Is Security Engineering?

The drive toward pervasive interconnectivity and interoperability of networks, computers, applications, and even enterprises is creating a more pivotal role for security in all systems and products. The focus of security has moved from safeguarding classified government data, to a wider application, including financial transactions, contractual agreements, personal information, and the Internet. As a result, it is necessary that potential security needs are considered and determined for any application. Examples of needs to consider include confidentiality, integrity, availability, accountability, privacy, and assurance.

6.1.2 Description of Security Engineering

Security engineering is an evolving discipline. As such, a precise definition with community consensus does not exist today. However, some generalizations are possible.

6.1.3 Security Engineering Organizations

Security engineering activities are practised by various types of organizations.

6.1.4 Security Engineering Life Cycle

Security engineering activities are practised during all life cycle phases.

6.1.5 Security Engineering and Other Disciplines

Security engineering activities interface with many other disciplines.

Security engineering activities must be coordinated with many external entities because assurance and the acceptability of residual operational impacts are established in conjunction with the developer, integrator, acquirer, user, independent evaluator, and other groups. It is these interfaces and the requisite interaction across a broad set of organizations that make security engineering particularly complex and different from other engineering disciplines.

6.1.6 Security Engineering Specialties

While Security Engineering and Information Technology Security are very often the driving disciplines in the current security and business environment, other more traditional security disciplines, such as Physical Security and Personnel Security should not be overlooked. Security Engineering will need to draw upon these and many other specialist sub-disciplines if they are to achieve the most efficient and effective results in the performance of their work.

6.2 Security Engineering Process Overview

The SSE-CMM® divides security engineering into three basic areas: risk, engineering, and assurance, see figure 1. While these areas are by no means independent from one another, it is possible to consider them separately. At the simplest level, the risk process identifies and prioritizes dangers inherent to the developed product or system. The security engineering process works with the other engineering disciplines to determine and implement solutions to the problems presented by the dangers. Finally, the assurance process establishes

confidence in the security solutions and conveys this confidence to the customers. Together, these three areas work together with the goal of ensuring that the security engineering process results achieve the goals described above.

6.2.1 Risk

A major goal of security engineering is the reduction of risk. Risk assessment is the process of identifying problems that have not yet occurred. Risks are assessed by examining the likelihood of the threat and vulnerability and by considering the potential impact of an unwanted incident, see figure 2. Associated with that likelihood is a factor of uncertainty, which will vary dependent upon a particular situation. This means that the likelihood can only be predicted within certain limits. In addition, impact assessed for a particular risk also has associated uncertainty, as the unwanted incident may not turn out as expected. Because the factors may have a large amount of uncertainty as to the accuracy of the predictions associated with them, planning and the justification of security can be very difficult. One way to partially deal with this problem in a cost-effective manner is to implement techniques to detect the occurrence of an unwanted incident.

6.2.2 Engineering

Security engineering, like other engineering disciplines, is a process that proceeds through concept, design, implementation, test, deployment, operation, maintenance, and decommission. Throughout this process, security engineers must work closely with the other parts the system engineering team. The SSE-CMM® emphasizes that security engineers are part of a larger team and need to coordinate their activities with engineers from other disciplines. This helps to ensure that security is an integral part of the larger process, and not a separate and distinct activity.

6.2.3 Assurance

Assurance is defined as the degree of confidence that security needs are satisfied [NIST94a]. It is a very important product of security engineering. There are many forms of assurance. The SSE-CMM® contributes to one aspect, the confidence in the repeatability of the results from the security engineering process. The basis for this confidence is that a mature organization is more likely to repeat results than an immature organization, see figure 4. The detailed relationship between different forms of assurance is the subject of ongoing research.

6.3 SSE-CMM® Architecture Description

The SSE-CMM® architecture is designed to enable a determination of a security engineering organization's process maturity across the breadth of security engineering. The goal of the architecture is to clearly separate basic characteristics of the security engineering process from its management and institutionalization characteristics. In order to ensure this separation, the model has two dimensions, called "domain" and "capability" which are described below. Importantly, the SSE-CMM® does not imply that any particular group or role within an organization must do any of the processes described in the model. Nor does it require that the latest and greatest security engineering technique or methodology be used. The model does require, however, that an organization have a process in place that includes the basic security practices described in the model. The organization is free to create their own process and organizational structure in any way that meets their business objectives.

6.3.1 The Basic Model

The SSE-CMM® has two dimensions, "domain" and "capability." The domain dimension is perhaps the easier of the two dimensions to understand. This dimension simply consists of all the practices that collectively define security engineering. These practices are called "base practices." The structure and content of these base practices are discussed below. The capability dimension represents practices that indicate process

management and institutionalization capability. These practices are called "generic practices" as they apply across a wide range of domains. The generic practices represent activities that should be performed as part of doing a base practices.

6.3.2 *The Base Practices*

The SSE-CMM® contains 129 base practices, organized into 22 process areas. Of these 61 base practices, organized in 11 process areas, cover all major areas of security engineering. The remaining 68 base practices, organized in 11 process areas, address the project and organization domains. They have been drawn from the Systems Engineering and Software CMM®. They are required to provide a context and support for the Systems Security Engineering process areas. The base practices for security were gathered from a wide range of existing materials, practice, and expertise. The practices selected represent the best existing practice of the security engineering community, not untested practices.

6.3.3 *The Generic Practices*

Generic practices are activities that apply to all processes. They address the management, measurement, and institutionalization aspects of a process. In general, they are used during an appraisal to determine the capability of an organization to perform a process.

Generic practices are grouped into logical areas called "Common Features" which are organized into five "Capability Levels" which represent increasing organizational capability. Unlike the base practices of the domain dimension, the generic practices of the capability dimension are ordered according to maturity. Therefore, generic practices that indicate higher levels of process capability are located at top of the capability dimension.

6.3.4 *The Capability Levels*

There is more than one way to group practices into common features and common features into capability levels. The following discussion addresses these common features.

The ordering of the common features stems from the observation that implementation and institutionalization of some practices benefit from the presence of others. This is especially true if practices are well established. Before an organization can define, tailor, and use a process effectively, individual projects should have some experience managing the performance of that process. Before institutionalizing a specific estimation process for an entire organization, for example, an organization should first attempt to use the estimation process on a project. However, some aspects of process implementation and institutionalization should be considered together (not one ordered before the other) since they work together toward enhancing capability.

6.3.5 *Capability Dimension / Measurement Framework Mapping*

The capability dimension of the SSE-CMM® and the measurement framework of ISO/IEC 15504-2 differ somewhat in terms of structure, but very little in terms of the detail and intent. In the case of the SSE-CMM® the capability dimension is organized into a number of "capability levels". Each capability level is made up of a number of "common features", which in turn are made up of one or more "generic practices"; see figure 10. In the case of ISO/IEC 15504-2 measurement framework, this is made up of a number of "levels" with each level consisting of a number of process attributes (PA)s.

6.3.6 *Relationship to ISO/IEC CD 15288 - System Life Cycle Processes.*

This International Standard the SSE-CMM® has been developed outside the normal ISO/IEC environment. This means that some differences in the use of terminology and detail exist between ISO/IEC 21827 and ISO/IEC 15288. In addition, ISO/IEC 21827 is targeted at a different domain and discipline, systems security engineering, which inevitably, gives rise to some differences. These differences are minor and are note

where applicable. However, the underlying concepts and approaches used by both ISO/IEC 21827 and ISO/IEC 15288 are very similar.

7. Security Base Practices

This clause contains the base practices, that is, the practices considered essential to the conduct of basic security engineering. Note that the process areas are numbered in no particular order since the SSE-CMM® does not prescribe a specific process or sequence. An organization can be assessed against any one single process area or combination of process areas. The process areas together, however, are intended to cover all base practices for security engineering and there are many inter-relationships between the process areas. At present, the SSE-CMM® comprises 11 security process areas, each of which contains a number of base practices.

7.1 PA01 - Administer Security Controls

7.1.1 Process Area

The purpose of Administer Security Controls is to ensure that the intended security for the system that was integrated into the system design, is in fact achieved by the resultant system in its operational state.

7.1.2 BP.01.01 - Establish Security Responsibilities

Establish responsibilities and accountability for security controls and communicate them to everyone in the organization.

- # Some aspects of security can be managed within the normal management structure, while others require more specialized management.
- # The procedures should ensure that those charged with responsibility are made accountable and empowered to act. It should also ensure that whatever security controls are adopted are clear and consistently applied. In addition, they should ensure that whatever structure is adopted it is communicated, not only to those within the structure, but also the whole organization.

7.1.3 BP.01.02 - Manage Security Configuration

Manage the configuration of system security controls.

- # Security configuration of all devices requires management. This base practice recognizes that system security relies to a great extent on a number of interrelated components (hardware, software, and procedures) and that normal configuration management practices may not capture the interrelated dependencies required for secure systems.

7.1.4 BP.01.03 - Manage Security Awareness, Training, and Education Programs

Manage security awareness, training, and education programs for all users and administrators.

- # The security awareness, training and education of all staff requires management in the same way that other awareness, training and education needs to be managed.

7.1.5 BP.01.04 - Manage Security Services and Control Mechanisms

Manage periodic maintenance and administration of security services and control mechanisms.

- # The general management of security services and mechanisms is similar to other service and mechanism management. This includes the protection of the services and mechanisms from corruption, either accidental or deliberate, and appropriate archival in compliance with legal and policy requirements.

7.2 PA02 - Assess Impact

7.2.1 Process Area

The purpose of Assess Impact is to identify impacts that are of concern with respect to the system and to assess the likelihood of the impacts occurring. Impacts may be tangible, such as the loss of revenue or financial penalties, or intangible, such as loss of reputation or goodwill.

7.2.2 BP.02.01 - Prioritize Capabilities

Identify, analyse, and prioritize operational, business, or mission capabilities leveraged by the system.

Identify, analyse, and prioritize operational, business, or mission directives. The influence of the business strategies should also be considered. These will influence and moderate the impacts to which the organization may be subjected. This in turn is likely to influence the sequence in which risks are addressed in other base practices and process areas. It is therefore important to factor in these influences when the potential impacts are being examined. This base practice is related to the activities of PA01 Specify Security Needs.

7.2.3 BP.02.02 - Identify System Assets

Identify and characterize the system assets that support the key capabilities or the security objectives of the system.

Identify system resources and data necessary to support the security objectives or the key capabilities (operational, business, or mission functions) of the system. Define each of these assets by assessing the significance of each asset in providing such support within a defined environment.

7.2.4 BP.02.03 - Select Impact Metric(s)

Select the impact metric(s) to be used for this assessment.

A number of metrics can be used to measure the impact of an event. It is advantageous to predetermine which metrics will be used for the particular system under consideration.

7.2.5 BP.02.04 - Identify Metric Relationship

Identify the relationship between the selected metrics for this assessment and metric conversion factors if required.

Some impacts may need to be assessed using different metrics. The relationship between different metrics needs to be established to ensure a consistent approach for all exposures throughout the impact assessment. In some cases it will be necessary to combine metrics to be able to produce a single consolidated result. Thus an approach for consolidation needs to be established. This will usually vary on a system to system basis. When qualitative metrics are in use, rules also need to be established to guide the combination of qualitative factors during the consolidation phase.

7.2.6 BP.02.05 - Identify and Characterize Impacts

Identify and characterize the unwanted impacts of unwanted incidents with either multiple metrics or consolidated metrics as appropriate.

Starting with the assets and capabilities identified in BP.02.01 and BP.02.02, identify the consequences that would cause harm. For each asset, these might include corruption, disclosure, obstruction, or disappearance. Unwanted impacts to capabilities might include interruption, delay, or weakening.

Once a relatively complete list has been created, the impacts can be characterized using the metrics identified in BP.02.03 and BP.02.04. This step may require some research into actuarial tables, almanacs, or other sources. The uncertainty in the metrics should also be captured and associated with each impact.

7.2.7 BP.02.06 - Monitor Impacts

Monitor ongoing changes in the Impacts.

- # The impacts applicable to any location and situation are dynamic. New impacts can become relevant. It is therefore important to monitor both existing impacts and to check for the potential for new impacts on a regular basis. This base practice is closely linked to the generalized monitoring activity in BP.07.02.

7.3 PA03 - Assess Security Risk

7.3.1 Process Area

The purpose of Assess Security Risk is to identify the security risks involved with relying on a system in a defined environment. This process area focuses on ascertaining these risks based on an established understanding of how capabilities and assets are vulnerable to threats. Specifically, this activity involves identifying and assessing the likelihood of the occurrence of exposures. "Exposure" refers to a combination of a threat, vulnerability, and impact that could cause significant harm. This set of activities is performed any time during a system's life cycle to support decisions related to developing, maintaining, or operating the system within a known environment.

7.3.2 BP.03.01 - Select Risk Analysis Method

Select the methods, techniques, and criteria by which security risks, for the system in a defined environment are analysed, assessed, compared, and prioritized.

- # This base practice consists of defining the method for identifying security risks for the system in a defined environment in a way that permits them to be analysed, assessed, and compared. This should include a scheme for categorizing and prioritizing the risks based on threats, operational functions, established system vulnerabilities, potential loss, security requirements, or areas of concern.

7.3.3 BP.03.02 - Exposure Identification

Identify threat/vulnerability/impact triples (exposures).

- # The purpose of identifying the exposures is to recognize which of the threats and vulnerabilities are of concern and to identify the impact of an occurrence of the threat and vulnerability. These are the exposures that will need to be considered in the selection of safeguards to protect the system.

7.3.4 BP.03.03 - Assess Exposure Risk

Assess the risk associated with each exposure.

- # Identify the likelihood of the occurrence of an exposure.

7.3.5 BP.03.04 - Assess Total Uncertainty

Assess the total uncertainty associated with the risk for the exposure.

- # Each risk will have uncertainty associated with it. The total risk uncertainty is a cumulation of the uncertainties that have been identified for the threats, vulnerabilities, and impacts and their characteristics in BP.04.05 "Assess the likelihood of an occurrence of a threat event;" BP.05.03, Gather data related to the properties of the vulnerabilities; and BP.02.05, Assess impact of the realization of an exposure. This base practice is closely associated with the activities of PA06 Build Assurance Argument as assurance can be used to modify, and in some cases reduce uncertainty.

7.3.6 BP.03.05 - Prioritize Risks

Order risks by priority.

- # The risks that have been identified should be ordered based on the organization priorities, likelihood of occurrence, uncertainty associated with them and funds available. A risk can be mitigated, avoided, transferred or accepted. Combinations of these can also be used. The mitigation can address the threat, vulnerability, impact, or

the risk itself. Actions should be selected with due regard to the stakeholders needs as identified in PA01 Specify Security Needs, business priorities, and the overall system architecture.

7.3.7 BP.03.06 - Monitor Risks and Their Characteristics

Monitor ongoing changes in the risk spectrum and changes to their characteristics.

- # The risk spectrum applicable to any location and situation is dynamic. New risks can become relevant and the characteristics of existing risks can change. It is therefore important to monitor both existing risks and their characteristics, and to check for new risks on a regular basis. This base practice is closely linked to the generalized monitoring activity in BP.07.02 Monitor changes in threats, vulnerabilities, impacts, risks and the environment.

7.4 PA04 - Assess Threat

7.4.1 Process Area

The purpose of the Assess Threat process area is to identify security threats and their properties and characteristics.

7.4.2 BP.04.01 - Identify Natural Threats

Identify applicable threats arising from a natural source.

- # Threats arising from natural sources include earthquakes, tsunamis, and tornadoes. However, not all natural based threats can occur in all locations. For example it is not possible for a tsunami to occur in the centre of a large continent. Thus it is important to identify which natural based threats can occur in a specific location.

7.4.3 BP.04.02 - Identify Man-made Threats

Identify applicable threats arising from man-made sources, either accidental or deliberate.

- # Threats arising from man-made sources require a somewhat different type of approach. There are basically two types of man-made threats: those that arise from accidental sources and those that result from a deliberate act. Some man-made threats may not be applicable in the target environment. These should be eliminated from further considerations in the analysis.

7.4.4 BP.04.03 - Identify Threat Units of Measure

Identify appropriate units of measure, and applicable ranges, in a specified environment.

- # The majority of natural threats and many man-made threats have units of measure associated with them. An example is the Richter scale for earthquakes. In most cases the total range of the unit of measure will not be applicable in a particular location. It is therefore appropriate to establish the maximum, and in some cases the minimum, occurrence of an event that can occur in the particular location under consideration.

7.4.5 BP.04.04 - Assess Threat Agent Capability

Assess capability and motivation of threat agent for threats arising from man-made sources.

- # This process area focuses on the determination of a potential human adversary's ability and capability of executing a successful attack against the system. Ability addresses the adversaries knowledge of attacks (e.g. do they have the training / knowledge). Capability is a measure of the likelihood that an able adversary can actually execute the attack (e.g. do they have the resources).

7.4.6 BP.04.05 - Assess Threat Likelihood

Assess the likelihood of an occurrence of a threat event.

- # Assess how likely a threat event is to occur. Many factors need to be considered in making this assessment ranging from the chance occurrence of a natural event to the deliberate or accidental act of an individual. Many of the factors to be considered do

not lend themselves to calculation or measurement. A consistent metric for reporting is desirable.

7.4.7 BP.04.06 - Monitor Threats and Their Characteristics

Monitor ongoing changes in the threat spectrum and changes to their characteristics.

- # The threat spectrum applicable to any location and situation is dynamic. New threats can become relevant and the characteristics of existing threats can change. It is therefore important to monitor both existing threats and their characteristics, and to check for new threats on a regular basis. This base practice is closely linked to the generalized monitoring activity in BP.07.02 Monitor changes in threats, vulnerabilities, impacts, risks and the environment.

7.5 PA05 - Assess Vulnerability

7.5.1 Process Area

The purpose of Assess Vulnerability is to identify and characterize system security vulnerabilities. This process area includes analysing system assets, defining specific vulnerabilities, and providing an assessment of the overall system vulnerability. The terms associated with security risk and vulnerability assessment are used differently in many contexts. For the purposes of this model, "vulnerability" refers to an aspect of a system that can be exploited for purposes other than those originally intended, weaknesses, security holes, or implementation flaws within a system that are likely to be attacked by a threat. These vulnerabilities are independent of any particular threat instance or attack. This set of activities is performed any time during a system's life-cycle to support the decision to develop, maintain, or operate the system within the known environment.

7.5.2 BP.05.01 - Select Vulnerability Analysis Method

Select the methods, techniques, and criteria by which system security vulnerabilities in a defined environment are identified and characterized.

- # This base practice consists of defining the method for establishing security vulnerabilities for the system in a way that permits them to be identified and characterized. This may include a scheme for categorizing and prioritizing the vulnerabilities based on threats and their likelihood, operational functions, security requirements, or other areas of concern when provided. Identifying the depth and breadth of the analysis allows the security engineers and the customer to determine target systems to be part of the exercise and its comprehensiveness. Analysis should be performed within the framework of a known and recorded configuration during a prearranged and specified time period. The methodology for the analysis should include expected results. Specific objectives for the analysis should be clearly stated.

7.5.3 BP.05.02 - Identify Vulnerabilities

Identify system security vulnerabilities.

- # System vulnerabilities may be found in both security and non-security related parts of the system. In many cases, non-security mechanisms that support security functions or work in concert with security mechanisms are found to have exploitable vulnerabilities. The methodology of attack scenarios as developed in BP.05.01 should be followed to the extent that vulnerabilities are validated. All system vulnerabilities discovered should be recorded.

7.5.4 BP.05.03 - Gather Vulnerability Data

Gather data related to the properties of the vulnerabilities.

- # Vulnerabilities have properties associated with them. The intent of this base practice is to gather data associated with those properties. In some cases a vulnerability may have a unit of measure similar to those associated with threats, see BP.04.03 Identify

Threat Unit of Measure. The ease with which the vulnerability can be exploited and the likelihood that the vulnerability exists should be identified and gathered.

7.5.5 BP.05.04 - *Synthesize System Vulnerability*

Assess the system vulnerability and aggregate vulnerabilities that result from specific vulnerabilities and combinations of specific vulnerabilities.

- # Analyse which vulnerabilities or combination of vulnerabilities result in problems for the system. Analysis should identify additional characteristics of the vulnerability, such as the likelihood of vulnerability exploitation and the chance for successful exploitation. Recommendations for addressing the synthesized vulnerabilities may also be included in the results.

7.5.6 BP.05.05 - *Monitor Vulnerabilities and Their Characteristics*

Monitor ongoing changes in the applicable vulnerabilities and changes to their characteristics.

- # The vulnerability spectrum applicable to any location and situation is dynamic. New vulnerabilities can become relevant and the characteristics of existing vulnerabilities can change. It is therefore important to monitor both existing vulnerabilities and their characteristics, and to check for new vulnerabilities on a regular basis. This base practice is closely linked to the generalized monitoring activity in BP.07.02 Monitor changes in threats, vulnerabilities, impacts, risks and the environment.

PA06 – Construir Argumentos do Grau de Conforto (7.6)

7.6.1 *Process Area*

The purpose of Build Assurance Argument is to clearly convey that the customer's security needs are met. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple sources and levels of abstraction.

This process includes identifying and defining assurance related requirements; evidence production and analysis activities; and additional evidence activities needed to support assurance requirements. Additionally, the evidence generated by these activities is gathered, packaged, and prepared for presentation.

7.6.2 BP.06.01 - *Identify Assurance Objectives*

Identify the security assurance objectives.

- # Assurance objectives as determined by the customer, identify the level of confidence needed in the system. The system security assurance objectives specify a level of confidence that the system security policy is enforced. Adequacy of the objectives is determined by the developer, integrator, customer, and those who will approve the operation of the system, if any.
- # Identification of new, and modification to existing, security assurance objectives are coordinated with all security-related groups internal to the engineering organization and groups external to the engineering organization (e.g., customer, systems security certifier, user).
- # The security assurance objectives are updated to reflect changes. Examples of changes requiring a modification in security assurance objectives include changes in the level of acceptable risk by the customer, system security certifier, or user, or changes in the requirements or interpretations of the requirements.
- # Security assurance objectives must be communicated so as to be unambiguous. Applicable interpretations are included or developed if necessary.

7.6.3 BP.06.02 - *Define Assurance Strategy*

Define a security assurance strategy to address all assurance objectives.

- # The purpose of a security assurance strategy is to plan for and ensure that the security objectives are implemented and enforced correctly. Evidence produced through the

implementation of a security assurance strategy should provide an acceptable level of confidence that the system security measures are adequate to manage the security risk. Effective management of the assurance related activities is achieved through the development and enactment of a security assurance strategy. Early identification and definition of assurance related requirements is essential to producing the necessary supporting evidence. Understanding and monitoring the satisfaction of customer assurance needs through continuous external coordination ensures a high quality assurance package.

7.6.4 BP.06.03 - Control Assurance Evidence

Identify and control security assurance evidence.

- # Security assurance evidence is gathered as defined in the security assurance strategy through interaction with all security engineering process areas to identify evidence at various levels of abstraction. This evidence is controlled to ensure currency with existing work products and relevancy with security assurance objectives.

7.6.5 BP.06.04 - Analyse Evidence

Perform analysis of security assurance evidence.

- # Assurance evidence analysis is conducted to provide confidence that the evidence that is collected meets the security objectives, thus satisfying the customer's security needs. An analysis of the assurance evidence determines if system security engineering and security verification processes are adequate and complete enough to conclude that the security features and mechanisms are satisfactorily implemented. Additionally, the evidence is analysed to ensure that the engineering artifacts are complete and correct with respect to the baseline system. In the event of insufficient or inadequate assurance evidence, this analysis may necessitate revisions to the system, security work products and processes that support the security objectives.

7.6.6 BP.06.05 - Provide Assurance Argument

Provide a security assurance argument that demonstrates the customer's security needs are met.

- # An overall assurance argument is developed to demonstrate compliance with security assurance objectives and provided to the customer. An assurance argument is a set of stated assurance objectives that are supported by a combination of assurance evidence that may be derived from multiple levels of abstraction. The assurance argument should be reviewed for deficiencies in the presentation of evidence as well as for deficiencies in meeting security assurance objectives.

7.7 PA07 - Coordinate Security

7.7.1 Process Area

The purpose of Coordinate Security is to ensure that all parties are aware of and involved with security engineering activities. This activity is critical as security engineering cannot succeed in isolation. This coordination involves maintaining open communications between all project personnel and external groups. Various mechanisms may be used to coordinate and communicate the security engineering decisions and recommendations between these parties, including memoranda, documents, e-mail, meetings, and working groups.

7.7.2 BP.07.01 - Define Coordination Objectives

Define security engineering coordination objectives and relationships.

- # Many groups need to be aware of and involved with security engineering activities. The objectives for sharing information with these groups is determined by examining the project structure, information needs, and project requirements. Relationships and commitments with the other groups are established. Successful relationships take many forms, but must be acknowledged by all the involved parties.

7.7.3 BP.07.02 - Identify Coordination Mechanisms

Identify coordination mechanisms for security engineering.

- # There are many ways that the security engineering decisions and recommendations can be shared with all engineering groups. This activity identifies the different ways that security is coordinated on a project.
- # It is not uncommon to have multiple security personnel working on the same project. In these situations, all security engineers should be working toward a commonly understood goal. Interface identification, security mechanism selection, training and development efforts need to be conducted in such a way as to ensure that each security component operates as expected when placed in the operational system. Additionally, all engineering teams must understand the security engineering efforts and engineering activities, to allow for clean integration of security into the system. The customer must also be aware of events and activities related to security to ensure that requirements are identified and addressed appropriately.

7.7.4 BP.07.03 - Facilitate Coordination

Facilitate security engineering coordination.

- # Successful relationships rely on good facilitation. Communication between different groups with different priorities may result in conflicts. This base practice ensures that disputes are resolved in an appropriate productive manner.

7.7.5 BP.07.04 - Coordinate Security Decisions and Recommendations

Use the identified mechanisms to coordinate decisions and recommendations related to security.

- # The purpose of this base practice is to communicate security decisions and recommendations among the various security engineers, other engineering groups, external entities, and other appropriate parties.

7.8 PA08 - Monitor Security Posture

7.8.1 Process Area

The purpose of Monitor Security Posture is to ensure that all breaches of, attempted breaches of, or mistakes that could potentially lead to a breach of security are identified and reported. The external and internal environments are monitored for all factors that may have an impact on the security of the system.

7.8.2 BP.08.01 - Analyse Event Records

Analyse event records to determine the cause of an event, how it proceeded, and likely future events.

- # Examine historical and event records (compositions of log records) for security relevant information. The events of interest should be identified along with the factors used to correlate events among multiple records. Multiple event records can then be fused into a single event record.

7.8.3 BP.08.02 - Monitor Changes

Monitor changes in threats, vulnerabilities, impacts, risks, and the environment.

- # Look for any changes that may impact the effectiveness of the current security posture, either positively or negatively.
- # The security implemented for any system should be in relation to the threats, vulnerabilities, impacts and risks as they relate to its environment both internal and external. None of these are static and changes influence both the effectiveness and appropriateness of the system's security. All must be monitored for change, and the changes analysed to assess their significance with regard to the effectiveness of the security.

7.8.4 BP.08.03 - Identify Security Incidents

Identify security relevant incidents.

- # Determine if a security relevant incident has occurred, identify the details, and make a report if necessary. Security relevant incidents may be detected using historical event data, system configuration data, integrity tools, and other system information. Since some incidents occur over a long period of time, this analysis is likely to involve comparison of system states over time.

7.8.5 BP.08.04 - Monitor Security Safeguards

Monitor the performance and functional effectiveness of security safeguards.

- # Monitor the performance and functional effectiveness of security safeguards.

7.8.6 BP.08.05 - Review Security Posture

Review the security posture of the system to identify necessary changes.

- # The security posture of a system is subject to change based on the threat environment, operational requirements, and system configuration. This practice re-examines the reasons why security was put in place and the requirements security places on other disciplines.

7.8.7 BP.08.06 - Manage Security Incident Response

Manage the response to security relevant incidents.

- # In many cases, the continued availability of systems is critical. Many events can not be prevented, thus the ability to respond to disruption is essential. A contingency plan requires the identification of the maximum period of non-functionality of the system; the identification of the essential elements of the system for functionality; the identification and development of a recovery strategy and plan; testing of the plan; the maintenance of the plan.
- # In some cases contingencies may include incident response and active engagement of hostile agents (e.g. viruses, hackers etc.).

7.8.8 BP.08.07 - Protect Security Monitoring Artifacts

Ensure that the artifacts related to security monitoring are suitably protected.

- # If the products of monitoring activities can not be depended upon they are of little value. This activity includes the sealing and archiving of related logs, audit reports and related analysis.

7.9 PA09 - Provide Security Input

7.9.1 Process Area

The purpose of Provide Security Input is to provide system architects, designers, implementers, or users with the security information they need. This information includes security architecture, design, or implementation alternatives and security guidance. The input is developed, analysed, provided to and coordinated with the appropriate organization members based on the security needs identified in PA01 Specify Security Needs.

7.9.2 BP.09.01 - Understand Security Input Needs

Work with designers, developers, and users to ensure that appropriate parties have a common understanding of security input needs.

- # Security engineering is coordinated with other disciplines to determine the types of security input that are helpful to those disciplines. Security input includes any sort of guidance, designs, documents, or ideas related to security that should be considered by other disciplines. Input can take many forms, including documents, memoranda, e-mail, training, and consultation.

- # This input is based on the needs determined in PA01 Specify Security Needs. For example, a set of security rules may need to be developed for the software engineers. Some of the inputs are more related to the environment than the system.

7.9.3 BP.09.02 - Determine Security Constraints and Considerations

Determine the security constraints and considerations needed to make informed engineering choices.

- # The purpose of this base practice is to identify all the security constraints and considerations needed to make informed engineering choices. The security engineering group performs analysis to determine any security constraints and considerations on the requirements, design, implementation, configuration, and documentation. Constraints may be identified at all times during the system's life. They may be identified at many different levels of abstraction. Note that these constraints can be either positive (always do this) or negative (never do this).

7.9.4 BP.09.03 - Identify Security Alternatives

Identify solutions to security related engineering problems.

- # The purpose of this base practice is to identify alternative solutions to security related engineering problems. This process is iterative and transforms security related requirements into implementations. These solutions can be provided in many forms, such as architectures, models, and prototypes. This base practice involves decomposing, analysing, and recomposing security related requirements until effective alternative solutions are identified.

7.9.5 BP.09.04 - Analyse Security of Engineering Alternatives

Analyse and prioritize engineering alternatives using security constraints and considerations.

- # The purpose of this base practice is to analyse and prioritize engineering alternatives. Using the security constraints and considerations identified when determining security constraints and considerations (BP.02.02), security engineers can evaluate each engineering alternative and come up with a recommendation for the engineering group. The security engineers should also consider the engineering guidance from other engineering groups.
- # If the products of monitoring activities can not be depended upon they are of little value. This activity includes the sealing and archiving of related logs, audit reports and related analysis.

7.9.6 BP.09.05 - Provide Security Engineering Guidance

Provide security related guidance to engineering groups.

- # The purpose of this base practice is to develop security related guidance and provide it to the engineering groups. Security engineering guidance is used by the engineering groups to make decisions about architecture, design, and implementation choices.

7.9.7 BP.09.06 - Provide Operational Security Guidance

Provide security related guidance to operational system users and administrators.

- # The purpose of this base practice is to develop security related guidance and provide it to system users and administrators. This operational guidance tells the users and administrators what must be done to install, configure, operate, and decommission the system in a secure manner. To ensure that this is possible, the development of the operational security guidance should start early in the life cycle.

7.10 PA10 - Specify Security Needs

7.10.1 Process Area

The purpose of Specify Security Needs is to explicitly identify the needs related to security for the system. Specify Security Needs involves defining the basis for security

in the system in order to meet all legal, policy, and organizational requirements for security. These needs are tailored based upon the target operational security context of the system, the current security and systems environment of the organization, and a set of security objectives are identified. A set of security-related requirements is defined for the system that becomes the baseline for security within the system upon approval.

7.10.2 BP.10.01 - Gain Understanding of Customer's Security Needs

Gain an understanding of the customer's security needs.

- # The purpose of this base practice is to collect all information necessary for a comprehensive understanding of the customer's security needs. These needs are influenced by the importance to the customer of security risk. The target environment in which the system is intended to operate also influences the customer's needs with regard to security.

7.10.3 BP.10.02 - Identify Applicable Laws, Policies, And Constraints

Identify the laws, policies, standards, external influences and constraints that govern the system.

- # The purpose of this base practice is to gather all external influences which affect the security of the system. A determination of applicability should identify the laws, regulations, policies and commercial standards which govern the target environment of the system. A determination of precedence between global and local policies should be performed. Requirements for security placed on the system by the system customer must be identified and the security implications extracted.

7.10.4 BP.10.03 - Identify System Security Context

Identify the purpose of the system in order to determine the security context.

- # The purpose of this base practice is to identify how the system's context impacts security. This involves understanding the purpose of the system (for example, intelligence, financial, medical). Mission processing and operations scenarios are assessed for security considerations. A high-level understanding of the threat to which the system is or may be subject to is required at this stage. Performance and functional requirements are assessed for possible impacts on security. Operating constraints are also reviewed for their security implications.
- # The environment might also include interfaces with other organizations or systems in order to define the security perimeter of the system. Interface elements are determined to be either inside or outside of the security perimeter.
- # Many factors external to the organization also influence to varying degrees the security needs of the organization. These factors include the political orientation and changes in political focus, technology developments, economic influences, global events, and Information Warfare activities. As none of these factors are static they require monitoring and periodic assessment of the potential impact of change.

7.10.5 BP.10.04 - Capture Security View of System Operation

Capture a high-level security oriented view of the system operation.

- # The purpose of the base practice is to develop a high-level security oriented view of the enterprise, including roles, responsibilities, information flow, assets, resources, personnel protection, and physical protection. This description should include a discussion of how the enterprise can be conducted within the constraints of the system requirements. This view of the system is typically provided in a security concept of operations and should include a high-level security view of the system architecture, procedures, and the environment. Requirements related to the system development environment are also captured at this stage.

7.10.6 BP.10.05 - Capture Security High-Level Goals

Capture high-level goals that define the security of the system.

- # The purpose of this base practice is to identify what security objectives should be met to provide adequate security for the system in its operational environment. The assurance objectives of the system, determined in PA06 Build Assurance Argument may influence the security objectives.

7.10.7 BP.10.06 - Define Security Related Requirements

Define a consistent set of requirements which define the protection to be implemented in the system.

- # The purpose of this base practice is to define the security-related requirements of the system. The practice should ensure each requirement is consistent with the applicable policy, laws, standards, requirements for security and constraints on the system. These requirements should completely define the security needs of the system including those requirements to be provided through non-technical means. It is normally necessary to define or specify the boundary of the target, logical or physical, to ensure that all aspects are addressed. The requirements should be mapped or related to the objectives of the system. The security-related requirements should be clearly and concisely stated and should not contradict one another. Security should, whenever possible, minimize any impact on the system functionality and performance. The security-related requirements should provide a basis for evaluating the security of the system in its target environment.

7.10.8 BP.10.07 - Obtain Agreement On Security

Obtain agreement that the specified security requirements match the customer's needs.

- # The purpose of this base practice is to obtain concurrence between all applicable parties on the security requirements. In cases where a generic group is identified, rather than a specific customer, the requirements should satisfy the objectives set. The specified security requirements should be a complete and consistent reflection of governing policy, laws, and customer needs. Issues should be identified and reworked until concurrence is gained.

7.11 PA11 - Verify and Validate Security

7.11.1 Process Area

The purpose of Verify and Validate Security is to ensure that solutions verified and validated with respect to security. Solutions are verified against the security requirements, architecture, and design using observation, demonstration, analysis, and testing. Solutions are validated against the customer's operational security needs.

7.11.2 BP.11.01 - Identify Verification and Validation Targets

Identify the solution to be verified and validated.

- # The purpose of this base practice is to identify the targets of the verification and validation activities, respectively. Verification demonstrates that the solution is correctly implemented, while validation demonstrates that the solution is effective. This involves coordination with the all the engineering groups throughout the life cycle.

7.11.3 BP.11.02 - Define Verification and Validation Approach

Define the approach and level of rigour for verifying and validating each solution.

- # The purpose of this base practice is to define the approach and level of rigour for verifying and validating each solution. Identifying the approach involves selecting how each requirement is verified and validated. The level of rigour should indicate how intense the scrutiny of the verification and validation effort should be and is influenced by the output of the assurance strategy from PA06 Build Assurance Argument. For example, some projects may require a cursory inspection for compliance with the requirements and others may require much more rigorous examination.

- # The methodology should also include a means to maintain traceability from customer's operational security needs to security requirements to solutions to validation and verification results.

7.11.4 BP.11.03 - Perform Verification

Verify that the solution implements the requirements associated with the previous level of abstraction.

- # The purpose of this base practice is to verify that the solution is correct by showing that it implements the requirements associated with the previous level of abstraction including the assurance requirements identified as a result of PA06 Build Assurance Argument. There are many methods of verifying requirements, including testing, analysis, observation, and demonstration. The method to be used is identified in BP.03.02. Both the individual requirements and the overall system are examined.

7.11.5 BP.11.04 - Perform Validation

Validate the solution by showing that it satisfies the needs associated with the previous level of abstraction, ultimately meeting the customer's operational security needs.

- # The purpose of this base practice is to validate that the solution satisfies the needs associated with the previous level of abstraction. Validation demonstrates that the solution meets these needs effectively. There are many ways to validate that these needs have been met, including testing the solution in an operational or representative test setting. The method to be used is identified in BP.03.02.

7.11.6 BP.11.05 - Provide Verification and Validation Results

Capture the verification and validation results for engineering groups.

- # The purpose of this base practice is to capture and provide the verification and validation results. The verification and validation results should be provided in a way that is easy to understand and use. The results should be tracked so that the traceability from needs, to requirements, to solution, and to test results is not lost.

SP800-12 – An Introduction to Computer Security: The NIST Handbook

2 ELEMENTS OF COMPUTER SECURITY

2.1 Computer Security Supports the Mission of the Organization

The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as thwarting the mission of the organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake they are put in place to protect important assets and thereby support the overall organizational mission.

2.2 Computer Security is an Integral Element of Sound Management

Information and computer systems are often critical assets that support the mission of an organization. Protecting them can be as critical as protecting other organizational resources, such as money, physical assets, or employees.

2.3 Computer Security Should Be Cost-Effective

The costs and benefits of security should be carefully examined in both monetary and nonmonetary terms to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the computer systems and to the severity, probability and extent of potential harm. Requirements for security vary, depending upon the particular computer system.

2.4 Computer Security Responsibilities and Accountability Should Be Made Explicit

The responsibilities and accountability of owners, providers, and users of computer systems and other parties concerned with the security of computer systems should be explicit. The assignment of responsibilities may be internal to an organization or may extend across organizational boundaries.

2.5 Systems Owners Have Security Responsibilities Outside Their Own Organizations

If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of security measures so that other users can be confident that the system is adequately secure. (This does not imply that all systems must meet any minimum level of security, but does imply that system owners should inform their clients or users about the nature of the security).

2.6 Computer Security Requires a Comprehensive and Integrated Approach

Providing effective computer security requires a comprehensive approach that considers a variety of areas both within and outside of the computer security field. This comprehensive approach extends throughout the entire information life cycle.

2.6.1 Interdependencies of Security Controls

To work effectively, security controls often depend upon the proper functioning of other controls. In fact, many such interdependencies exist. If appropriately chosen, managerial, operational, and technical controls can work together synergistically. On the other hand, without a firm understanding of the interdependencies of security controls, they can actually undermine one another.

2.6.2 Other Interdependencies

The effectiveness of security controls also depends on such factors as system management, legal issues, quality assurance, and internal and management controls. Computer security needs to work with traditional security disciplines including physical

and personnel security. Many other important interdependencies exist that are often unique to the organization or system environment. Managers should recognize how computer security relates to other areas of systems and organizational management.

2.7 Computer Security Should Be Periodically Reassessed

Computers and the environments they operate in are dynamic. System technology and users, data and information in the systems, risks associated with the system and, therefore, security requirements are ever-changing. Many types of changes affect system security: technological developments (whether adopted by the system owner or available for use by others); connecting to external networks; a change in the value or use of information; or the emergence of a new threat.

2.8 Computer Security is Constrained by Societal Factors

The ability of security to support the mission of the organization(s) may be limited by various factors, such as social issues. For example, security and workplace privacy can conflict. Commonly, security is implemented on a computer system by identifying users and tracking their actions. However, expectations of privacy vary and can be violated by some security measures. (In some cases, privacy may be mandated by law.)

3 ROLES AND RESPONSIBILITIES

This chapter is intended to give the reader a basic familiarity with the major organizational elements that play a role in computer security. It does not describe all responsibilities of each in detail, nor will this chapter apply uniformly to all organizations. Organizations, like individuals, have unique characteristics, and no single template can apply to all.

3.1 Senior Management

Ultimately, responsibility for the success of an organization lies with its senior managers. They establish the organization's computer security program and its overall program goals, objectives, and priorities in order to support the mission of the organization. Ultimately, the head of the organization is responsible for ensuring that adequate resources are applied to the program and that it is successful. Senior managers are also responsible for setting a good example for their employees by following all applicable security practices.

3.2 Computer Security Management

The Computer Security Program Manager (and support staff) directs the organization's day-to-day management of its computer security program. This individual is also responsible for coordinating all security-related interactions among organizational elements involved in the computer security program as well as those external to the organization.

3.3 Program and Functional Managers/Application Owners

Program or Functional Managers/Application Owners are responsible for a program or function (e.g., procurement or payroll) including the supporting computer system. Their responsibilities include providing for appropriate security, including management, operational, and technical controls. These officials are usually assisted by a technical staff that oversees the actual workings of the system. This kind of support is no different for other staff members who work on other program implementation issues.

3.4 Technology Providers

- *System Management/System Administrators*. These personnel are the managers and technicians who design and operate computer systems.
- *Communications/Telecommunications Staff*. This office is normally responsible for providing communications services, including voice, data, video, and fax service.
- *System Security Manager/Officers*. Often assisting system management officials in this effort is a system security manager/officer responsible for day-to-day security implementation/administration duties.

- *Help Desk*. Whether or not a Help Desk is tasked with incident handling, it needs to be able to recognize security incidents and refer the caller to the appropriate person or organization for a response.

3.5 Supporting Functions

The security responsibilities of managers, technology providers and security officers are supported by functions normally assigned to others. Some of the more important of these are described below.

- *Audit*. Auditors are responsible for examining systems to see whether the system is meeting stated security requirements, including system and organization policies, and whether security controls are appropriate. Informal audits can be performed by those operating the system under review or, if impartiality is important, by outside auditors.
- *Physical Security*. The physical security office is usually responsible for developing and enforcing appropriate physical security controls, in consultation with computer security management, program and functional managers, and others, as appropriate. Physical security should address not only central computer installations, but also backup facilities and office environments. In the government, this office is often responsible for the processing of personnel background checks and security clearances.
- *Disaster Recovery/Contingency Planning Staff*. Some organizations have a separate disaster recovery/contingency planning staff. In this case, they are normally responsible for contingency planning for the organization as a whole, and normally work with program and functional managers/application owners, the computer security staff, and others to obtain additional contingency planning support, as needed.
- *Quality Assurance*. Many organizations have established a quality assurance program to improve the products and services they provide to their customers. The quality officer should have a working knowledge of computer security and how it can be used to improve the quality of the program, for example, by improving the integrity of computer-based information, the availability of services, and the confidentiality of customer information, as appropriate.
- *Procurement*. The procurement office is responsible for ensuring that organizational procurements have been reviewed by appropriate officials. The procurement office cannot be responsible for ensuring that goods and services meet computer security expectations, because it lacks the technical expertise. Nevertheless, this office should be knowledgeable about computer security standards and should bring them to the attention of those requesting such technology.
- *Training Office*. An organization has to decide whether the primary responsibility for training users, operators, and managers in computer security rests with the training office or the computer security program office. In either case, the two organizations should work together to develop an effective training program.
- *Personnel*. The personnel office is normally the first point of contact in helping managers determine if a security background investigation is necessary for a particular position. The personnel and security offices normally work closely on issues involving background investigations. The personnel office may also be responsible for providing security-related exit procedures when employees leave an organization.
- *Risk Management/Planning Staff*. Some organizations have a full-time staff devoted to studying all types of risks to which the organization may be exposed. This function should include computer security-related risks, although this office normally focuses on "macro" issues. Specific risk analyses for specific computer systems is normally not performed by this office.
- *Physical Plant*. This office is responsible for ensuring the provision of such services as electrical power and environmental controls, necessary for the safe and secure operation of an organization's systems. Often they are augmented by separate medical, fire, hazardous waste, or life safety personnel.

3.6 Users

Users also have responsibilities for computer security. Two kinds of users, and their associated responsibilities, are described below.

- *Users of Information.* Individuals who use information provided by the computer can be considered the "consumers" of the applications. Sometimes they directly interact with the system (e.g., to generate a report on screen) in which case they are also users of the system (as discussed below). Other times, they may only read computer-prepared reports or only be briefed on such material. Some users of information may be very far removed from the computer system. Users of information are responsible for letting the functional managers/application owners (or their representatives) know what their needs are for the protection of information, especially for its integrity and availability.
- *Users of Systems.* Individuals who directly use computer systems (typically via a keyboard) are responsible for following security procedures, for reporting security problems, and for attending required computer security and functional training.

4 COMMON THREATS: A BRIEF OVERVIEW

This chapter presents a broad view of the risky environment in which systems operate today. The threats and associated losses presented in this chapter were selected based on their prevalence and significance in the current computing environment and their expected growth. This list is not exhaustive, and some threats may combine elements from more than one area. This overview of many of today's common threats may prove useful to organizations studying their own threat environments; however, the perspective of this chapter is very broad. Thus, threats against particular systems could be quite different from those discussed here.

4.1 Errors and Omissions

Errors and omissions are an important threat to data and system integrity. These errors are caused not only by data entry clerks processing hundreds of transactions per day, but also by all types of users who create and edit data. Many programs, especially those designed by users for personal computers, lack quality control measures. However, even the most sophisticated programs cannot detect all types of input errors or omissions. A sound awareness and training program can help an organization reduce the number and severity of errors and omissions.

4.2 Fraud and Theft

Computer systems can be exploited for both fraud and theft both by "automating" traditional methods of fraud and by using new methods. For example, individuals may use a computer to skim small amounts of money from a large number of financial accounts, assuming that small discrepancies may not be investigated. Financial systems are not the only ones at risk. Systems that control access to any resource are targets (e.g., time and attendance systems, inventory systems, school grading systems, and long-distance telephone systems).

4.3 Employee Sabotage

Employees are most familiar with their employer's computers and applications, including knowing what actions might cause the most damage, mischief, or sabotage. The downsizing of organizations in both the public and private sectors has created a group of individuals with organizational knowledge, who may retain potential system access (e.g., if system accounts are not deleted in a timely manner). The number of incidents of employee sabotage is believed to be much smaller than the instances of theft, but the cost of such incidents can be quite high.

4.4 Loss of Physical and Infrastructure Support

The loss of supporting infrastructure includes power failures (outages, spikes, and brownouts), loss of communications, water outages and leaks, sewer problems, lack of transportation services, fire, flood, civil unrest, and strikes. These losses include such dramatic events as

the explosion at the World Trade Center and the Chicago tunnel flood, as well as more common events, such as broken water pipes. Many of these issues are covered in Chapter 15. A loss of infrastructure often results in system downtime, sometimes in unexpected ways.

4.5 Malicious Hackers

The term malicious hackers, sometimes called crackers, refers to those who break into computers without authorization. They can include both outsiders and insiders. Much of the rise of hacker activity is often attributed to increases in connectivity in both government and industry. One 1992 study of a particular Internet site (i.e., one computer system) found that hackers attempted to break in at least once every other day.

4.6 Industrial Espionage

Industrial espionage is the act of gathering proprietary data from private companies or the government for the purpose of aiding another company(ies). Industrial espionage can be perpetrated either by companies seeking to improve their competitive advantage or by governments seeking to aid their domestic industries. Foreign industrial espionage carried out by a government is often referred to as economic espionage. Since information is processed and stored on computer systems, computer security can help protect against such threats; it can do little, however, to reduce the threat of authorized employees selling that information.

4.7 Malicious Code

Malicious code refers to viruses, worms, Trojan horses, logic bombs, and other "uninvited" software. Sometimes mistakenly associated only with personal computers, malicious code can attack other platforms.

4.8 Foreign Government Espionage

In some instances, threats posed by foreign government intelligence services may be present. In addition to possible economic espionage, foreign intelligence services may target unclassified systems to further their intelligence missions. Some unclassified information that may be of interest includes travel plans of senior officials, civil defense and emergency preparedness, manufacturing technologies, satellite data, personnel and payroll data, and law enforcement, investigative, and security files. Guidance should be sought from the cognizant security office regarding such threats.

4.9 Threats to Personal Privacy

The accumulation of vast amounts of electronic information about individuals by governments, credit bureaus, and private companies, combined with the ability of computers to monitor, process, and aggregate large amounts of information about individuals have created a threat to individual privacy. The possibility that all of this information and technology may be able to be linked together has arisen as a specter of the modern information age. This is often referred to as "Big Brother." To guard against such intrusion, Congress has enacted legislation, over the years, such as the Privacy Act of 1974 and the Computer Matching and Privacy Protection Act of 1988, which defines the boundaries of the legitimate uses of personal information collected by the government.

5 COMPUTER SECURITY POLICY

In discussions of computer security, the term policy has more than one meaning. Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term policy is also used to refer to the specific security rules for particular systems. Additionally, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization's e-mail privacy policy or fax security policy.

In this chapter the term computer security policy is defined as the "documentation of computer security decisions" which covers all the types of policy described above. In making these decisions, managers face hard choices involving resource allocation, competing objectives, and organizational strategy related to protecting both technical and information resources as well as guiding employee behavior. Managers at all levels make choices that can result in policy, with the scope of the policy's applicability varying according to the scope of the manager's authority. In this chapter we use the term policy in a broad manner to encompass all of the types of policy described above regardless of the level of manager who sets the particular policy.

5.1 Program Policy

A management official, normally the head of the organization or the senior administration official, issues program policy to establish (or restructure) the organization's computer security program and its basic structure. This high-level policy defines the purpose of the program and its scope within the organization; assigns responsibilities (to the computer security organization) for direct program implementation, as well as other responsibilities to related offices (such as the Information Resources Management [IRM] organization); and addresses compliance issues.

5.1.1 Basic Components of Program Policy

Components of program policy should address:

- # *Purpose.*
- # *Scope.*
- # *Responsibilities.*
- # *Compliance.*

5.2 Issue-Specific Policy

Whereas program policy is intended to address the broad organizationwide computer security program, issue-specific policies are developed to focus on areas of current relevance and concern (and sometimes controversy) to an organization. Management may find it appropriate, for example, to issue a policy on how the organization will approach contingency planning (centralized vs. decentralized) or the use of a particular methodology for managing risk to systems.

5.2.1 Example Topics for Issue-Specific Policy

There are many areas for which issue-specific policy may be appropriate. Two examples are explained below.

- # *Internet Access.*
- # *E-Mail Privacy.*

Other potential candidates for issue-specific policies include: approach to risk management and contingency planning, protection of confidential/proprietary information, unauthorized software, acquisition of software, doing computer work at home, bringing in disks from outside the workplace, access to other employees' files, encryption of files and e-mail, rights of privacy, responsibility for correctness of data, suspected malicious code, and physical emergencies.

5.2.2 Basic Components of Issue-Specific Policy

As suggested for program policy, a useful structure for issue-specific policy is to break the policy into its basic components.

- # *Issue Statement.*
- # *Statement of the Organization's Position.*
- # *Applicability.*
- # *Roles and Responsibilities.*
- # *Compliance.*
- # *Points of Contact and Supplementary Information.*

5.3 System-Specific Policy

Program policy and issue-specific policy both address policy from a broad level, usually encompassing the entire organization. However, they do not provide sufficient information or direction, for example, to be used in establishing an access control list or in training users on what actions are permitted. System-specific policy fills this need. It is much more focused, since it addresses only one system.

5.3.1 Security Objectives

The first step in the management process is to define security objectives for the specific system. Although, this process may start with an analysis of the need for integrity, availability, and confidentiality, it should not stop there. A security objective needs to be more specific; it should be concrete and well defined. It also should be stated so that it is clear that the objective is achievable. This process will also draw upon other applicable organization policies;

5.3.2 Operational Security Rules

After management determines the security objectives, the rules for operating a system can be laid out, for example, to define authorized and unauthorized modification. Who (by job category, organization placement, or name) can do what (e.g., modify, delete) to which specific classes and records of data, and under what conditions;

5.3.3 System-Specific Policy Implementation

Technology plays an important but not sole role in enforcing system-specific policies. When technology is used to enforce policy, it is important not to neglect nontechnology-based methods.

5.4 Interdependencies

Policy is related to many of the topics covered in this handbook:

- *Program Management.*
- *Access Controls.*
- *Links to Broader Organizational Policies.*

5.5 Cost Considerations

A number of potential costs are associated with developing and implementing computer security policies. Overall, the major cost of policy is the cost of implementing the policy and its impacts upon the organization.

6 COMPUTER SECURITY PROGRAM MANAGEMENT

This chapter presents an organizationwide approach to computer security and discusses its important management function. Because organizations differ vastly in size, complexity, management styles, and culture, it is not possible to describe one ideal computer security program. However, this chapter does describe some of the features and issues common to many federal organizations.

6.1 Structure of a Computer Security Program

Many computer security programs that are distributed throughout the organization have different elements performing various functions. While this approach has benefits, the distribution of the computer security function in many organizations is haphazard, usually based upon history (i.e., who was available in the organization to do what when the need arose). Ideally, the distribution of computer security functions should result from a planned and integrated management philosophy.

6.2 Central Computer Security Programs

The purpose of a central computer security program is to address the overall management of computer security within an organization. In the federal government, the organization could consist of a department, agency, or other major operating unit.

6.2.1 Benefits of Central Computer Security Programs

A central security program should provide two quite distinct types of benefits:

- # Increased efficiency and economy of security throughout the organization, and
- # the ability to provide centralized enforcement and oversight;

6.2.2 Efficient, Economic Coordination of Information

A central computer security program helps to coordinate and manage effective use of security-related resources throughout the organization. The most important of these resources are normally information and financial resources;

6.2.3 Central Enforcement and Oversight

Besides helping an organization improve the economy and efficiency of its computer security program, a centralized program can include an independent evaluation or enforcement function to ensure that organizational subunits are cost-effectively securing resources and following applicable policy. While the Office of the Inspector General (OIG) and external organizations, such as the General Accounting Office (GAO), also perform a valuable evaluation role, they operate outside the regular management channels.

6.3 Elements of an Effective Central Computer Security Program

For a central computer security program to be effective, it should be an established part of organization management. If system managers and applications owners do not need to consistently interact with the security program, then it can become an empty token of upper management's "commitment to security."

- *Stable Program Management Function.*
- *Stable Resource Base.*
- *Existence of Policy.*
- *Published Mission and Functions Statement.*
- *Long-Term Computer Security Strategy.*
- *Compliance Program.*
- *Intraorganizational Liaison.*
- *Liaison with External Groups.*

6.4 System-Level Computer Security Programs

While the central program addresses the entire spectrum of computer security for an organization, system-level programs ensure appropriate and cost-effective security for each system. This includes influencing decisions about what controls to implement, purchasing and installing technical controls, day-to-day computer security administration, evaluating system vulnerabilities, and responding to security problems. It encompasses all the areas discussed in the handbook.

6.5 Elements of Effective System-Level Programs

Like the central computer security program, many factors influence how successful a system-level computer security program is. Many of these are similar to the central program. This section addresses some additional considerations.

- *Security Plans.*
- *System-Specific Security Policy.*
- *Life Cycle Management.*
- *Integration With System Operations.*
- *Separation From Operations.*

6.6 Central and System-Level Program Interactions

A system-level program that is not integrated into the organizational program may have difficulty influencing significant areas affecting security. The system-level computer security program implements the policies, guidance, and regulations of the central computer

security program. The system-level office also learns from the information disseminated by the central program and uses the experience and expertise of the entire organization. The system-level computer security program further distributes information to systems management as appropriate.

6.7 Interdependencies

The general purpose of the computer security program, to improve security, causes it to overlap with other organizational operations as well as the other security controls discussed in the handbook. The central or system computer security program will address most controls at the policy, procedural, or operational level.

- *Policy.*
- *Life Cycle Management.*
- *Independent Audit.*

6.8 Cost Considerations

This chapter discussed how an organizationwide computer security program can manage security resources, including financial resources, more effectively. The cost considerations for a systemlevel computer security program are more closely aligned with the overall cost savings in having security.

7 COMPUTER SECURITY RISK MANAGEMENT

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Though perhaps not always aware of it, individuals manage risks every day. Actions as routine as buckling a car safety belt, carrying an umbrella when rain is forecast, or writing down a list of things to do rather than trusting to memory fall into the purview of risk management. People recognize various threats to their best interests and take precautions to guard against them or to minimize their effects.

7.1 Risk Assessment

Risk assessment, the process of analyzing and interpreting risk, is comprised of three basic activities: (1) determining the assessment's scope and methodology; (2) collecting and analyzing data; and (3) interpreting the risk analysis results.

7.1.1 Determining the Assessment's Scope and Methodology

The first step in assessing risk is to identify the system under consideration, the part of the system that will be analyzed, and the analytical method including its level of detail and formality.

7.1.2 Collecting and Analyzing Data

Risk has many different components: assets, threats, vulnerabilities, safeguards, consequences, and likelihood. This examination normally includes gathering data about the threatened area and synthesizing and analyzing the information to make it useful.

- # *Asset Valuation.*
- # *Consequence Assessment.*
- # *Threat Identification.*
- # *Safeguard Analysis.*
- # *Vulnerability Analysis.*
- # *Likelihood Assessment.*

7.1.3 Interpreting Risk Analysis Results

The risk assessment is used to support two related functions: the acceptance of risk and the selection of cost-effective controls. To accomplish these functions, the risk assessment must produce a meaningful output that reflects what is truly important to the organization. Limiting the risk interpretation activity to the most significant risks is

another way that the risk management process can be focused to reduce the overall effort while still yielding useful results.

7.2 Risk Mitigation

Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management, within applicable constraints. Although there is flexibility in how risk assessment is conducted, the sequence of identifying boundaries, analyzing input, and producing an output is quite natural. The process of risk mitigation has greater flexibility, and the sequence will differ more, depending on organizational culture and the purpose of the risk management activity. Although these activities are discussed in a specific sequence, they need not be performed in that sequence. In particular, the selection of safeguards and risk acceptance testing are likely to be performed simultaneously.

7.2.1 Selecting Safeguards

A primary function of computer security risk management is the identification of appropriate controls. In designing (or reviewing) the security of a system, it may be obvious that some controls should be added (e.g., because they are required by law or because they are clearly costeffective). It may also be just as obvious that other controls may be too expensive (considering both monetary and nonmonetary factors).

7.2.2 Accept Residual Risk

At some point, management needs to decide if the operation of the computer system is acceptable, given the kind and severity of remaining risks. Many managers do not fully understand computerbased risk for several reasons: (1) the type of risk may be different from risks previously associated with the organization or function; (2) the risk may be technical and difficult for a lay person to understand, or (3) the proliferation and decentralization of computing power can make it difficult to identify key assets that may be at risk.

7.2.3 Implementing Controls and Monitoring Effectiveness

Merely selecting appropriate safeguards does not reduce risk; those safeguards need to be effectively implemented. Moreover, to continue to be effective, risk management needs to be an ongoing process. This requires a periodic assessment and improvement of safeguards and reanalysis of risks. Chapter 8 discusses how periodic risk assessment is an integral part of the overall management of a system.

7.3 Uncertainty Analysis

Risk management often must rely on speculation, best guesses, incomplete data, and many unproven assumptions. The uncertainty analysis attempts to document this so that the risk management results can be used knowledgeably. There are two primary sources of uncertainty in the risk management process: (1) a lack of confidence or precision in the risk management model or methodology and (2) a lack of sufficient information to determine the exact value of the elements of the risk model, such as threat frequency, safeguard effectiveness, or consequences.

7.4 Interdependencies

Risk management touches on every control and every chapter in this handbook. It is, however, most closely related to life cycle management and the security planning process. The requirement to perform risk management is often discussed in organizational policy and is an issue for organizational oversight. These issues are discussed in Chapters 5 and 6.

7.5 Cost Considerations

The building blocks of risk management presented in this chapter can be used creatively to develop methodologies that concentrate expensive analysis work where it is most needed. Risk management can become expensive very quickly if an expansive boundary and detailed scope are selected. It is very important to use screening techniques, as discussed in

this chapter, to limit the overall effort. The goals of risk management should be kept in mind as a methodology is selected or developed. The methodology should concentrate on areas where identification of risk and the selection of cost-effective safeguards are needed.

8 SECURITY AND PLANNING IN THE COMPUTER SYSTEM LIFE CYCLE

Like other aspects of information processing systems, security is most effective and efficient if planned and managed throughout a computer system's life cycle, from initial planning, through design, implementation, and operation, to disposal. Many security-relevant events and analyses occur during a system's life. This chapter explains the relationship among them and how they fit together. It also discusses the important role of security planning in helping to ensure that security issues are addressed comprehensively.

8.1 Computer Security Act Issues for Federal Systems

Planning is used to help ensure that security is addressed in a comprehensive manner throughout a system's life cycle. For federal systems, the Computer Security Act of 1987 sets forth a statutory requirement for the preparation of computer security plans for all sensitive systems. The intent and spirit of the Act is to improve computer security in the federal government, not to create paperwork. In keeping with this intent, the Office of Management and Budget (OMB) and NIST have guided agencies toward a planning process that emphasizes good planning and management of computer security within an agency and for each computer system. As emphasized in this chapter, computer security management should be a part of computer systems management. The benefit of having a distinct computer security plan is to ensure that computer security is not overlooked.

8.2 Benefits of Integrating Security in the Computer System Life Cycle

Although a computer security plan can be developed for a system at any point in the life cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle. Security, like other aspects of a computer system, is best managed if planned for throughout the computer system life cycle. It has long been a tenet of the computer community that it costs ten times more to add a feature in a system after it has been designed than to include the feature in the system at the initial design phase. The principal reason for implementing security during a system's development is that it is more difficult to implement it later (as is usually reflected in the higher costs of doing so). It also tends to disrupt ongoing operations.

8.3 Overview of the Computer System Life Cycle

There are many models for the computer system life cycle but most contain five basic phases, as pictured in Figure 8.1.

- *Initiation.*
- *Development/Acquisition.*
- *Implementation.*
- *Operation/Maintenance.*
- *Disposal.*

8.4 Security Activities in the Computer System Life Cycle

This section reviews the security activities that arise in each stage of the computer system life cycle.

8.4.1 Initiation

The conceptual and early design process of a system involves the discovery of a need for a new system or enhancements to an existing system; early ideas as to system characteristics and proposed functionality; brainstorming sessions on architectural, performance, or functional system aspects; and environmental, financial, political, or other constraints. At the same time, the basic security aspects of a system should be

developed along with the early system design. This can be done through a sensitivity assessment.

8.4.1.1 Conducting a Sensitivity Assessment – A sensitivity assessment looks at the sensitivity of both the information to be processed and the system itself. The assessment should consider legal implications, organization policy (including federal and agency policy if a federal system), and the functional needs of the system. Sensitivity is normally expressed in terms of integrity, availability, and confidentiality. Such factors as the importance of the system to the organization's mission and the consequences of unauthorized modification, unauthorized disclosure, or unavailability of the system or data need to be examined when assessing sensitivity. To address these types of issues, the people who use or own the system or information should participate in the assessment.

8.4.2 Development/Acquisition

For most systems, the development/acquisition phase is more complicated than the initiation phase. Security activities can be divided into three parts:

- # determining security features, assurances, and operational practices;
- # incorporating these security requirements into design specifications; and
- # actually acquiring them.

8.4.2.1 Determining Security Requirements – During the first part of the development/acquisition phase, system planners define the requirements of the system. Security requirements should be developed at the same time. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for system developers), or operational practices (e.g., awareness and training). System security requirements, like other system requirements, are derived from a number of sources including law, policy, applicable standards and guidelines, functional needs of the system, and cost-benefit trade-offs.

Law.

Policy.

Standards and Guidelines.

Functional Needs of the System.

Cost-Benefit Analysis.

8.4.2.2 Incorporating Security Requirements Into Specifications – Determining security features, assurances, and operational practices can yield significant security information and often voluminous requirements. This information needs to be validated, updated, and organized into the detailed security protection requirements and specifications used by systems designers or purchasers. Specifications can take on quite different forms, depending on the methodology used for to develop the system, or whether the system, or parts of the system, are being purchased off the shelf.

8.4.2.3 Obtaining the System and Related Security Activities – During this phase, the system is actually built or bought. If the system is being built, security activities may include developing the system's security aspects, monitoring the development process itself for security problems, responding to changes, and monitoring threat. Threats or vulnerabilities that may arise during the development phase include Trojan horses, incorrect code, poorly functioning development tools, manipulation of code, and malicious insiders.

8.4.3 Implementation

A separate implementation phase is not always specified in some life cycle planning efforts. (It is often incorporated into the end of development and acquisition or the beginning of operation and maintenance.) However, from a security point of view, a critical security activity, accreditation, occurs between development and the start of system operation. The other activities described in this section, turning on the controls and testing, are often incorporated at the end of the development/acquisition phase.

8.4.3.1 Install/Turn-On Controls – While obvious, this activity is often overlooked. When acquired, a system often comes with security features disabled. These need to be enabled and configured. For many systems this is a complex task requiring significant skills. Custom-developed systems may also require similar work.

8.4.3.2 Security Testing – System security testing includes both the testing of the particular parts of the system that have been developed or acquired and the testing of the entire system. Security management, physical facilities, personnel, procedures, the use of commercial or in-house services (such as networking services), and contingency planning are examples of areas that affect the security of the entire system, but may be specified outside of the development or acquisition cycle. Since only items within the development or acquisition cycle will have been tested during system acceptance testing, separate tests or reviews may need to be performed for these additional security elements.

8.4.3.3 Accreditation – System security accreditation is the formal authorization by the accrediting (management) official for system operation and an explicit acceptance of risk. It is usually supported by a review of the system, including its management, operational, and technical controls. This review may include a detailed technical evaluation (such as a Federal Information Processing Standard 102 certification, particularly for complex, critical, or high-risk systems), security evaluation, risk assessment, audit, or other such review. If the life cycle process is being used to manage a project (such as a system upgrade), it is important to recognize that the accreditation is for the entire system, not just for the new addition.

8.4.4 Operation and Maintenance

Many security activities take place during the operational phase of a system's life. In general, these fall into three areas: (1) security operations and administration; (2) operational assurance; and (3) periodic re-analysis of the security. Figure 8.2 diagrams the flow of security activities during the operational phase.

8.4.4.1 Security Operations and Administration – Operation of a system involves many security activities discussed throughout this handbook. Performing backups, holding training classes, managing cryptographic keys, keeping up with user administration and access privileges, and updating security software are some examples.

8.4.4.2 Operational Assurance – Security is never perfect when a system is implemented. In addition, system users and operators discover new ways to intentionally or unintentionally bypass or subvert security. Changes in the system or the environment can create new vulnerabilities. Strict adherence to procedures is rare over time, and procedures become outdated. Thinking risk is minimal, users may tend to bypass security measures and procedures.

8.4.4.3 Managing Change – Computer systems and the environments in which they operate change continually. In response to various events such as user complaints, availability of new features and services, or the discovery of new threats and vulnerabilities, system managers and users modify the system and incorporate new features, new procedures, and software updates.

8.4.4.4 Periodic Reaccreditation – Periodically, it is useful to formally reexamine the security of a system from a wider perspective. The analysis, which leads to reaccreditation, should address such questions as: Is the security still sufficient? Are major changes needed?

8.4.5 Disposal

The disposal phase of the computer system life cycle involves the disposition of information, hardware, and software. Information may be moved to another system, archived, discarded, or destroyed. When archiving information, consider the method for retrieving the information in the future. The technology used to create the records may not be readily available in the future.

8.5 Interdependencies

Like many management controls, life cycle planning relies upon other controls. Three closely linked control areas are policy, assurance, and risk management.

- *Policy.*
- *Assurance.*
- *Risk Management.*

8.6 Cost Considerations

Security is a factor throughout the life cycle of a system. Sometimes security choices are made by default, without anyone analyzing why choices are made; sometimes security choices are made carefully, based on analysis. The first case is likely to result in a system with poor security that is susceptible to many types of loss. In the second case, the cost of life cycle management should be much smaller than the losses avoided. The major cost considerations for life cycle management are personnel costs and some delays as the system progresses through the life cycle for completing analyses and reviews and obtaining management approvals.

9 ASSURANCE

Computer security assurance is the degree of confidence one has that the security measures, both technical and operational, work as intended to protect the system and the information it processes. Assurance is not, however, an absolute guarantee that the measures work as intended. Like the closely related areas of reliability and quality, assurance can be difficult to analyze; however, it is something people expect and obtain (though often without realizing it).

Assurance is a degree of confidence, not a true measure of how secure the system actually is. This distinction is necessary because it is extremely difficult -- and in many cases virtually impossible -- to know exactly how secure a system is.

9.1 Accreditation and Assurance

Accreditation is a management official's formal acceptance of the adequacy of a system's security. The best way to view computer security accreditation is as a form of quality control. It forces managers and technical staff to work together to find workable, cost-effective solutions given security needs, technical constraints, operational constraints, and mission or business requirements. The accreditation process obliges managers to make the critical decision regarding the adequacy of security safeguards and, therefore, to recognize and perform their role in securing their systems. In order for the decisions to be sound, they need to be based on reliable information about the implementation of both technical and nontechnical safeguards.

9.1.1 Accreditation and Assurance

Assurance is an extremely important -- but not the only -- element in accreditation. As shown in the diagram, assurance addresses whether the technical measures and procedures operate either (1) according to a set of security requirements and specifications or (2) according to general quality principles. Accreditation also addresses whether the system's security requirements are correct and well implemented and whether the level of quality is sufficiently high. These activities are discussed in Chapters 7 and 8;

9.1.2 Selecting Assurance Methods

The accrediting official makes the final decision about how much and what types of assurance are needed for a system. For this decision to be informed, it is derived from a review of security, such as a risk assessment or other study (e.g., certification), as deemed appropriate by the accrediting official. The accrediting official needs to be in a position to analyze the pros and cons of the cost of assurance, the cost of controls, and the risks to the organization. At the end of the accreditation process, the accrediting

official will be the one to accept the remaining risk. Thus, the selection of assurance methods should be coordinated with the accrediting official.

9.2 Planning and Assurance

Assurance planning should begin during the planning phase of the system life cycle, either for new systems or a system upgrades. Planning for assurance when planning for other system requirements makes sense. If a system is going to need extensive testing, it should be built to facilitate such testing.

9.3 Design and Implementation Assurance

Design and implementation assurance addresses whether the features of a system, application, or component meets security requirements and specifications and whether they are they are well designed and well built. Chapter 8 discusses the source for security requirements and specifications. Design and implementation assurance examines system design, development, and installation. Design and implementation assurance is usually associated with the development/acquisition and implementation phase of the system life cycle; however, it should also be considered throughout the life cycle as the system is modified.

9.3.1 Testing and Certification

Testing can address the quality of the system as built, as implemented, or as operated. Thus, it can be performed throughout the development cycle, after system installation, and throughout its operational phase. Some common testing techniques include functional testing (to see if a given function works according to its requirements) or penetration testing (to see if security can be bypassed). These techniques can range from trying several test cases to in-depth studies using metrics, automated tools, or multiple detailed test cases.

Certification.

9.3.2 NIST Conformance Testing and Validation Suites

NIST produces validation suites and conformance testing to determine if a product (software, hardware, firmware) meets specified standards. These test suites are developed for specific standards and use many methods. Conformance to standards can be important for many reasons, including interoperability or strength of security provided. NIST publishes a list of validated products quarterly.

9.3.3 Use of Advanced or Trusted Development

In the development of both commercial off-the-shelf products and more customized systems, the use of advanced or trusted system architectures, development methodologies, or software engineering techniques can provide assurance. Examples include security design and development reviews, formal modeling, mathematical proofs, ISO 9000 quality techniques, or use of security architecture concepts, such as a trusted computing base (TCB) or reference monitor.

9.3.4 Use of Reliable Architectures

Some system architectures are intrinsically more reliable, such as systems that use fault-tolerance, redundancy, shadowing, or redundant array of inexpensive disks (RAID) features. These examples are primarily associated with system availability.

9.3.5 Use of Reliable Security

One factor in reliable security is the concept of ease of safe use, which postulates that a system that is easier to secure will be more likely to be secure. Security features may be more likely to be used when the initial system defaults to the "most secure" option. In addition, a system's security may be deemed more reliable if it does not use very new technology that has not been tested in the "real" world (often called "bleeding-edge" technology). Conversely, a system that uses older, well-tested software may be less likely to contain bugs.

9.3.6 Evaluations

A product evaluation normally includes testing. Evaluations can be performed by many types of organizations, including government agencies, both domestic and foreign; independent organizations, such as trade and professional organizations; other vendors or commercial groups; or individual users or user consortia. Product reviews in trade literature are a form of evaluation, as are more formal reviews made against specific criteria. Important factors for using evaluations are the degree of independence of the evaluating group, whether the evaluation criteria reflect needed security features, the rigor of the testing, the testing environment, the age of the evaluation, the competence of the evaluating organization, and the limitations placed on the evaluations by the evaluating group (e.g., assumptions about the threat or operating environment).

9.3.7 Assurance Documentation

The ability to describe security requirements and how they were met can reflect the degree to which a system or product designer understands applicable security issues. Without a good understanding of the requirements, it is not likely that the designer will be able to meet them.

9.3.8 Accreditation of Product to Operate in Similar Situation

The accreditation of a product or system to operate in a similar situation can be used to provide some assurance. However, it is important to realize that an accreditation is environment- and system-specific. Since accreditation balances risk against advantages, the same product may be appropriately accredited for one environment but not for another, even by the same accrediting official.

9.3.9 Self-Certification

A vendor's, integrator's, or system developer's self-certification does not rely on an impartial or independent agent to perform a technical evaluation of a system to see how well it meets a stated security requirement. Even though it is not impartial, it can still provide assurance. The selfcertifier's reputation is on the line, and a resulting certification report can be read to determine whether the security requirement was defined and whether a meaningful review was performed.

9.3.10 Warranties, Integrity Statements, and Liabilities

Warranties are another source of assurance. If a manufacturer, producer, system developer, or integrator is willing to correct errors within certain time frames or by the next release, this should give the system manager a sense of commitment to the product and of the product's quality. An integrity statement is a formal declaration or certification of the product. It can be backed up by a promise to (a) fix the item (warranty) or (b) pay for losses (liability) if the product does not conform to the integrity statement.

9.3.11 Manufacturer's Published Assertions

A manufacturer's or developer's published assertion or formal declaration provides a limited amount of assurance based exclusively on reputation.

9.3.12 Distribution Assurance

It is often important to know that software has arrived unmodified, especially if it is distributed electronically. In such cases, checkbits or digital signatures can provide high assurance that code has not been modified. Anti-virus software can be used to check software that comes from sources with unknown reliability (such as a bulletin board).

9.4 Operational Assurance

Design and implementation assurance addresses the quality of security features built into systems. Operational assurance addresses whether the system's technical features are being bypassed or have vulnerabilities and whether required procedures are being followed. It

does not address changes in the system's security requirements, which could be caused by changes to the system and its operating or threat environment).

9.4.1 Audit Methods and Tools

An audit conducted to support operational assurance examines whether the system is meeting stated or implied security requirements including system and organization policies. Some audits also examine whether security requirements are appropriate, but this is outside the scope of operational assurance. (See Chapter 8.) Less formal audits are often called security reviews;

9.4.1.1 Automated Tools – Even for small multiuser computer systems, it is a big job to manually review security features. Automated tools make it feasible to review even large computer systems for a variety of security flaws.

There are two types of automated tools: (1) active tools, which find vulnerabilities by trying to exploit them, and (2) passive tests, which only examine the system and infer the existence of problems from the state of the system.

9.4.1.2 Internal Controls Audit – An auditor can review controls in place and determine whether they are effective. The auditor will often analyze both computer and noncomputer-based controls. Techniques used include inquiry, observation, and testing (of both the controls themselves and the data). The audit can also detect illegal acts, errors, irregularities, or a lack of compliance with laws and regulations. Security checklists and penetration testing, discussed below, may be used.

9.4.1.3 Security Checklists – Within the government, the computer security plan provides a checklist against which the system can be audited. This plan, discussed in Chapter 8, outlines the major security considerations for a system, including management, operational, and technical issues. One advantage of using a computer security plan is that it reflects the unique security environment of the system, rather than a generic list of controls. Other checklists can be developed, which include national or organizational security policies and practices (often referred to as baselines). Lists of "generally accepted security practices" (GSSPs) can also be used. Care needs to be taken so that deviations from the list are not automatically considered wrong, since they may be appropriate for the system's particular environment or technical constraints.

9.4.1.4 Penetration Testing – Penetration testing can use many methods to attempt a system break-in. In addition to using active automated tools as described above, penetration testing can be done "manually." The most useful type of penetration testing is to use methods that might really be used against the system. For hosts on the Internet, this would certainly include automated tools. For many systems, lax procedures or a lack of internal controls on applications are common vulnerabilities that penetration testing can target. Another method is "social engineering," which involves getting users or administrators to divulge information about systems, including their passwords.

9.4.2 Monitoring Methods and Tools

Security monitoring is an ongoing activity that looks for vulnerabilities and security problems. Many of the methods are similar to those used for audits, but are done more regularly or, for some automated tools, in real time.

9.4.2.1 Review of System Logs – As discussed in Chapter 8, a periodic review of system-generated logs can detect security problems, including attempts to exceed access authority or gain system access during unusual hours.

9.4.2.2 Automated Tools – Several types of automated tools monitor a system for security problems. Some examples follow:

Virus scanners.

Checksumming.

Password crackers.

Integrity verification programs.

Intrusion detectors.

System performance monitoring.

9.4.2.3 Configuration Management – From a security point of view, configuration management provides assurance that the system in operation is the correct version (configuration) of the system and that any changes to be made are reviewed for security implications. Configuration management can be used to help ensure that changes take place in an identifiable and controlled environment and that they do not unintentionally harm any of the system's properties, including its security. Some organizations, particularly those with very large systems (such as the federal government), use a configuration control board for configuration management. When such a board exists, it is helpful to have a computer security expert participate. In any case, it is useful to have computer security officers participate in system management decision making.

9.4.2.4 Trade Literature/Publications/Electronic News – In addition to monitoring the system, it is useful to monitor external sources for information. Such sources as trade literature, both printed and electronic, have information about security vulnerabilities, patches, and other areas that impact security. The Forum of Incident Response Teams (FIRST) has an electronic mailing list that receives information on threats, vulnerabilities, and patches.

9.5 Interdependencies

Assurance is an issue for every control and safeguard discussed in this handbook. Are user ID and access privileges kept up to date? Has the contingency plan been tested? Can the audit trail be tampered with? One important point to be reemphasized here is that assurance is not only for technical controls, but for operational controls as well. Although the chapter focused on information systems assurance, it is also important to have assurance that management controls are working well. Is the security program effective? Are policies understood and followed? As noted in the introduction to this chapter, the need for assurance is more widespread than people often realize.

9.6 Cost Considerations

There are many methods of obtaining assurance that security features work as anticipated. Since assurance methods tend to be qualitative rather than quantitative, they will need to be evaluated. Assurance can also be quite expensive, especially if extensive testing is done. It is useful to evaluate the amount of assurance received for the cost to make a best-value decision. In general, personnel costs drive up the cost of assurance. Automated tools are generally limited to addressing specific problems, but they tend to be less expensive.

10 PERSONNEL/USER ISSUES

Many important issues in computer security involve human users, designers, implementors, and managers. A broad range of security issues relate to how these individuals interact with computers and the access and authorities they need to do their job. No computer system can be secured without properly addressing these security issues.

This chapter examines issues concerning the staffing of positions that interact with computer systems; the administration of users on a system, including considerations for terminating employee access; and special considerations that may arise when contractors or the public have access to systems. Personnel issues are closely linked to logical access controls, discussed in Chapter 17.

10.1 Staffing

The staffing process generally involves at least four steps and can apply equally to general users as well as to application managers, system management personnel, and security

personnel. These four steps are: (1) defining the job, normally involving the development of a position description; (2) determining the sensitivity of the position; (3) filling the position, which involves screening applicants and selecting an individual; and (4) training.

10.1.1 Groundbreaking Position Definition

Early in the process of defining a position, security issues should be identified and dealt with. Once a position has been broadly defined, the responsible supervisor should determine the type of computer access needed for the position. There are two general principles to apply when granting access: *separation of duties* and *least privilege*.

10.1.2 Determining Position Sensitivity

Knowledge of the duties and access levels that a particular position will require is necessary for determining the sensitivity of the position. The responsible management official should correctly identify position sensitivity levels so that appropriate, cost-effective screening can be completed;

10.1.3 Filling the Position -- Screening and Selecting

Once a position's sensitivity has been determined, the position is ready to be staffed. In the federal government, this typically includes publishing a formal vacancy announcement and identifying which applicants meet the position requirements. More sensitive positions typically require preemployment background screening; screening after employment has commenced (postentry-on-duty) may suffice for less sensitive positions;

10.1.4 Employee Training and Awareness

Even after a candidate has been hired, the staffing process cannot yet be considered complete employees still have to be trained to do their job, which includes computer security responsibilities and duties. As discussed in Chapter 13, such security training can be very cost-effective in promoting security.

10.2 User Administration

Effective administration of users' computer access is essential to maintaining system security. User account management focuses on identification, authentication, and access authorizations. This is augmented by the process of auditing and otherwise periodically verifying the legitimacy of current accounts and access authorizations. Finally, there are considerations involved in the timely modification or removal of access and associated issues for employees who are reassigned, promoted, or terminated, or who retire.

10.2.1 User Account Management

User account management involves (1) the process of requesting, establishing, issuing, and closing user accounts; (2) tracking users and their respective access authorizations; and (3) managing these functions;

10.2.2 Audit and Management Reviews

From time to time, it is necessary to review user account management on a system. Within the area of user access issues, such reviews may examine the levels of access each individual has, conformity with the concept of least privilege, whether all accounts are still active, whether management authorizations are up-to-date, whether required training has been completed, and so forth;

10.2.3 Detecting Unauthorized/Illegal Activities

Several mechanisms are used besides auditing and analysis of audit trails to detect unauthorized and illegal acts. (See Chapters 9 and 18.) For example, fraudulent activities may require the regular physical presence of the perpetrator(s). In such cases, the fraud may be detected during the employee's absence. Mandatory vacations for critical systems and applications personnel can help detect such activity (however, this is not a guarantee, for example, if problems are saved for the employees to handle upon

their return). It is useful to avoid creating an excessive dependence upon any single individual, since the system will have to function during periods of absence. Particularly within the government, periodic rescreening of personnel is used to identify possible indications of illegal activity (e.g., living a lifestyle in excess of known income level);

10.2.4 Temporary Assignments and In-house Transfers

One significant aspect of managing a system involves keeping user access authorizations up to date. Access authorizations are typically changed under two types of circumstances: (1) change in job role, either temporarily (e.g., while covering for an employee on sick leave) or permanently (e.g., after an in-house transfer) and (2) termination discussed in the following section;

10.2.5 Termination

Termination of a user's system access generally can be characterized as either "friendly" or "unfriendly." Friendly termination may occur when an employee is voluntarily transferred, resigns to accept a better position, or retires. Unfriendly termination may include situations when the user is being fired for cause, "RIFed," or involuntarily transferred. Fortunately, the former situation is more common, but security issues have to be addressed in both situations.

10.2.5.1 Friendly Termination – Friendly termination refers to the removal of an employee from the organization when there is no reason to believe that the termination is other than mutually acceptable. Since terminations can be expected regularly, this is usually accomplished by implementing a standard set of procedures for outgoing or transferring employees. These are part of the standard employee "out-processing," and are put in place, for example, to ensure that system accounts are removed in a timely manner. Out-processing often involves a sign-out form initialed by each functional manager with an interest in the separation. This normally includes the group(s) managing access controls, the control of keys, the briefing on the responsibilities for confidentiality and privacy, the library, the property clerk, and several other functions not necessarily related to information security.

10.2.5.2 Unfriendly Termination – Unfriendly termination involves the removal of an employee under involuntary or adverse conditions. This may include termination for cause, RIF, involuntary transfer, resignation for "personality conflicts," and situations with pending grievances. The tension in such terminations may multiply and complicate security issues. Additionally, all of the issues involved in friendly terminations are still present, but addressing them may be considerably more difficult.

10.3 Contractor Access Considerations

Many federal agencies as well as private organizations use contractors and consultants to assist with computer processing. Contractors are often used for shorter periods of time than regular employees. This factor may change the cost-effectiveness of conducting screening. The often higher turnover among contractor personnel generates additional costs for security programs in terms of user administration.

10.4 Public Access Considerations

Many federal agencies have begun to design, develop, and implement public access systems for electronic dissemination of information to the public. Some systems provide electronic interaction by allowing the public to send information to the government (e.g., electronic tax filing) as well as to receive it. When systems are made available for access by the public (or a large or significant subset thereof), additional security issues arise due to: (1) increased threats against public access systems and (2) the difficulty of security administration.

10.5 Interdependencies

User issues are tied to topics throughout this handbook.

– *Training and Awareness.*

- *Identification and Authentication and Access Controls.*
- *Policy.*

10.6 Cost Considerations

There are many security costs under the category of user issues. Among these are:

- *Screening.*
- *Training and Awareness.*
- *User Administration.*
- *Access Administration.*
- *Auditing.*

11 PREPARING FOR CONTINGENCIES AND DISASTERS

A computer security contingency is an event with the potential to disrupt computer operations, thereby disrupting critical mission and business functions. Such an event could be a power outage, hardware failure, fire, or storm. If the event is very destructive, it is often called a disaster.

To avert potential contingencies and disasters or minimize the damage they cause organizations can take steps early to control the event. Generally called contingency planning, this activity is closely related to incident handling, which primarily addresses malicious technical threats such as hackers and viruses.

11.1 Step 1: Identifying the Mission- or Business-Critical Functions

Protecting the continuity of an organization's mission or business is very difficult if it is not clearly identified. Managers need to understand the organization from a point of view that usually extends beyond the area they control. The definition of an organization's critical mission or business functions is often called a business plan.

11.2 Step 2: Identifying the Resources That Support Critical Functions

After identifying critical missions and business functions, it is necessary to identify the supporting resources, the time frames in which each resource is used (e.g., is the resource needed constantly or only at the end of the month?), and the effect on the mission or business of the unavailability of the resource. In identifying resources, a traditional problem has been that different managers oversee different resources. They may not realize how resources interact to support the organization's mission or business. Many of these resources are not computer resources. Contingency planning should address all the resources needed to perform a function, regardless whether they directly relate to a computer.

11.2.1 Human Resources

People are perhaps an organization's most obvious resource. Some functions require the effort of specific individuals, some require specialized expertise, and some only require individuals who can be trained to perform a specific task. Within the information technology field, human resources include both operators (such as technicians or system programmers) and users (such as data entry clerks or information analysts);

11.2.2 Processing Capability

Traditionally contingency planning has focused on processing power (i.e., if the data center is down, how can applications dependent on it continue to be processed?). Although the need for data center backup remains vital, today's other processing alternatives are also important. Local area networks (LANs), minicomputers, workstations, and personal computers in all forms of centralized and distributed processing may be performing critical tasks;

11.2.3 Automated Applications and Data

Computer systems run applications that process data. Without current electronic versions of both applications and data, computerized processing may not be possible. If the processing is being performed on alternate hardware, the applications must be compatible with the alternate hardware, operating systems and other software (including version and configuration), and numerous other technical factors. Because of the complexity, it is normally necessary to periodically verify compatibility. (See Step 6, Testing and Revising.);

11.2.4 Computer-Based Services

An organization uses many different kinds of computer-based services to perform its functions. The two most important are normally communications services and information services. Communications can be further categorized as data and voice communications; however, in many organizations these are managed by the same service. Information services include any source of information outside of the organization. Many of these sources are becoming automated, including on-line government and private databases, news services, and bulletin boards;

11.2.5 Physical Infrastructure

For people to work effectively, they need a safe working environment and appropriate equipment and utilities. This can include office space, heating, cooling, venting, power, water, sewage, other utilities, desks, telephones, fax machines, personal computers, terminals, courier services, file cabinets, and many other items. In addition, computers also need space and utilities, such as electricity. Electronic and paper media used to store applications and data also have physical requirements;

11.2.6 Documents and Papers

Many functions rely on vital records and various documents, papers, or forms. These records could be important because of a legal need (such as being able to produce a signed copy of a loan) or because they are the only record of the information. Records can be maintained on paper, microfiche, microfilm, magnetic media, or optical disk.

11.3 Step 3: Anticipating Potential Contingencies or Disasters

Although it is impossible to think of all the things that can go wrong, the next step is to identify a likely range of problems. The development of scenarios will help an organization develop a plan to address the wide range of things that can go wrong. Scenarios should include small and large contingencies. While some general classes of contingency scenarios are obvious, imagination and creativity, as well as research, can point to other possible, but less obvious, contingencies. The contingency scenarios should address each of the resources described above. The following are examples of some of the types of questions that contingency scenarios may address:

- *Human Resources*: Can people get to work? Are key personnel willing to cross a picket line? Are there critical skills and knowledge possessed by one person? Can people easily get to an alternative site?
- *Processing Capability*: Are the computers harmed? What happens if some of the computers are inoperable, but not all?
- *Automated Applications and Data*: Has data integrity been affected? Is an application sabotaged? Can an application run on a different processing platform?
- *Computer-Based Services*: Can the computers communicate? To where? Can people communicate? Are information services down? For how long?
- *Infrastructure*: Do people have a place to sit? Do they have equipment to do their jobs? Can they occupy the building?
- *Documents/Paper*: Can needed records be found? Are they readable?

11.4 Step 4: Selecting Contingency Planning Strategies

The next step is to plan how to recover needed resources. In evaluating alternatives, it is necessary to consider what controls are in place to prevent and minimize contingencies. Since no set of controls can cost-effectively prevent all contingencies, it is necessary to coordinate prevention and recovery efforts.

11.4.1 Human Resources

To ensure an organization has access to workers with the right skills and knowledge, training and documentation of knowledge are needed. During a major contingency, people will be under significant stress and may panic. If the contingency is a regional disaster, their first concerns will probably be their family and property. In addition, many people will be either unwilling or unable to come to work. Additional hiring or temporary services can be used. The use of additional personnel may introduce security vulnerabilities;

11.4.2 Processing Capability

Strategies for processing capability are normally grouped into five categories: hot site; cold site; redundancy; reciprocal agreements; and hybrids. These terms originated with recovery strategies for data centers but can be applied to other platforms;

11.4.3 Automated Applications and Data

Normally, the primary contingency strategy for applications and data is regular backup and secure offsite storage. Important decisions to be addressed include how often the backup is performed, how often it is stored off-site, and how it is transported (to storage, to an alternate processing site, or to support the resumption of normal operations);

11.4.4 Computer-Based Services

Service providers may offer contingency services. Voice communications carriers often can reroute calls (transparently to the user) to a new location. Data communications carriers can also reroute traffic. Hot sites are usually capable of receiving data and voice communications. If one service provider is down, it may be possible to use another. However, the type of communications carrier lost, either local or long distance, is important. Local voice service may be carried on cellular. Local data communications, especially for large volumes, is normally more difficult. In addition, resuming normal operations may require another rerouting of communications services;

11.4.5 Physical Infrastructure

Hot sites and cold sites may also offer office space in addition to processing capability support. Other types of contractual arrangements can be made for office space, security services, furniture, and more in the event of a contingency. If the contingency plan calls for moving offsite, procedures need to be developed to ensure a smooth transition back to the primary operating facility or to a new facility. Protection of the physical infrastructure is normally an important part of the emergency response plan, such as use of fire extinguishers or protecting equipment from water damage;

11.4.6 Documents and Papers

The primary contingency strategy is usually backup onto magnetic, optical, microfiche, paper, or other medium and offsite storage. Paper documents are generally harder to backup than electronic ones. A supply of forms and other needed papers can be stored offsite.

11.4.6 Documents and Papers

Once the contingency planning strategies have been selected, it is necessary to make appropriate preparations, document the strategies, and train employees. Many of these tasks are ongoing.

11.5.1 Implementation

Much preparation is needed to implement the strategies for protecting critical functions and their supporting resources. For example, one common preparation is to establish procedures for backing up files and applications. Another is to establish contracts and agreements, if the contingency strategy calls for them. Existing service contracts may need to be renegotiated to add contingency services. Another preparation may be to purchase equipment, especially to support a redundant capability;

11.5.2 Documenting

The contingency plan needs to be written, kept up-to-date as the system and other factors change, and stored in a safe place. A written plan is critical during a contingency, especially if the person who developed the plan is unavailable. It should clearly state in simple language the sequence of tasks to be performed in the event of a contingency so that someone with minimal knowledge could immediately begin to execute the plan. It is generally helpful to store up-to-date copies of the contingency plan in several locations, including any off-site locations, such as alternate processing sites or backup data storage facilities;

11.5.3 Training

All personnel should be trained in their contingency-related duties. New personnel should be trained as they join the organization, refresher training may be needed, and personnel will need to practice their skills.

11.6 Step 6: Testing and Revising

A contingency plan should be tested periodically because there will undoubtedly be flaws in the plan and in its implementation. The plan will become dated as time passes and as the resources used to support critical functions change. Responsibility for keeping the contingency plan current should be specifically assigned. The extent and frequency of testing will vary between organizations and among systems. There are several types of testing, including reviews, analyses, and simulations of disasters.

11.7 Interdependencies

Since all controls help to prevent contingencies, there is an interdependency with all of the controls in the handbook.

- *Risk Management.*
- *Physical and Environmental Controls.*
- *Incident Handling.*
- *Support and Operations.*
- *Policy.*

11.8 Cost Considerations

The cost of developing and implementing contingency planning strategies can be significant, especially if the strategy includes contracts for backup services or duplicate equipment. There are too many options to discuss cost considerations for each type.

12 COMPUTER SECURITY INCIDENT HANDLING

Computer systems are subject to a wide range of mishaps from corrupted data files, to viruses, to natural disasters. Some of these mishaps can be fixed through standard operating procedures. For example, frequently occurring events (e.g., a mistakenly deleted file) can usually be readily repaired (e.g., by restoration from the backup file). More severe mishaps, such as outages caused by natural disasters, are normally addressed in an organization's contingency plan. Other damaging events result from deliberate malicious technical activity (e.g., the creation of viruses or system hacking).

This chapter describes how organizations can address computer security incidents (in the context of their larger computer security program) by developing a computer security incident handling capability.

12.1 Benefits of an Incident Handling Capability

The primary benefits of an incident handling capability are containing and repairing damage from incidents, and preventing future damage. In addition, there are less obvious side benefits related to establishing an incident handling capability.

12.1.1 Containing and Repairing Damage From Incidents

When left unchecked, malicious software can significantly harm an organization's computing, depending on the technology and its connectivity. An incident handling capability provides a way for users to report incidents and the appropriate response and assistance to be provided to aid in recovery. Technical capabilities (e.g., trained personnel and virus identification software) are prepositioned, ready to be used as necessary. Moreover, the organization will have already made important contacts with other supportive sources (e.g., legal, technical, and managerial) to aid in containment and recovery efforts;

12.1.2 Preventing Future Damage

An incident handling capability also assists an organization in preventing (or at least minimizing) damage from future incidents. Incidents can be studied internally to gain a better understanding of the organizations's threats and vulnerabilities so more effective safeguards can be implemented. Additionally, through outside contacts (established by the incident handling capability) early warnings of threats and vulnerabilities can be provided. Mechanisms will already be in place to warn users of these risks;

12.1.3 Side Benefits

Finally, establishing an incident handling capability helps an organization in perhaps unanticipated ways. Three are discussed here.

Uses of Threat and Vulnerability Data.

Enhancing Internal Communications and Organization Preparedness.

Enhancing the Training and Awareness Program.

12.2 Characteristics of a Successful Incident Handling Capability

A successful incident handling capability has several core characteristics:

- an understanding of the constituency it will serve;
- an educated constituency;
- a means for centralized communications;
- expertise in the requisite technologies; and
- links to other groups to assist in incident handling (as needed).

12.2.1 Defining the Constituency to Be Served

The constituency includes computer users and program managers. Like any other customervendor relationship, the constituency will tend to take advantage of the capability if the services rendered are valuable;

12.2.2 Educated Constituency

Users need to know about, accept, and trust the incident handling capability or it will not be used. Through training and awareness programs, users can become knowledgeable about the existence of the capability and how to recognize and report incidents. Users trust in the value of the service will build with reliable performance;

12.2.3 Centralized Reporting and Communications

Successful incident handling requires that users be able to report incidents to the incident handling team in a convenient, straightforward fashion; this is referred to as centralized reporting. A successful incident handling capability depends on timely reporting. If it is

difficult or time consuming to report incidents, the incident handling capability may not be fully used. Usually, some form of a hotline, backed up by pagers, works well;

12.2.4 Technical Platform and Communications Expertise

The technical staff members who comprise the incident handling capability need specific knowledge, skills, and abilities;

12.2.5 Liaison With Other Organizations

Due to increasing computer connectivity, intruder activity on networks can affect many organizations, sometimes including those in foreign countries. Therefore, an organization's incident handling team may need to work with other teams or security groups to effectively handle incidents that range beyond its constituency. Additionally, the team may need to pool its knowledge with other teams at various times. Thus, it is vital to the success of an incident handling capability that it establish ties and contacts with other related counterparts and supporting organizations.

12.3 Technical Support for Incident Handling

Incident handling will be greatly enhanced by technical mechanisms that enable the dissemination of information quickly and conveniently.

12.3.1 Communications for Centralized Reporting of Incidents

The technical ability to report incidents is of primary importance, since without knowledge of an incident, response is precluded. Fortunately, such technical mechanisms are already in place in many organizations;

12.3.2 Rapid Communications Facilities

Some form of rapid communications is essential for quickly communicating with the constituency as well as with management officials and outside organizations. The team may need to send out security advisories or collect information quickly, thus some convenient form of communications, such as electronic mail, is generally highly desirable. With electronic mail, the team can easily direct information to various subgroups within the constituency, such as system managers or network managers, and broadcast general alerts to the entire constituency as needed. When connectivity already exists, e-mail has low overhead and is easy to use. (However, it is possible for the e-mail system itself to be attacked, as was the case with the 1988 Internet worm.);

12.3.3 Secure Communications Facilities

Incidents can range from the trivial to those involving national security. Often when exchanging information about incidents, using encrypted communications may be advisable. This will help prevent the unintended distribution of incident-related information. Encryption technology is available for voice, fax, and e-mail communications.

12.4 Interdependencies

An incident handling capability generally depends upon other safeguards presented in this handbook. The most obvious is the strong link to other components of the contingency plan. The following paragraphs detail the most important of these interdependencies.

- *Contingency Planning.*
- *Support and Operations.*
- *Training and Awareness.*
- *Risk Management.*

12.5 Cost Considerations

There are a number of start-up costs and funding issues to consider when planning an incident handling capability. Because the success of an incident handling capability relies so heavily on users' perceptions of its worth and whether they use it, it is very important that the capability be able to meet users' requirements. Two important funding issues are:

- *Personnel.*
- *Education and Training.*

13 AWARENESS, TRAINING, AND EDUCATION

People, who are all fallible, are usually recognized as one of the weakest links in securing systems. The purpose of computer security awareness, training, and education is to enhance security by:

- improving awareness of the need to protect system resources;
- developing skills and knowledge so computer users can perform their jobs more securely; and
- building in-depth knowledge, as needed, to design, implement, or operate security programs for organizations and systems.

13.1 Behavior

People are a crucial factor in ensuring the security of computer systems and valuable information resources. Human actions account for a far greater degree of computer-related loss than all other sources combined. Of such losses, the actions of an organization's insiders normally cause far more harm than the actions of outsiders.

13.2 Accountability

Both the dissemination and the enforcement of policy are critical issues that are implemented and strengthened through training programs. Employees cannot be expected to follow policies and procedures of which they are unaware. In addition, enforcing penalties may be difficult if users can claim ignorance when caught doing something wrong.

13.3 Awareness

Awareness stimulates and motivates those being trained to care about security and to remind them of important security practices. Explaining what happens to an organization, its mission, customers, and employees if security fails motivates people to take security seriously.

13.4 Training

The purpose of training is to teach people the skills that will enable them to perform their jobs more securely. This includes teaching people what they should do and how they should (or can) do it. Training can address many levels, from basic security practices to more advanced or specialized skills. It can be specific to one computer system or generic enough to address all systems.

13.5 Education

Security education is more in-depth than security training and is targeted for security professionals and those whose jobs require expertise in security.

13.6 Implementation

An effective computer security awareness and training (CSAT) program requires proper planning, implementation, maintenance, and periodic evaluation. The following seven steps constitute one approach for developing a CSAT program.

13.6.1 Identify Program Scope, Goals, and Objectives

The first step in developing a CSAT program is to determine the program's scope, goals, and objectives. The scope of the CSAT program should provide training to all types of people who interact with computer systems. The scope of the program can be an entire organization or a subunit. Since users need training which relates directly to their use of particular systems, a large organizationwide program may need to be supplemented by more specific programs. In addition, the organization should specifically address whether the program applies to employees only or also to other users of organizational systems.

13.6.2 Identify Training Staff

There are many possible candidates for conducting the training including internal training departments, computer security staff, or contract services. Regardless of who is chosen, it is important that trainers have sufficient knowledge of computer security issues, principles, and techniques. It is also vital that they know how to communicate information and ideas effectively.

13.6.3 Identify Target Audiences

Not everyone needs the same degree or type of computer security information to do their jobs. A CSAT program that distinguishes between groups of people, presents only the information needed by the particular audience, and omits irrelevant information will have the best results. Segmenting audiences (e.g., by their function or familiarity with the system) can also improve the effectiveness of a CSAT program. For larger organizations, some individuals will fit into more than one group. For smaller organizations, segmenting may not be needed.

13.6.4 Motivate Management and Employees

To successfully implement an awareness and training program, it is important to gain the support of management and employees. Consideration should be given to using motivational techniques to show management and employees how their participation in the CSAT program will benefit the organization.

Management.

Employees.

13.6.5 Administer the Program

There are several important considerations for administering the CSAT program.

Visibility.

Training Methods.

Training Topics.

Training Materials.

Training Presentation.

13.6.6 Maintain the Program

Computer technology is an ever-changing field. Efforts should be made to keep abreast of changes in computer technology and security requirements. A training program that meets an organization's needs today may become ineffective when the organization starts to use a new application or changes its environment, such as by connecting to the Internet. Likewise, an awareness program can become obsolete if laws or organization policies change.

13.6.7 Evaluate the Program

It is often difficult to measure the effectiveness of an awareness or training program. Nevertheless, an evaluation should attempt to ascertain how much information is retained, to what extent computer security procedures are being followed, and general attitudes toward computer security. The results of such an evaluation should help identify and correct problems.

13.7 Interdependencies

Training can, and in most cases should, be used to support every control in the handbook. All controls are more effective if designers, implementers, and users are thoroughly trained.

– *Policy.*

– *Security Program Management.*

– *Personnel/User Issues.*

13.8 Cost Considerations

The major cost considerations in awareness, training, and education programs are:

- the cost of preparing and updating materials, including the time of the preparer;
- the cost of those providing the instruction;
- employee time attending courses and lectures or watching videos;
- the cost of outside courses and consultants (both of which may including travel expenses); including course maintenance.

14 SECURITY CONSIDERATIONS IN COMPUTER SUPPORT AND OPERATIONS

Computer support and operations refers to everything done to run a computer system. This includes both system administration and tasks external to the system that support its operation (e.g., maintaining documentation). It does not include system planning or design. The support and operation of any computer system, from a three-person local area network to a worldwide application serving thousands of users, is critical to maintaining the security of a system. Support and operations are routine activities that enable computer systems to function correctly. These include fixing software or hardware problems, loading and maintaining software, and helping users resolve problems.

14.1 User Support

In many organizations, user support takes place through a Help Desk. Help Desks can support an entire organization, a subunit, a specific system, or a combination of these. For smaller systems, the system administrator normally provides direct user support. Experienced users provide informal user support on most systems.

14.2 Software Support

Software is the heart of an organization's computer operations, whatever the size and complexity of the system. Therefore, it is essential that software function correctly and be protected from corruption. There are many elements of software support.

14.3 Configuration Management

Closely related to software support is configuration management the process of keeping track of changes to the system and, if needed, approving them. Configuration management normally addresses hardware, software, networking, and other changes; it can be formal or informal. The primary security goal of configuration management is ensuring that changes to the system do not unintentionally or unknowingly diminish security. Some of the methods discussed under software support, such as inspecting and testing software changes, can be used. Chapter 9 discusses other methods.

14.4 Backups

Support and operations personnel and sometimes users back up software and data. This function is critical to contingency planning. Frequency of backups will depend upon how often data changes and how important those changes are. Program managers should be consulted to determine what backup schedule is appropriate. Also, as a safety measure, it is useful to test that backup copies are actually usable. Finally, backups should be stored securely, as appropriate (discussed below).

14.5 Media Controls

Media controls include a variety of measures to provide physical and environmental protection and accountability for tapes, diskettes, printouts, and other media. From a security perspective, media controls should be designed to prevent the loss of confidentiality, integrity, or availability of information, including data or software, when stored outside the system. This can include storage of information before it is input to the system and after it is output.

14.5.1 Marking

Controlling media may require some form of physical labeling. The labels can be used to identify media with special handling instructions, to locate needed information, or to log

media (e.g., with serial/control numbers or bar codes) to support accountability. Identification is often by colored labels on diskettes or tapes or banner pages on printouts.

14.5.2 Logging

The logging of media is used to support accountability. Logs can include control numbers (or other tracking data), the times and dates of transfers, names and signatures of individuals involved, and other relevant information. Periodic spot checks or audits may be conducted to determine that no controlled items have been lost and that all are in the custody of individuals named in control logs. Automated media tracking systems may be helpful for maintaining inventories of tape and disk libraries.

14.5.3 Integrity Verification

When electronically stored information is read into a computer system, it may be necessary to determine whether it has been read correctly or subject to any modification. The integrity of electronic information can be verified using error detection and correction or, if intentional modifications are a threat, cryptographic-based technologies.

14.5.4 Physical Access Protection

Media can be stolen, destroyed, replaced with a look-alike copy, or lost. Physical access controls, which can limit these problems, include locked doors, desks, file cabinets, or safes.

14.5.5 Environmental Protection

Magnetic media, such as diskettes or magnetic tape, require environmental protection, since they are sensitive to temperature, liquids, magnetism, smoke, and dust. Other media (e.g., paper and optical storage) may have different sensitivities to environmental factors.

14.5.6 Transmittal

Media control may be transferred both within the organization and to outside elements. Possibilities for securing such transmittal include sealed and marked envelopes, authorized messenger or courier, or U.S. certified or registered mail.

14.5.7 Disposition

When media is disposed of, it may be important to ensure that information is not improperly disclosed. This applies both to media that is external to a computer system (such as a diskette) and to media inside a computer system, such as a hard disk. The process of removing information from media is called sanitization.

14.5.7 Disposition

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently. The security of a system also needs to be documented. This includes many types of documentation, such as security plans, contingency plans, risk analyses, and security policies and procedures. Much of this information, particularly risk and threat analyses, has to be protected against unauthorized disclosure. Security documentation also needs to be both current and accessible. Accessibility should take special factors into account (such as the need to find the contingency plan during a disaster).

14.6 Documentation

Documentation of all aspects of computer support and operations is important to ensure continuity and consistency. Formalizing operational practices and procedures with sufficient

detail helps to eliminate security lapses and oversights, gives new personnel sufficiently detailed instructions, and provides a quality assurance function to help ensure that operations will be performed correctly and efficiently.

The security of a system also needs to be documented. This includes many types of documentation, such as security plans, contingency plans, risk analyses, and security policies and procedures. Much of this information, particularly risk and threat analyses, has to be protected against unauthorized disclosure. Security documentation also needs to be both current and accessible. Accessibility should take special factors into account (such as the need to find the contingency plan during a disaster).

14.7 Maintenance

System maintenance requires either physical or logical access to the system. Support and operations staff, hardware or software vendors, or third-party service providers may maintain a system. Maintenance may be performed on site, or it may be necessary to move equipment to a repair site. Maintenance may also be performed remotely via communications connections. If someone who does not normally have access to the system performs maintenance, then a security vulnerability is introduced.

14.8 Interdependencies

There are support and operations components in most of the controls discussed in this handbook.

- *Personnel.*
- *Incident Handling.*
- *Contingency Planning.*
- *Security Awareness, Training, and Education.*
- *Physical and Environmental.*
- *Technical Controls.*
- *Assurance.*

14.9 Cost Considerations

The cost of ensuring adequate security in day-to-day support and operations is largely dependent upon the size and characteristics of the operating environment and the nature of the processing being performed. If sufficient support personnel are already available, it is important that they be trained in the security aspects of their assigned jobs; it is usually not necessary to hire additional support and operations security specialists. Training, both initial and ongoing, is a cost of successfully incorporating security measures into support and operations activities.

15 PHYSICAL AND ENVIRONMENTAL SECURITY

The term *physical and environmental security*, as used in this chapter, refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Physical and environmental security controls include the following three broad areas:

1. The physical facility is usually the building, other structure, or vehicle housing the system and network components. Systems can be characterized, based upon their operating location, as static, mobile, or portable. Static systems are installed in structures at fixed locations. Mobile systems are installed in vehicles that perform the function of a structure, but not at a fixed location. Portable systems are not installed in fixed operating locations. They may be operated in wide variety of locations, including buildings or vehicles, or in the open. The physical characteristics of these structures and vehicles determine the level of such physical threats as fire, roof leaks, or unauthorized access;
2. The facility's general geographic operating location determines the characteristics of natural threats, which include earthquakes and flooding; man-made threats such as burglary, civil

disorders, or interception of transmissions and emanations; and damaging nearby activities, including toxic chemical spills, explosions, fires, and electromagnetic interference from emitters, such as radars;

3. Supporting facilities are those services (both technical and human) that underpin the operation of the system. The system's operation usually depends on supporting facilities such as electric power, heating and air conditioning, and telecommunications. The failure or substandard performance of these facilities may interrupt operation of the system and may cause physical damage to system hardware or stored data.

15.1 Physical Access Controls

Physical access controls restrict the entry and exit of personnel (and often equipment and media) from an area, such as an office building, suite, data center, or room containing a LAN server.

The controls over physical access to the elements of a system can include controlled areas, barriers that isolate each area, entry points in the barriers, and screening measures at each of the entry points. In addition, staff members who work in a restricted area serve an important role in providing physical security, as they can be trained to challenge people they do not recognize.

15.2 Fire Safety Factors

Building fires are a particularly important security threat because of the potential for complete destruction of both hardware and data, the risk to human life, and the pervasiveness of the damage. Smoke, corrosive gases, and high humidity from a localized fire can damage systems throughout an entire building. Consequently, it is important to evaluate the fire safety of buildings that house systems. Following are important factors in determining the risks from fire.

- *Ignition Sources.*
- *Fuel Sources.*
- *Building Operation.*
- *Building Occupancy.*
- *Fire Detection.*
- *Fire Extinguishment.*

15.3 Failure of Supporting Utilities

Systems and the people who operate them need to have a reasonably well-controlled operating environment. Consequently, failures of heating and air-conditioning systems will usually cause a service interruption and may damage hardware. These utilities are composed of many elements, each of which must function properly.

15.4 Structural Collapse

A building may be subjected to a load greater than it can support. Most commonly this is a result of an earthquake, a snow load on the roof beyond design criteria, an explosion that displaces or cuts structural members, or a fire that weakens structural members. Even if the structure is not completely demolished, the authorities may decide to ban its further use, sometimes even banning entry to remove materials. This threat applies primarily to high-rise buildings and those with large interior spaces without supporting columns.

15.5 Plumbing Leaks

While plumbing leaks do not occur every day, they can be seriously disruptive. The building's plumbing drawings can help locate plumbing lines that might endanger system hardware. These lines include hot and cold water, chilled water supply and return lines, steam lines, automatic sprinkler lines, fire hose standpipes, and drains. If a building includes a laboratory or manufacturing spaces, there may be other lines that conduct water, corrosive or toxic chemicals, or gases.

15.6 Interception of Data

Depending on the type of data a system processes, there may be a significant risk if the data is intercepted. There are three routes of data interception: direct observation, interception of data transmission, and electromagnetic interception.

- *Direct Observation.*
- *Interception of Data Transmissions.*
- *Electromagnetic Interception.*

15.7 Mobile and Portable Systems

The analysis and management of risk usually has to be modified if a system is installed in a vehicle or is portable, such as a laptop computer. The system in a vehicle will share the risks of the vehicle, including accidents and theft, as well as regional and local risks.

Portable and mobile systems share an increased risk of theft and physical damage. In addition, portable systems can be "misplaced" or left unattended by careless users. Secure storage of laptop computers is often required when they are not in use.

15.8 Approach to Implementation

Like other security measures, physical and environmental security controls are selected because they are cost-beneficial. This does not mean that a user must conduct a detailed cost-benefit analysis for the selection of every control. There are four general ways to justify the selection of controls:

1. *They are required by law or regulation.*
2. *The cost is insignificant, but the benefit is material.*
3. *The security measure addresses a potentially "fatal" security exposure but has a reasonable cost.*
4. *The security measure is estimated to be cost-beneficial.*

15.9 Interdependencies

Physical and environmental security measures rely on and support the proper functioning of many of the other areas discussed in this handbook. Among the most important are the following:

- *Logical Access Controls.*
- *Contingency Planning.*
- *Identification and Authentication (I&A).*
- *Other.*

15.10 Cost Considerations

Costs associated with physical security measures range greatly. Useful generalizations about costs, therefore, are difficult to make. Some measures, such as keeping a door locked, may be a trivial expense. Other features, such as fire-detection and -suppression systems, can be far more costly. Cost considerations should include operation.

16 IDENTIFICATION AND AUTHENTICATION

For most systems, identification and authentication (I&A) is the first line of defense. I&A is a technical measure that prevents unauthorized people (or unauthorized processes) from entering a computer system.

I&A is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability. Access control often requires that the system be able to identify and differentiate among users.

- *Identification* is the means by which a user provides a claimed identity to the system.
- *Authentication* is the means of establishing the validity of this claim.

There are three means of authenticating a user's identity which can be used alone or in combination:

- something the individual knows (a secret e.g., a password, Personal Identification Number (PIN), or cryptographic key);
- something the individual possesses (a token e.g., an ATM card or a smart card); and
- something the individual is (a biometric e.g., such characteristics as a voice pattern, handwriting dynamics, or a fingerprint).

16.1 I&A Based on Something the User Knows

The most common form of I&A is a user ID coupled with a password. This technique is based solely on something the user knows. There are other techniques besides conventional passwords that are based on knowledge, such as knowledge of a cryptographic key.

16.1.1 Passwords

In general, password systems work by requiring the user to enter a user ID and password (or passphrase or personal identification number). The system compares the password to a previously stored password for that user ID. If there is a match, the user is authenticated and granted access.

Benefits of Passwords.

Problems With Passwords.

Passwords Used as Access Control.

16.1.2 Cryptographic Keys

Although the authentication derived from the knowledge of a cryptographic key may be based entirely on something the user knows, it is necessary for the user to also possess (or have access to) something that can perform the cryptographic computations, such as a PC or a smart card. For this reason, the protocols used are discussed in the Smart Tokens section of this chapter. However, it is possible to implement these types of protocols without using a smart token. Additional discussion is also provided under the Single Log-in section.

16.2 I&A Based on Something the User Possesses

Although some techniques are based solely on something the user possesses, most of the techniques described in this section are combined with something the user knows. This combination can provide significantly stronger security than either something the user knows or possesses alone.

16.2.1 Memory Tokens

Memory tokens store, but do not process, information. Special reader/writer devices control the writing and reading of data to and from the tokens. The most common type of memory token is a magnetic striped card, in which a thin stripe of magnetic material is affixed to the surface of a card (e.g., as on the back of credit cards). A common application of memory tokens for authentication to computer systems is the automatic teller machine (ATM) card. This uses a combination of something the user possesses (the card) with something the user knows (the PIN).

16.2.2 Smart Tokens

A smart token expands the functionality of a memory token by incorporating one or more integrated circuits into the token itself. When used for authentication, a smart token is another example of authentication based on something a user possesses (i.e., the token itself). A smart token typically requires a user also to provide something the user knows (i.e., a PIN or password) in order to "unlock" the smart token for use.

I&A Based on Something the User Is (16.3)

Biometric authentication technologies use the unique characteristics (or attributes) of an individual to authenticate that person's identity. These include physiological attributes (such as fingerprints, hand geometry, or retina patterns) or behavioral attributes (such as voice

patterns and hand-written signatures). Biometric authentication technologies based upon these attributes have been developed for computer log-in applications.

16.3 I&A Based on Something the User Is

Some of the important implementation issues for I&A systems include administration, maintaining authentication, and single log-in.

16.4.1 Administration

Administration of authentication data is a critical element for all types of authentication systems. The administrative overhead associated with I&A can be significant. I&A systems need to create, distribute, and store authentication data. For passwords, this includes creating passwords, issuing them to users, and maintaining a password file. Token systems involve the creation and distribution of tokens/PINs and data that tell the computer how to recognize valid tokens/PINs. For biometric systems, this includes creating and storing profiles;

16.4.2 Maintaining Authentication

So far, this chapter has discussed initial authentication only. It is also possible for someone to use a legitimate user's account after log-in. Many computer systems handle this problem by logging a user out or locking their display or session after a certain period of inactivity. However, these methods can affect productivity and can make the computer less user-friendly;

16.4.3 Single Log-in

From an efficiency viewpoint, it is desirable for users to authenticate themselves only once and then to be able to access a wide variety of applications and data available on local and remote systems, even if those systems require users to authenticate themselves. This is known as single log-in. If the access is within the same host computer, then the use of a modern access control system (such as an access control list) should allow for a single log-in. If the access is across multiple platforms, then the issue is more complicated, as discussed below. There are three main techniques that can provide single log-in across multiple computers: host-to-host authentication, authentication servers, and user-to-host authentication.

Host-to-Host Authentication.

Authentication Servers.

User-to-Host.

16.5 Interdependencies

There are many interdependencies among I&A and other controls. Several of them have been discussed in the chapter.

- *Logical Access Controls.*
- *Audit.*
- *Cryptography.*

16.6 Cost Considerations

In general, passwords are the least expensive authentication technique and generally the least secure. They are already embedded in many systems. Memory tokens are less expensive than smart tokens, but have less functionality. Smart tokens with a human interface do not require readers, but are more inconvenient to use. Biometrics tend to be the most expensive.

17 LOGICAL ACCESS CONTROL

On many multiuser systems, requirements for using (and prohibitions against the use of) various computer resources vary considerably. Typically, for example, some information must be accessible to all users, some may be needed by several groups or departments, and some should be accessed by only a few individuals. While it is obvious that users must have access to the

information they need to do their jobs, it may also be required to deny access to non-job-related information. It may also be important to control the kind of access that is afforded (e.g., the ability for the average user to execute, but not change, system programs). These types of access restrictions enforce policy and help ensure that unauthorized actions are not taken.

17.1 Access Criteria

In deciding whether to permit someone to use a system resource logical access controls examine whether the user is authorized for the type of access requested. (Note that this inquiry is usually distinct from the question of whether the user is authorized to use the system at all, which is usually addressed in an identification and authentication process).

17.1.1 Identity

It is probably fair to say that the majority of access controls are based upon the identity of the user (either human or process), which is usually obtained through identification and authentication (I&A). (See Chapter 16.) The identity is usually unique, to support individual accountability, but can be a group identification or can even be anonymous. For example, public information dissemination systems may serve a large group called "researchers" in which the individual researchers are not known.

17.1.2 Roles

Access to information may also be controlled by the job assignment or function (i.e., the role) of the user who is seeking access. Examples of roles include data entry clerk, purchase officer, project leader, programmer, and technical editor. Access rights are grouped by role name, and the use of resources is restricted to individuals authorized to assume the associated role. An individual may be authorized for more than one role, but may be required to act in only a single role at a time. Changing roles may require logging out and then in again, or entering a role-changing command. Note that use of roles is not the same as shared-use accounts. An individual may be assigned a standard set of rights of a shipping department data entry clerk, for example, but the account would still be tied to that individual's identity to allow for auditing. (See Chapter 18.)

17.1.3 Location

Access to particular system resources may also be based upon physical or logical location. For example, in a prison, all users in areas to which prisoners are physically permitted may be limited to read-only access. Changing or deleting is limited to areas to which prisoners are denied physical access. The same authorized users (e.g., prison guards) would operate under significantly different logical access controls, depending upon their physical location. Similarly, users can be restricted based upon network addresses (e.g., users from sites within a given organization may be permitted greater access than those from outside).

17.1.4 Time

Time-of-day or day-of-week restrictions are common limitations on access. For example, use of confidential personnel files may be allowed only during normal working hours and maybe denied before 8:00 a.m. and after 6:00 p.m. and all day during weekends and holidays.

17.1.5 Transaction

Another approach to access control can be used by organizations handling transactions (e.g., account inquiries). Phone calls may first be answered by a computer that requests that callers key in their account number and perhaps a PIN. Some routine transactions can then be made directly, but more complex ones may require human intervention. In such cases, the computer, which already knows the account number, can grant a clerk, for example, access to a particular account for the duration of the transaction. When completed, the access authorization is terminated. This means that users have no choice in which accounts they have access to, and can reduce the potential for mischief. It also

eliminates employee browsing of accounts (e.g., those of celebrities or their neighbors) and can thereby heighten privacy.

17.1.6 Service Constraints

Service constraints refer to those restrictions that depend upon the parameters that may arise during use of the application or that are preestablished by the resource owner/manager. For example, a particular software package may only be licensed by the organization for five users at a time. Access would be denied for a sixth user, even if the user were otherwise authorized to use the application. Another type of service constraint is based upon application content or numerical thresholds.

17.1.7 Common Access Modes

In addition to considering criteria for when access should occur, it is also necessary to consider the types of access, or access modes. The concept of access modes is fundamental to access control.

17.2 Policy: The Impetus for Access Controls

Logical access controls are a technical means of implementing policy decisions. Policy is made by a management official responsible for a particular system, application, subsystem, or group of systems. The development of an access control policy may not be an easy endeavor. It requires balancing the often-competing interests of security, operational requirements, and userfriendliness. In addition, technical constraints have to be considered.

17.3 Technical Implementation Mechanisms

Many mechanisms have been developed to provide internal and external access controls, and they vary significantly in terms of precision, sophistication, and cost. These methods are not mutually exclusive and are often employed in combination. Managers need to analyze their organization's protection requirements to select the most appropriate, costeffective logical access controls.

17.3.1 Internal Access Controls

Internal access controls are a logical means of separating what defined users (or user groups) can or cannot do with system resources. Five methods of internal access control are discussed in this section: passwords, encryption, access control lists, constrained user interfaces, and labels.

17.3.1.1 Passwords – Passwords are most often associated with user authentication. (See Chapter 16.) However, they are also used to protect data and applications on many systems, including PCs. For instance, an accounting application may require a password to access certain financial data or to invoke a restricted application (or function of an application).

17.3.1.2 Encryption – Another mechanism that can be used for logical access control is encryption. Encrypted information can only be decrypted by those possessing the appropriate cryptographic key. This is especially useful if strong physical access controls cannot be provided, such as for laptops or floppy diskettes. Thus, for example, if information is encrypted on a laptop computer, and the laptop is stolen, the information cannot be accessed. While encryption can provide strong access control, it is accompanied by the need for strong key management. Use of encryption may also affect availability.

17.3.1.3 Access Control Lists – Access Control Lists (ACLs) refer to a register of: (1) users (including groups, machines, processes) who have been given permission to use a particular system resource, and (2) the types of access they have been permitted.

17.3.1.4 Constrained User Interfaces – Often used in conjunction with ACLs are constrained user interfaces, which restrict users' access to specific functions by never allowing them to request the use of information, functions, or other specific system

resources for which they do not have access. Three major types exist: (1) menus, (2) database views, and (3) physically constrained user interfaces.

- 17.3.1.5 Security Labels – A security label is a designation assigned to a resource (such as a file). Labels can be used for a variety of purposes, including controlling access, specifying protective measures, or indicating additional handling instructions. In many implementations, once this designator has been set, it cannot be changed (except perhaps under carefully controlled conditions that are subject to auditing).

17.3.2 External Access Controls

External access controls are a means of controlling interactions between the system and outside people, systems, and services. External access controls use a wide variety of methods, often including a separate physical device (e.g., a computer) that is between the system being protected and a network.

- 17.3.2.1 Port Protection Devices – Fitted to a communications port of a host computer, a port protection device (PPD) authorizes access to the port itself, prior to and independent of the computer's own access control functions. A PPD can be a separate device in the communications stream, or it may be incorporated into a communications device (e.g., a modem). PPDs typically require a separate authenticator, such as a password, in order to access the communications port.

- 17.3.2.2 Secure Gateways/Firewalls – Often called firewalls, secure gateways block or filter access between two networks, often between a private network and a larger, more public network such as the Internet, which attract malicious hackers. Secure gateways allow internal users to connect to external networks and at the same time prevent malicious hackers from compromising the internal systems.

- 17.3.2.3 Host-Based Authentication – Host-based authentication grants access based upon the identity of the host originating the request, instead of the identity of the user making the request. Many network applications in use today use host-based authentication to determine whether access is allowed. Under certain circumstances it is fairly easy to masquerade as the legitimate host, especially if the masquerading host is physically located close to the host being impersonated. Security measures to protect against misuse of some host-based authentication systems are available (e.g., Secure RPC uses DES to provide a more secure identification of the client host).

17.4 Administration of Access Controls

One of the most complex and challenging aspects of access control, administration involves implementing, monitoring, modifying, testing, and terminating user accesses on the system. These can be demanding tasks, even though they typically do not include making the actual decisions as to the type of access each user may have. Decisions regarding accesses should be guided by organizational policy, employee job descriptions and tasks, information sensitivity, user "need-to-know" determinations, and many other factors.

17.4.1 Centralized Administration

Using centralized administration, one office or individual is responsible for configuring access controls. As users' information processing needs change, their accesses can be modified only through the central office, usually after requests have been approved by the appropriate official. This allows very strict control over information, because the ability to make changes resides with very few individuals. Each user's account can be centrally monitored, and closing all accesses for any user can be easily accomplished if that individual leaves the organization. Since relatively few individuals oversee the process, consistent and uniform procedures and criteria are usually not difficult to enforce. However, when changes are needed quickly, going through a central administration office can be frustrating and time-consuming.

17.4.2 Decentralized Administration

In decentralized administration, access is directly controlled by the owners or creators of the files, often the functional manager. This keeps control in the hands of those most accountable for the information, most familiar with it and its uses, and best able to judge who needs what kind of access. This may lead, however, to a lack of consistency among owners/creators as to procedures and criteria for granting user accesses and capabilities. Also, when requests are not processed centrally, it may be much more difficult to form a systemwide composite view of all user accesses on the system at any given time. Different application or data owners may inadvertently implement combinations of accesses that introduce conflicts of interest or that are in some other way not in the organization's best interest. It may also be difficult to ensure that all accesses are properly terminated when an employee transfers internally or leaves an organization.

17.4.3 Hybrid Approach

A hybrid approach combines centralized and decentralized administration. One typical arrangement is that central administration is responsible for the broadest and most basic accesses, and the owners/creators of files control types of accesses or changes in users' abilities for the files under their control. The main disadvantage to a hybrid approach is adequately defining which accesses should be assignable locally and which should be assignable centrally.

17.5 Coordinating Access Controls

It is vital that access controls protecting a system work together. At a minimum, three basic types of access controls should be considered: physical, operating system, and application. In general, access controls within an application are the most specific. However, for application access controls to be fully effective they need to be supported by operating system access controls. Otherwise access can be made to application resources without going through the application. Operating system and application access controls need to be supported by physical access controls.

17.6 Interdependencies

Logical access controls are closely related to many other controls. Several of them have been discussed in the chapter.

- *Policy and Personnel.*
- *Audit Trails.*
- *Identification and Authentication.*
- *Physical Access Control.*

17.7 Cost Considerations

Incorporating logical access controls into a computer system involves the purchase or use of access control mechanisms, their implementation, and changes in user behavior.

18 AUDIT TRAILS

Audit trails maintain a record of system activity both by system and application processes and by user activity of systems and applications. In conjunction with appropriate tools and procedures, audit trails can assist in detecting security violations, performance problems, and flaws in applications.

18.1 Benefits and Objectives

Audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem analysis.

18.1.1 Individual Accountability

Audit trails are a technical mechanism that help managers maintain individual accountability. By advising users that they are personally accountable for their actions, which are tracked by an audit trail that logs user activities, managers can help promote proper user behavior. Users are less likely to attempt to circumvent security policy if they know that their actions will be recorded in an audit log.

18.1.2 Reconstruction of Events

Audit trails can also be used to reconstruct events after a problem has occurred. Damage can be more easily assessed by reviewing audit trails of system activity to pinpoint how, when, and why normal operations ceased. Audit trail analysis can often distinguish between operator-induced errors (during which the system may have performed exactly as instructed) or system-created errors (e.g., arising from a poorly tested piece of replacement code).

18.1.3 Intrusion Detection

If audit trails have been designed and implemented to record appropriate information, they can assist in intrusion detection. Although normally thought of as a real-time effort, intrusions can be detected in real time, by examining audit records as they are created (or through the use of other kinds of warning flags/notices), or after the fact (e.g., by examining audit records in a batch process).

18.1.4 Problem Analysis

Audit trails may also be used as on-line tools to help identify problems other than intrusions as they occur. This is often referred to as real-time auditing or monitoring. If a system or application is deemed to be critical to an organization's business or mission, real-time auditing may be implemented to monitor the status of these processes (although, as noted above, there can be difficulties with real-time analysis). An analysis of the audit trails may be able to verify that the system operated normally (i.e., that an error may have resulted from operator error, as opposed to a system-originated error). Such use of audit trails may be complemented by system performance logs.

18.2 Audit Trails and Logs

A system can maintain several different audit trails concurrently. There are typically two kinds of audit records, (1) an event-oriented log and (2) a record of every keystroke, often called keystroke monitoring. Event-based logs usually contain records describing system events, application events, or user events.

18.2.1 Keystroke Monitoring

Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. Examples of keystroke monitoring would include viewing characters as they are typed by users, reading users' electronic mail, and viewing other recorded information typed by users.

18.2.2 Audit Events

System audit records are generally used to monitor and fine-tune system performance. Application audit trails may be used to discern flaws in applications, or violations of security policy committed within an application. User audits records are generally used to hold individuals accountable for their actions. An analysis of user audit records may expose a variety of security violations, which might range from simple browsing to attempts to plant Trojan horses or gain unauthorized privileges.

18.2.2.1 System-Level Audit Trails – If a system-level audit capability exists, the audit trail should capture, at a minimum, any attempt to log on (successful or unsuccessful), the log-on ID, date and time of each log-on attempt, date and time of each log-off, the devices used, and the function(s) performed once logged on (e.g., the applications that

the user tried, successfully or unsuccessfully, to invoke). System-level logging also typically includes information that is not specifically security-related, such as system operations, cost-accounting charges, and network performance.

18.2.2.2 Application-Level Audit Trails – System-level audit trails may not be able to track and log events within applications, or may not be able to provide the level of detail needed by application or data owners, the system administrator, or the computer security manager. In general, application-level audit trails monitor and log user activities, including data files opened and closed, specific actions, such as reading, editing, and deleting records or fields, and printing reports. Some applications may be sensitive enough from a data availability, confidentiality, and/or integrity perspective that a "before" and "after" picture of each modified record (or the data element(s) changed within a record) should be captured by the audit trail.

18.2.2.3 User Audit Trails – User audit trails can usually log:

- all commands directly initiated by the user;
- all identification and authentication attempts; and
- files and resources accessed.

18.3 Implementation Issues

Audit trail data requires protection, since the data should be available for use when needed and is not useful if it is not accurate. Also, the best planned and implemented audit trail is of limited value without timely review of the logged data. Audit trails may be reviewed periodically, as needed (often triggered by occurrence of a security event), automatically in realtime, or in some combination of these. System managers and administrators, with guidance from computer security personnel, should determine how long audit trail data will be maintained either on the system or in archive files.

18.3.1 Protecting Audit Trail Data

Access to on-line audit logs should be strictly controlled. Computer security managers and system administrators or managers should have access for review purposes; however, security and/or administration personnel who maintain logical access functions may have no need for access to audit logs.

18.3.2 Review of Audit Trails

Audit trails can be used to review what occurred after an event, for periodic reviews, and for realtime analysis. Reviewers should know what to look for to be effective in spotting unusual activity. They need to understand what normal activity looks like. Audit trail review can be easier if the audit trail function can be queried by user ID, terminal ID, application name, date and time, or some other set of parameters to run reports of selected information.

18.3.3 Tools for Audit Trail Analysis

Many types of tools have been developed to help to reduce the amount of information contained in audit records, as well as to distill useful information from the raw data. Especially on larger systems, audit trail software can create very large files, which can be extremely difficult to analyze manually. The use of automated tools is likely to be the difference between unused audit trail data and a robust program.

18.4 Interdependencies

The ability to audit supports many of the controls presented in this handbook. The following paragraphs describe some of the most important interdependencies.

- *Policy.*
- *Assurance.*
- *Identification and Authentication.*
- *Logical Access Control.*
- *Contingency Planning.*

– *Cryptography.*

18.5 Cost Considerations

Audit trails involve many costs. First, some system overhead is incurred recording the audit trail. Additional system overhead will be incurred storing and processing the records. The more detailed the records, the more overhead is required. Another cost involves human and machine time required to do the analysis. This can be minimized by using tools to perform most of the analysis. Many simple analyzers can be constructed quickly (and cheaply) from system utilities, but they are limited to audit reduction and identifying particularly sensitive events. More complex tools that identify trends or sequences of events are slowly becoming available as off-the-shelf software. (If complex tools are not available for a system, development may be prohibitively expensive. Some intrusion detection systems, for example, have taken years to develop).

19 CRYPTOGRAPHY

Cryptography is a branch of mathematics based on the transformation of data. It provides an important tool for protecting information and is used in many aspects of computer security. For example, cryptography can help provide data confidentiality, integrity, electronic signatures, and advanced user authentication. Although modern cryptography relies upon advanced mathematics, users can reap its benefits without understanding its mathematical underpinnings.

19.1 Basic Cryptographic Technologies

Cryptography relies upon two basic components: an algorithm (or cryptographic methodology) and a key. In modern cryptographic systems, algorithms are complex mathematical formulae and keys are strings of bits. For two parties to communicate, they must use the same algorithm (or algorithms that are designed to work together). In some cases, they must also use the same key. Many cryptographic keys must be kept secret; sometimes algorithms are also kept secret.

19.1.1 Secret Key Cryptography

In secret key cryptography, two (or more) parties share the same key, and that key is used to encrypt and decrypt data. As the name implies, secret key cryptography relies on keeping the key secret. If the key is compromised, the security offered by cryptography is severely reduced or eliminated. Secret key cryptography assumes that the parties who share a key rely upon each other not to disclose the key and protect it against modification.

19.1.2 Public Key Cryptography

Whereas secret key cryptography uses a single key shared by two (or more) parties, public key cryptography uses a pair of keys for each party. One of the keys of the pair is "public" and the other is "private." The public key can be made known to other parties; the private key must be kept confidential and must be known only to its owner. Both keys, however, need to be protected against modification.

19.1.3 Hybrid Cryptographic Systems

Public and secret key cryptography have relative advantages and disadvantages. Although public key cryptography does not require users to share a common key, secret key cryptography is much faster: equivalent implementations of secret key cryptography can run 1,000 to 10,000 times faster than public key cryptography.

19.1.4 Key Escrow

Because cryptography can provide extremely strong encryption, it can thwart the government's efforts to lawfully perform electronic surveillance. For example, if strong cryptography is used to encrypt a phone conversation, a court-authorized wiretap will not be effective. To meet the needs of the government and to provide privacy, the

federal government has adopted voluntary key escrow cryptography. This technology allows the use of strong encryption, but also allows the government when legally authorized to obtain decryption keys held by escrow agents. NIST has published the Escrowed Encryption Standard as FIPS 185. Under the Federal Government's voluntary key escrow initiative, the decryption keys are split into parts and given to separate escrow authorities. Access to one part of the key does not help decrypt the data; both keys must be obtained.

19.2 Uses of Cryptography

Cryptography is used to protect data both inside and outside the boundaries of a computer system. Outside the computer system, cryptography is sometimes the only way to protect data. While in a computer system, data is normally protected with logical and physical access controls (perhaps supplemented by cryptography). However, when in transit across communications lines or resident on someone else's computer, data cannot be protected by the originator's logical or physical access controls. Cryptography provides a solution by protecting data even when the data is no longer in the control of the originator.

19.2.1 Data Encryption

One of the best ways to obtain costeffective data confidentiality is through the use of encryption. Encryption transforms intelligible data, called plaintext, into an unintelligible form, called ciphertext. This process is reversed through the process of decryption. Once data is encrypted, the ciphertext does not have to be protected against disclosure. However, if ciphertext is modified, it will not decrypt correctly.

19.2.2 Integrity

In computer systems, it is not always possible for humans to scan information to determine if data has been erased, added, or modified. Even if scanning were possible, the individual may have no way of knowing what the correct data should be. For example, "do" may be changed to "do not," or \$1,000 may be changed to \$10,000. It is therefore desirable to have an automated means of detecting both intentional and unintentional modifications of data.

19.2.3 Electronic Signatures

Today's computer systems store and process increasing numbers of paper-based documents in electronic form. Having documents in electronic form permits rapid processing and transmission and improves overall efficiency. However, approval of a paper document has traditionally been indicated by a written signature. What is needed, therefore, is the electronic equivalent of a written signature that can be recognized as having the same legal status as a written signature. In addition to the integrity protections, discussed above, cryptography can provide a means of linking a document with a particular person, as is done with a written signature. Electronic signatures can use either secret key or public key cryptography; however, public key methods are generally easier to use.

19.2.3.1 Secret Key Electronic Signatures – An electronic signature can be implemented using secret key message authentication codes (MACs). For example, if two parties share a secret key, and one party receives data with a MAC that is correctly verified using the shared key, that party may assume that the other party signed the data. This assumes, however, that the two parties trust each other. Thus, through the use of a MAC, in addition to data integrity, a form of electronic signature is obtained. Using additional controls, such as key notarization and key attributes, it is possible to provide an electronic signature even if the two parties do not trust each other.

19.2.3.2 Public Key Electronic Signatures – Another type of electronic signature called a digital signature is implemented using public key cryptography. Data is electronically signed by applying the originator's private key to the data. (The exact

mathematical process for doing this is not important for this discussion.) To increase the speed of the process, the private key is applied to a shorter form of the data, called a "hash" or "message digest," rather than to the entire set of data. The resulting digital signature can be stored or transmitted along with the data. The signature can be verified by any party using the public key of the signer. This feature is very useful, for example, when distributing signed copies

19.2.4 User Authentication

Cryptography can increase security in user authentication techniques. As discussed in Chapter 16, cryptography is the basis for several advanced authentication methods. Instead of communicating passwords over an open network, authentication can be performed by demonstrating knowledge of a cryptographic key. Using these methods, a one-time password, which is not susceptible to eavesdropping, can be used. User authentication can use either secret or public key cryptography.

19.3 Implementation Issues

This section explores several important issues that should be considered when using (e.g., designing, implementing, integrating) cryptography in a computer system.

19.3.1 Selecting Design and Implementation Standards

NIST and other organizations have developed numerous standards for designing, implementing, and using cryptography and for integrating it into automated systems. By using these standards, organizations can reduce costs and protect their investments in technology. Standards provide solutions that have been accepted by a wide community and that have been reviewed by experts in relevant areas. Standards help ensure interoperability among different vendors' equipment, thus allowing an organization to select from among various products in order to find cost-effective equipment.

19.3.2 Deciding on Hardware vs. Software Implementations

The trade-offs among security, cost, simplicity, efficiency, and ease of implementation need to be studied by managers acquiring various security products meeting a standard. Cryptography can be implemented in either hardware or software. Each has its related costs and benefits.

19.3.3 Managing Keys

The proper management of cryptographic keys is essential to the effective use of cryptography for security. Ultimately, the security of information protected by cryptography directly depends upon the protection afforded to keys.

19.3.4 Security of Cryptographic Modules

Cryptography is typically implemented in a module of software, firmware, hardware, or some combination thereof. This module contains the cryptographic algorithm(s), certain control parameters, and temporary storage facilities for the key(s) being used by the algorithm(s). The proper functioning of the cryptography requires the secure design, implementation, and use of the cryptographic module. This includes protecting the module against tampering.

19.3.5 Applying Cryptography to Networks

The use of cryptography within networking applications often requires special considerations. In these applications, the suitability of a cryptographic module may depend on its capability for handling special requirements imposed by locally attached communications equipment or by the network protocols and software.

19.3.6 Complying with Export Rules

The U.S. Government controls the export of cryptographic implementations. The rules governing export can be quite complex, since they consider multiple factors. In addition, cryptography is a rapidly changing field, and rules may change from time to

time. Questions concerning the export of a particular implementation should be addressed to appropriate legal counsel.

19.4 Interdependencies

There are many interdependencies among cryptography and other security controls highlighted in this handbook. Cryptography both depends on other security safeguards and assists in providing them.

- *Physical Security.*
- *User Authentication.*
- *Logical Access Control.*
- *Audit Trails.*
- *Assurance.*

19.5 Cost Considerations

Using cryptography to protect information has both direct and indirect costs. Cost is determined in part by product availability; a wide variety of products exist for implementing cryptography in integrated circuits, add-on boards or adapters, and stand-alone units.

19.5.1 Direct Costs

The direct costs of cryptography include:

- # Acquiring or implementing the cryptographic module and integrating it into the computer system. The medium (i.e., hardware, software, firmware, or combination) and various other issues such as level of security, logical and physical configuration, and special processing requirements will have an impact on cost.
- # Managing the cryptography and, in particular, managing the cryptographic keys, which includes key generation, distribution, archiving, and disposition, as well as security measures to protect the keys, as appropriate.

19.5.2 Indirect Costs

The indirect costs of cryptography include:

- # A decrease in system or network performance, resulting from the additional overhead of applying cryptographic protection to stored or communicated data.
- # Changes in the way users interact with the system, resulting from more stringent security enforcement. However, cryptography can be made nearly transparent to the users so that the impact is minimal.

SP800-14 – Generally Accepted Principles and Practices for Securing Information Technology Systems

2. Generally Accepted System Security Principles

As the name implies, the principles are generally accepted -- that which is most commonly being used at the present time to secure IT resources. The principles that this document offers are of new to the security profession. They are based on the premise that (most) everyone applies these when developing or maintaining a system and they have become generally accepted.

This document uses the Organization for Economic Co-operation and Development's (OECD) Guidelines for the Security of Information Systems as the base for the principles. The OECD Guidelines were developed in 1992 by a group of international experts to provide a foundation from which governments and the private sector, acting singly and in concert, could construct a framework for securing IT systems. The OECD Guidelines are the current international guidelines which have been endorsed by the United States. A brief description of the nine OECD principles is provided in Figure 1. Using the spirit of the Guidelines, NIST developed principles which applies to federal systems. In developing this set of principles, NIST drew upon the OECD Guidelines, added material, combined some principles, and rewrote others. Most of the rewriting and combining was done to provide clarity. The principles added by NIST are in keeping with the OECD principles but not directly stated.

2.1 Computer Security Supports the Mission of the Organization

The purpose of computer security is to protect an organization's valuable resources, such as information, hardware, and software. Through the selection and application of appropriate safeguards, security helps the organization's mission by protecting its physical and financial resources, reputation, legal position, employees, and other tangible and intangible assets. Unfortunately, security is sometimes viewed as thwarting the mission of the organization by imposing poorly selected, bothersome rules and procedures on users, managers, and systems. On the contrary, well-chosen security rules and procedures do not exist for their own sake -- they are put in place to protect important assets and support the overall organizational mission. Security, therefore, is a means to an end and not an end in itself.

2.2 Computer Security is an Integral Element of Sound Management

Information and IT systems are often critical assets that support the mission of an organization. Protecting them can be as important as protecting other organizational resources, such as money, physical assets, or employees.

However, including security considerations in the management of information and computers does not completely eliminate the possibility that these assets will be harmed. Ultimately, organization managers have to decide what level of risk they are willing to accept, taking into account the cost of security controls.

2.3 Computer Security Should Be Cost-Effective

The costs and benefits of security should be carefully examined in both monetary and nonmonetary terms to ensure that the cost of controls does not exceed expected benefits. Security should be appropriate and proportionate to the value of and degree of reliance on the IT systems and to the severity, probability, and extent of potential harm. Requirements for security vary, depending upon the particular IT system.

2.4 Systems Owners Have Security Responsibilities Outside Their Own Organizations

If a system has external users, its owners have a responsibility to share appropriate knowledge about the existence and general extent of security measures so that other users can be confident that the system is adequately secure. This does not imply that all systems must

meet any minimum level of security, but does imply that system owners should inform their clients or users about the nature of the security.

2.5 Computer Security Responsibilities and Accountability Should Be Made Explicit

The responsibility and accountability of owners, providers, and users of IT systems and other parties concerned with the security of IT systems should be explicit. The assignment of responsibilities may be internal to an organization or may extend across organizational boundaries. Depending on the size of the organization, the computer security program may be large or small, even a collateral duty of another management official. However, even small organizations can prepare a document that states organization policy and makes explicit computer security responsibilities. This element does not specify that individual accountability must be provided for on all systems.

2.6 Computer Security Requires a Comprehensive and Integrated Approach

Providing effective computer security requires a comprehensive approach that considers a variety of areas both within and outside of the computer security field. This comprehensive approach extends throughout the entire information life cycle.

To work effectively, security controls often depend upon the proper functioning of other controls. Many such interdependencies exist. If appropriately chosen, managerial, operational, and technical controls can work together synergistically. On the other hand, without a firm understanding of the interdependencies of security controls, they can actually undermine one another.

2.7 Computer Security Should Be Periodically Reassessed

Computers and the environments in which they operate are dynamic. System technology and users, data and information in the systems, risks associated with the system, and security requirements are ever-changing. Many types of changes affect system security: technological developments (whether adopted by the system owner or available for use by others); connection to external networks; a change in the value or use of information; or the emergence of a new threat.

2.8 Computer Security is Constrained by Societal Factors

The ability of security to support the mission of an organization may be limited by various factors, such as social issues. For example, security and workplace privacy can conflict. Commonly, security is implemented on an IT system by identifying users and tracking their actions. However, expectations of privacy vary and can be violated by some security measures. (In some cases, privacy may be mandated by law).

3. Common IT Security Practices

The goal of this chapter is to assist the time-constrained security manager in reviewing their current policies and procedures against the common practices presented here. The list is not exhaustive; agencies should consider them as the minimum set. These practices are the ones currently employed in an effective computer security program. They do not take into account environmental or technological constraints, nor are they relevant to every situation. This chapter should be augmented with additional practices based on each agencies' unique requirements.

3.1 Policy

The term computer security policy has more than one meaning. Policy is senior management's directives to create a computer security program, establish its goals, and assign responsibilities. The term policy is also used to refer to the specific security rules for particular systems. Additionally, policy may refer to entirely different matters, such as the specific managerial decisions setting an organization's e-mail privacy policy or fax security policy.

3.1.1 Program Policy

An organization's program policy should:

- # *Create and Define a Computer Security Program.*
- # *Set Organizational Strategic Directions.*
- # *Assign Responsibilities.*
- # *Address Compliance Issues.*

3.1.2 Issue-Specific Policy

An organization's issue-specific policies should:

- # *Address Specific Areas.*
- # *Be Updated Frequently.*
- # *Contain an Issue Statement.*

3.1.3 System-Specific Policy

An organization's system-specific policies should:

- # *Focus on Decisions.*
- # *Be Made by Management Official.*
- # *Vary From System to System.*
- # *Be Expressed as Rules.*

3.1.4 All Policies

All three types of policy should be:

- # *Supplemented.*
- # *Visible.*
- # *Supported by Management.*
- # *Consistent.*

3.2 Program Management

Managing computer security at multiple levels brings many benefits. Each level contributes to the overall computer security program with different types of expertise, authority, and resources. In general, executive managers (such as those at the headquarters level) better understand the organization as a whole and have more authority. On the other hand, front-line managers (at the computer facility and applications levels) are more familiar with the specific requirements, both technical and procedural, and problems of the systems and the users. The levels of computer security program management should be complementary; each can help the other be more effective. Many organizations have at least two levels of computer security management; the central level and the system level.

3.2.1 Central Security Program

A central security program should provide distinct types of benefits: increased efficiency and economy of security throughout the organization and the ability to provide centralized enforcement and oversight. It should have the following:

- # *Stable Program Management Function.*
- # *Existence of Policy.*
- # *Published Mission and Functions Statement.*
- # *Long-Term Computer Security Strategies.*
- # *Compliance Program.*
- # *Intraorganizational Liaison.*
- # *Liaison with External Groups.*

3.2.2 System-Level Program

While the central program addresses the entire spectrum of computer security for an organization, system-level computer security programs ensure appropriate and cost-effective security for each system. System-level computer security programs may address, for example, the computing resources within an operational element, a major

application, or a group of similar systems (either technologically or functionally). They should have the following:

- # *System-Specific Security Policy.*
- # *Life Cycle Management.*
- # *Appropriate Integration with System Operations.*

3.3 Risk Management

Risk is the possibility of something adverse happening. Risk management is the process of assessing risk, taking steps to reduce risk to an acceptable level and maintaining that level of risk. Risk management requires the analysis of risk, relative to potential benefits, consideration of alternatives, and, finally, implementation of what management determines to be the best course of action. Risk management consists of two primary and one underlying activity; risk assessment and risk mitigation are the primary activities and uncertainty analysis is the underlying one. An organization should consider the following when assessing risks.

Risk Assessment (3.3.1)

Risk assessment, the process of analyzing and interpreting risk, is comprised of three basic activities:

- # *Determine the Assessment's Scope and Methodology.*
- # *Collecting and Analyzing Data.*
- # *Interpreting Risk Assessment Results.*

3.3.2 Risk Mitigation

Risk mitigation involves the selection and implementation of security controls to reduce risk to a level acceptable to management. Although there is flexibility in how risk assessment is conducted, the process of risk mitigation has greater flexibility than the sequence of events conducted in a risk assessment. The following activities are discussed in a specific sequence; however, they need not be performed in that sequence:

- # *Select Safeguards.*
- # *Accept Residual Risk.*
- # *Implementing Controls and Monitoring Effectiveness.*

3.3.3 Uncertainty Analysis

Risk management must often rely on speculation, best guesses, incomplete data, and many unproven assumptions. An uncertainty analysis should be performed and documented so that the risk management results can be used knowledgeably. There are two primary sources of uncertainty in the risk management process: (1) a lack of confidence or precision in the risk management model or methodology, and (2) a lack of sufficient information to determine the exact value of the elements of the risk model, such as threat frequency, safeguard effectiveness, or consequences.

3.4 Life Cycle Planning

Security, like other aspects of an IT system, is best managed if planned for throughout the IT system life cycle. There are many models for the IT system life cycle but most contain five basic phases: initiation, development/acquisition, implementation, operation, and disposal.

3.4.1 Security Plan

Organizations should ensure that security activities are accomplished during each of the phases.

- # *Prepare a Security Plan.*

3.4.2 Initiation Phase

During the initiation phase, the need for a system is expressed and the purpose of the system is documented.

- # *Conduct a Sensitivity Assessment.*

3.4.3 Development/Acquisition Phase

During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle. The following steps should be considered during this phase:

- # *Determine Security Requirements.*
- # *Incorporate Security Requirements Into Specifications.*
- # *Obtain the System and Related Security Activities.*

3.4.4 Implementation Phase

During implementation, the system is tested and installed or fielded. The following items should be considered during this phase:

- # *Install/Turn-On Controls.*
- # *Security Testing.*
- # *Accreditation.*

3.4.5 Operation/Maintenance Phase

During this phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. The following high-level items should be considered during this phase:

- # *Security Operations and Administration.*
- # *Operational Assurance.*
- # *Audits and Monitoring.*

3.4.6 Disposal Phase

The disposal phase of the IT system life cycle involves the disposition of information, hardware, and software. The following items should be considered during this phase:

- # *Information.*
- # *Media Sanitization.*

3.5 Personnel/User Issues

Many important issues in computer security involve users, designers, implementors, and managers. A broad range of security issues relate to how these individuals interact with computers and the access and authorities they need to do their job. No IT system can be secured without properly addressing these security issues.

Staffing (3.5.1)

An organization's staffing process should generally involve at least the following four steps which apply equally to general users as well as to application managers, system management personnel, and security personnel:

- # *Position Definition (Separation of duties, Least privilege)*
- # *Determining Position Sensitivity.*
- # *Screening.*
- # *Employee Training and Awareness.*

3.5.2 User Administration

Organizations should ensure effective administration of users' computer access to maintain system security, including user account management, auditing and the timely modification or removal of access. The following should be considered:

- # *User Account Management.*
- # *Audit and Management Reviews.*
- # *Detecting Unauthorized/Illegal Activities.*
- # *Friendly Termination.*
- # *Unfriendly Termination.*

3.6 Preparing for Contingencies and Disasters

Contingency planning directly supports an organization's goal of continued operations. Organizations should practice contingency planning because it makes good business sense. Contingency planning addresses how to keep an organization's critical functions operating in the event of disruptions, both large and small. This broad perspective on contingency planning is based on the distribution of computer support throughout an organization. The following six steps describe the basic functions an organization should employ when developing contingency plans.

3.6.1 Business Plan

An organization should identify mission- or business-critical functions. The identification of critical functions is often called a business plan.

- # Identify Functions and Priorities.

3.6.2 Identify Resources

- # Analyze Resources Needed.
- # Overlap of Areas.
- # Common Resources Used.
- # Time Frame Needed.

3.6.3 Develop Scenarios

An organization should anticipate potential contingencies or disasters. The development of scenarios should help an organization develop a plan to address the wide range of things that can go wrong. The following items should be considered:

- # Identify Possible Scenarios.
- # Address Each Resource.

3.6.4 Develop Strategies

The selection of a contingency planning strategy should be based on practical considerations, including feasibility and cost. Risk assessment can be used to help estimate the cost of options to decide on an optimal strategy. For example, is it more expensive to purchase and maintain a generator or to move processing to an alternate site, considering the likelihood of losing electrical power for various lengths of time? Whether the strategy is on-site or off-site, a contingency planning strategy normally consists of three parts: emergency response, recovery, and resumption.

- # Emergency Response.
- # Recovery.
- # Resumption.
- # Implementation.

3.6.5 Test and Revise Plan

An organization should test and revise the contingency plan. A contingency plan should be tested periodically because there will undoubtedly be flaws in the plan and its implementation. The following items should be considered:

- # Keep Current.
- # Test.

3.7 Computer Security Incident Handling

A computer security incident can result from a computer virus, other malicious code, or a system intruder, either an insider or an outsider. The definition of a computer security incident is somewhat flexible and may vary by organization and computing environment. An incident handling capability may be viewed as a component of contingency planning, because it provides the ability to react quickly and efficiently to disruptions in normal processing. Incident handling can be considered that portion of contingency planning that responds to malicious technical threats.

3.7.1 *Uses of a Capability*

An organization should address computer security incidents by developing an incident handling capability. The incident handling capability should be used to:

- # Provide Ability to Respond Quickly and Effectively.
- # Contain and Repair Damage From Incidents.
- # Prevent Future Damage.

3.7.2 *Characteristics*

An incident handling capability should have the following characteristics:

- # Understanding of the Constituency It Will Serve.
- # Educated Constituency.
- # Centralized Communications.
- # Expertise in the Requisite Technologies.
- # Ability to Communicate Effectively.
- # Links to Other Groups.

3.8 Awareness and Training

An effective computer security awareness and training program requires proper planning, implementation, maintenance, and periodic evaluation. In general, a computer security awareness and training program should encompass the following seven steps:

- Identify Program Scope, Goals, and Objectives.
- Identify Training Staff.
- Identify Target Audiences.
- Motivate Management and Employees.
- Administer the Program.
- Maintain the Program.
- Evaluate the Program.

3.9 Security Considerations in Computer Support and Operations

Computer support and operations refers to system administration and tasks external to the system that support its operation (e.g., maintaining documentation). Failure to consider security as part of the support and operations of IT systems is, for many organizations, a significant weakness. Computer security system literature includes many examples of how organizations undermined their often expensive security measures because of poor documentation, no control of maintenance accounts, or other shoddy practices. The following practices are what an organization's support and operation should include:

- User Support.
- Software Support.
- Configuration Management.
- Backups.
- Media Controls.
- Documentation.
- Maintenance.
- Standardized Log-on Banner.

3.10 Physical and Environmental Security

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical and environmental security program should address the following seven topics. In doing so, it can help prevent interruptions in computer services, physical damage, unauthorized disclosure of information, loss of control over system integrity, and theft.

- Physical Access Controls.
- Fire Safety Factors.

- Failure of Supporting Utilities.
- Structural Collapse.
- Plumbing Leaks.
- Interception of Data.
- Mobile and Portable Systems.

3.11 Identification and Authentication

Identification and Authentication is a critical building block of computer security since it is the basis for most types of access control and for establishing user accountability. Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on least privilege, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

3.11.1 Identification

Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID. The following should be considered when using user IDs:

- # Unique Identification.
- # Correlate Actions to Users.
- # Maintenance of User IDs.
- # Inactive User IDs.

3.11.2 Authentication

Authentication is the means of establishing the validity of this claim. There are three means of authenticating a user's identity which can be used alone or in combination: something the individual knows (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key); something the individual possesses (a token -- e.g., an ATM card or a smart card); and something the individual is (a biometric -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint). The following should be considered:

- # Require Users to Authenticate.
- # Restrict Access to Authentication Data.
- # Secure Transmission of Authentication Data.
- # Limit Log-on Attempts.
- # Secure Authentication Data as it is Entered.
- # Administer Data Properly.

3.11.3 Passwords

If passwords are used for authentication, organizations should:

- # Specify Required Attributes.
- # Change Frequently.
- # Train Users.

3.11.4 Advanced Authentication

Advanced authentication, such as a challenge-response system, generally requires more administrative overhead than passwords. If used, organizations should train users in the following:

- # How to Use.
- # Why it is Used.

3.12 Logical Access Control

Access is the ability to do something with a computer resource (e.g., use, change, or view).

Logical access controls are the system-based means by which the ability is explicitly enabled or restricted in some way. Logical access controls can prescribe not only who or what (e.g., in the case of a process) is to have access to a specific system resource but also the type of access that is permitted.

Organizations should implement logical access control based on policy made by a management official responsible for a particular system, application, subsystem, or group of systems. The policy should balance the often-competing interests of security, operational requirements, and user-friendliness. In general, organizations should base access control policy on the principle of least privilege, which states that users should be granted access only to the resources they need to perform their official functions.

3.12.1 Access Criteria

Organizations should control access to resources based on the following access criteria, as appropriate:

- # Identity (user ID).
- # Roles.
- # Location.
- # Time.
- # Transaction.
- # Service Constraints.
- # Access Modes.

3.12.2 Access Control Mechanisms

An organization should consider both internal and external access control mechanisms.

Internal access controls are a logical means of separating what defined users (or user groups) can or cannot do with system resources. External access controls are a means of controlling interactions between the system and outside people, systems, and services. When setting up access controls, organizations should consider the following mechanisms:

- # Access control lists (ACLs).
- # Constrained User Interfaces.
- # Encryption.
- # Port Protection Devices.
- # Secure Gateways/Firewalls.
- # Host-Based Authentication.

3.13 Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. Audit trails should be used for the following:

- Individual Accountability.
- Reconstruction of Events.
- Intrusion Detection.
- Problem Identification.

3.13.1 Contents of Audit Trail Records

An audit trail should include sufficient information to establish what events occurred and who (or what) caused them. Defining the scope and contents of the audit trail should be done carefully to balance security needs with possible performance, privacy, or other costs. In general, an event record should specify:

- # Type of Event.
- # When the Event Occurred.
- # User ID Associated With the Event.
- # Program or Command Used to Initiate the Event.

3.13.2 Audit Trail Security

Organizations should protect the audit trail from unauthorized access. The following precautions should be taken:

- # Control Online Audit Logs.
- # Separation of Duties.
- # Protect Confidentiality.

3.13.3 Audit Trail Reviews

Audit trails should be reviewed periodically. The following should be considered when reviewing audit trails:

- # Recognize Normal Activity.
- # Contain a Search Capability.
- # Follow-up Reviews.

3.13.4 Keystroke Monitoring

Keystroke monitoring is the process used to view or record both the keystrokes entered by a computer user and the computer's response during an interactive session. Keystroke monitoring is usually considered a special case of audit trails. The Department of Justice has advised that an ambiguity in U.S. law makes it unclear whether keystroke monitoring is considered equivalent to an unauthorized telephone wiretap. If keystroke monitoring is used in audit trails, organizations should:

- # Have Written Policy.
- # Notify Users.

3.14 Cryptography

Cryptography is a branch of mathematics based on the transformation of data. It provides an important tool for protecting information and is used in many aspects of computer security. Cryptography is traditionally associated only with keeping data secret. However, modern cryptography can be used to provide many security services, such as electronic signatures and ensuring that data has not been modified. Several important issues should be considered when designing, implementing, and integrating cryptography in an IT system.

- Select Design and Implementation Standards.
- Decide on Hardware vs. Software Implementations.
- Manage Keys.
- Secure Cryptographic Modules.
- Comply with Export Rules.

SP800-18 – Guide for Developing Security Plans for Information Technology Systems

2 System Analysis

Once completed, a security plan will contain technical information about the system, its security requirements, and the controls implemented to provide protection against its risks and vulnerabilities. Before the plan can be developed, a determination must be made as to which type of plan is required for a system. This section walks the reader through an analysis of the system to determine the boundaries of the system and the type of system.

2.1 System Boundaries

Defining what constitutes a “system” for the purposes of this guideline requires an analysis of system boundaries and organizational responsibilities. A system, as defined by this guideline, is identified by constructing logical boundaries around a set of processes, communications, storage, and related resources. The elements within these boundaries constitute a single system requiring a security plan.

2.2 Multiple Similar Systems

An organization may have systems that differ only in the responsible organization or the physical environment in which they are located (e.g., air traffic control systems). In such instances, it is appropriate and recommended to use plans that are identical except for those areas of difference. This approach provides consistent levels of protection for similar systems.

2.3 System Category

The next step is to categorize each system as either a “major application” or as a “general support system.” All applications should be covered by a security plan. The applications will either be covered individually if they have been designated as a major application or within the security plan of a general support system. A system may be designated as a major application even though it is also supported by a system that has been designated as a general support system.

2.3.1 Major Applications

All federal applications have value and require some level of protection. Certain applications, because of the information they contain, process, or transmit or because of their criticality to the organization’s missions, require special management oversight. These applications are major applications.

2.3.2 General Support System

A general support system is interconnected information resources under the same direct management control which shares common functionality. A general support system normally includes hardware, software, information, data, applications, communications, facilities, and people and provides support for a variety of users and/or applications.

3 Plan Development – All Systems

The remainder of this document guides the reader in writing a security plan. This section provides and requires general information that applies to all systems. Note: A template of all sections contained in a security plan is provided in Appendix C. The template is separated into two formats, one for major applications and one for general support systems.

3.1 Plan Control

All security plans, at a minimum, should be marked, handled, and controlled to the level of sensitivity determined by organizational policy. In addition, all security plans should be dated for ease of tracking modifications and approvals. Dating each page of a security plan

may be appropriate if updates are to be made through change pages. All plans begin with the following system identification section.

3.2 System Identification

The first section of the plan provides basic identifying information about the system. Both types of plans must contain general descriptive information regarding who is responsible for the system, the purpose of the system, and the sensitivity level of the system.

3.2.1 System Name/Title

The plan begins with listing the name and title of the system/application. Each system/application should be assigned a unique name/identifier. Assigning a unique identifier to each system helps to ensure that appropriate security requirements are met based on the unique requirements for the system, and that allocated resources are appropriately applied.

3.2.2 Responsible Organization

In this section, list the federal organizational sub-component responsible for the system. If a state or local government or contractor performs the function, identify both the federal and other organization and describe the relationship. Be specific about the organization and do not abbreviate. Include physical locations and addresses.

3.2.3 Information Contact(s)

List the name, title, organization, and telephone number of one or more persons designated to be the point(s) of contact for this system. One of the contacts given should be identified as the system owner. The designated persons should have sufficient knowledge of the system to be able to provide additional information or points of contact, as needed.

3.2.4 Assignment of Security Responsibility

An individual must be assigned responsibility in writing to ensure that the application or general support system has adequate security. To be effective, this individual must be knowledgeable of the management, operational, and technical controls used to protect the system.

3.3 System Operational Status

Indicate one or more of the following for the system's operational status. If more than one status is selected, list which part of the system is covered under each status.

- Operational — the system is operating.
- Under development — the system is being designed, developed, or implemented.
- Undergoing a major modification — the system is undergoing a major conversion or transition.

3.4 General Description/Purpose

Present a brief description (one-three paragraphs) of the function and purpose of the system (e.g., economic indicator, network support for an organization, business census data analysis, crop reporting support).

3.5 System Environment

Provide a brief (one-three paragraphs) general description of the technical system. Include any environmental or technical factors that raise special security concerns.

3.6 System Interconnection/ Information Sharing

System interconnection is the direct connection of systems for the purpose of sharing information resources. System interconnection, if not appropriately protected, may result in a compromise of all connected systems and the data they store, process, or transmit. It is important that system operators, information owners, and management obtain as much information as possible about the vulnerabilities associated with system interconnection and

information sharing and the increased controls required to mitigate those vulnerabilities. The security plan for the systems often serves as a mechanism to effect this security information exchange and allows management to make informed decisions regarding risk reduction and acceptance.

3.7 Sensitivity of Information Handled

This section provides a description of the types of information handled by the system and an analysis of the criticality of the information. The sensitivity and criticality of the information stored within, processed by, or transmitted by a system provides a basis for the value of the system and is one of the major factors in risk management.

The nature of the information sensitivity and criticality must be described in this section. The description must contain information on applicable laws, regulations, and policies affecting the system and a general description of sensitivity as discussed below.

3.7.1 Laws, Regulations, and Policies Affecting the System

List any laws, regulations, or policies that establish specific requirements for confidentiality, integrity, or availability of data/information in the system.

3.7.2 General Description of Sensitivity

Both information and information systems have distinct life cycles. It is important that the degree of sensitivity of information be assessed by considering the requirements for availability, integrity, and confidentiality of the information. This process should occur at the beginning of the information system's life cycle and be re-examined during each life cycle stage.

4 Management Controls

In this section, describe the management control measures (in place or planned) that are intended to meet the protection requirements of the major application or general support system. Management controls focus on the management of the computer security system and the management of risk for a system. The types of control measures shall be consistent with the need for protection of the major application or general support system.

4.1 Risk Assessment and Management

OMB Circular A-130 no longer requires the preparation of a formal risk analysis. It does, however, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. The methods used to assess the nature and level of risk to the system should include a consideration of the major factors in risk management: the value of the system or application, threats, vulnerabilities, and the effectiveness of current or proposed safeguards. The methods used should be described in at least one paragraph.

4.2 Review of Security Controls

OMB Circular A-130 requires that at least every three years an independent review of the security controls for each major application be performed. For general support systems, OMB Circular A-130 requires that the security controls be reviewed by an independent audit or self review at least every three years.

4.3 Rules of Behavior

Attach the rules of behavior for the general support system or major application as an appendix and reference the appendix number in this section, or insert the rules into this section. A set of rules of behavior must be established for each system. The security required by the rules is only as stringent as necessary to provide adequate security for the determining the rules.

4.4 Planning for Security in the Life Cycle

Although a computer security plan can be developed for a system at any point in the life cycle, the recommended approach is to draw up the plan at the beginning of the computer system life cycle. It is recognized that in some cases, the system may at any one time be in several phases of the life cycle.

4.4.1 Initiation Phase

During the initiation phase, the need for a system is expressed and the purpose of the system is documented. A sensitivity assessment can be performed which looks at the sensitivity of the information to be processed and the system itself. If the system or part of the system is in the initiation phase, reference the sensitivity assessment described in Section 3.7, Sensitivity of Information Handled.

4.4.2 Development/Acquisition Phase

During this phase, the system is designed, purchased, programmed, developed, or otherwise constructed. This phase often consists of other defined cycles, such as the system development cycle or the acquisition cycle.

During the first part of the development/acquisition phase, security requirements should be developed at the same time system planners define the requirements of the system. These requirements can be expressed as technical features (e.g., access controls), assurances (e.g., background checks for system developers), or operational practices (e.g., awareness and training). If the system or part of the system is in this phase, include a general description of any specifications that were used and whether they are being maintained.

4.4.3 Implementation Phase

In the implementation phase, the system's security features should be configured and enabled, the system should be tested and installed or fielded, and the system authorized for processing. (See Section 4.5, Authorize Processing, for a description of that requirement.) A design review and systems test should be performed prior to placing the system into operation to assure that it meets security specifications. In addition, if new controls are added to the application or the support system, additional acceptance tests of those new controls must be performed. This ensures that new controls meet security specifications and do not conflict with or invalidate existing controls. The results of the design reviews and system tests should be fully documented, updated as new reviews or tests are performed, and maintained in the official organization records.

4.4.4 Operation/Maintenance Phase

During this phase, the system performs its work. The system is almost always being continuously modified by the addition of hardware and software and by numerous other events. If the system is undergoing modifications, determine which phase of the life cycle the system modifications are in and describe the security activities conducted or planned for in that part of the system. For the system in the operation/maintenance phase, the security plan documents the security activities.

4.4.5 Disposal Phase

The disposal phase of the IT system life cycle involves the disposition of information, hardware, and software.

4.5 Authorize Processing

The term "authorize processing" is the authorization granted by a management official for a system to process information. (Note: Some agencies refer to this authorization as accreditation.) Authorization provides a form of quality control and is required under OMB Circular A-130. It forces managers and technical staff to find the best fit for security, given technical constraints, operational constraints, and mission requirements. By authorizing

processing in a system, a manager accepts the risk associated with it. In this section of the plan, include the date of authorization, name, and title of management official. If not authorized, provide the name and title of manager requesting approval to operate and date of request.

5 Operational Controls

Beginning in this chapter and continuing through Chapter 6, Technical Controls, there are two formats and related guidance provided: one format and related guidance for major applications and another set for general support systems. From this chapter on, there is enough of a difference between the controls for a major application and a general support system to warrant a division by system type. The section numbering of these two chapters differs from the rest of the document. The two chapters are numbered as 5.MA and 6.MA for Major Application, then 5.GSS and 6.GSS for General Support System.

5.MA. Major Application – Operational Controls

The operational controls address security methods that focus on mechanisms that primarily are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise – and often rely upon management activities as well as technical controls. In this section, describe the operational control measures (in place or planned) that are intended to meet the protection requirements of the major application.

5.MA.1 Personnel Security

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often, systems experience disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., the programmer who inserts one minor change, then installs the program into the production environment without testing).

5.MA.2 Physical and Environmental Protection

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical and environmental security program should address the following seven topics which are explained below. In this section, briefly describe the physical and environmental controls in place for the major application.

5.MA.2.1 Explanation of Physical and Environment Security – *Access Controls. Fire Safety Factors. Failure of Supporting Utilities. Structural Collapse. Interception of Data. Mobile and Portable Systems.*

5.MA.2.2 Computer Room Example – Appropriate and adequate controls will vary depending on the individual system requirements. The example list shows the types of controls for an application residing on a system in a computer room. The list is not intended to be all-inclusive or to imply that all systems should have all controls listed.

5.MA.3 Production, Input/Output Controls

In this section, provide a synopsis of the procedures in place that support the operations of the application.

5.MA.4 Contingency Planning

Procedures are required that will permit the organization to continue essential functions if information technology support is interrupted. These procedures (contingency plans, business interruption plans, and continuity of operations plans) should be coordinated with the backup, contingency, and recovery plans of any general support systems,

including networks used by the application. The contingency plans should ensure that interfacing systems are identified and contingency/disaster planning coordinated.

5.MA.5 Application Software Maintenance Controls

These controls are used to monitor the installation of, and updates to, application software to ensure that the software functions as expected and that a historical record is maintained of application changes. This helps ensure that only authorized software is installed on the system. Such controls may include a software configuration policy that grants managerial approval (re-authorize processing) to modifications and requires that changes be documented. Other controls include products and procedures used in auditing for or preventing illegal use of shareware or copyrighted software. Software maintenance procedures may also be termed version control, change management, or configuration management.

5.MA.6 Data Integrity/Validation Controls

Data integrity controls are used to protect data from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered. Validation controls refer to tests and evaluations used to determine compliance with security specifications and requirements. In this section, describe any controls that provide assurance to users that the information has not been altered and that the system functions as expected.

5.MA.7 Documentation

Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security in the application and the support system(s) on which it is processed, to include backup and contingency activities, as well as descriptions of user and operator procedures.

5.MA.8 Security Awareness and Training

The Computer Security Act requires federal agencies to provide for the mandatory periodic training in computer security awareness and accepted computer security practices for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency. This includes contractors as well as employees of the agency.

6.MA Major Application - Technical Controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations and should be consistent with the management of security within the organization. In this section, describe the technical control measures (in place or planned) that are intended to meet the protection requirements of the major application.

6.MA.1 Identification and Authentication

Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on least privilege, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

6.MA.1.1 Identification – Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID. In this section of the plan, briefly describe how the major application identifies access to the system.

6.MA.1.2 Authentication – Authentication is the means of establishing the validity of a user's claimed identity to the system. There are three means of authenticating a user's identity which can be used alone or in combination: something the individual knows (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key); something the individual possesses (a token -- e.g., an ATM card or a smart card); and something the individual is (a biometrics -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint). In this section, describe the major application's authentication control mechanisms.

6.MA.2 Logical Access Controls (Authorization/Access Controls)

Logical access controls are the system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted. In this section, discuss the controls in place to authorize or restrict the activities of users and system personnel within the application. Describe hardware or software features that are designed to permit only authorized access to or within the application, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists).

6.MA.3 Public Access Controls

Public access systems are subject to a greater threat from outside attacks. In public access systems, users are often anonymous and untrained in the system and their responsibilities. Attacks on public access systems could have a substantial impact on the organization's reputation and the level of public trust and confidence. Threats from insiders are also greater (e.g., errors introduced by disgruntled employees or unintentional errors by untrained users).

6.MA.4 Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification.

5.GSS General Support System – Operational Controls

The operational controls address security mechanisms that focus on methods that primarily are implemented and executed by people (as opposed to systems). These controls are put in place to improve the security of a particular system (or group of systems). They often require technical or specialized expertise and often rely upon management activities as well as technical controls. In this section, describe the operational control measures (in place or planned) that are intended to meet the protection requirements of the general support system.

5.GSS.1 Personnel Controls

The greatest harm/disruption to a system comes from the actions of individuals, both intentional and unintentional. All too often, systems experience disruption, damage, loss, or other adverse impact due to the well-intentioned actions of individuals authorized to use or maintain a system (e.g., the programmer who inserts one minor change, then installs the program into the production environment without testing).

In this section, include detailed information about the following personnel security measures. It is recommended that most of these measures be included as part of the rules of behavior. If they are incorporated in the rules of behavior, reference the applicable section.

5.GSS.2 Physical and Environmental Protection

Physical and environmental security controls are implemented to protect the facility housing system resources, the system resources themselves, and the facilities used to support their operation. An organization's physical and environmental security program should address the following seven topics which are explained below. In this section, briefly describe the physical and environmental controls in place or planned for the general support system.

5.GSS.2.1 Explanation of Physical and Environment Security – *Access Controls. Fire Safety Factors. Failure of Supporting Utilities. Structural Collapse. Plumbing Leaks. Interception of Data. Mobile and Portable Systems.*

5.GSS.2.2 Computer Room Example – Appropriate and adequate controls will vary depending on the individual system requirements. The example list shows the types of controls for an application residing on a system in a computer room. The list is not intended to be all inclusive or to imply that all systems should have all controls listed.

5.GSS.3 Production, Input/Output Controls

In this section, provide a synopsis of the procedures in place that support the general support system.

5.GSS.4 Contingency Planning (Continuity of Support)

General support systems require appropriate emergency, backup, and contingency plans. These plans should be tested regularly to assure the continuity of support in the event of system failure. Also, these plans should be known to users and coordinated with their plans for applications.

Describe the procedures (contingency plan) that would be followed to ensure the system continues to process all critical applications if a disaster should occur and provide a reference to the detailed plans.

5.GSS.5 Hardware and System Software Maintenance Controls

These controls are used to monitor the installation of, and updates to, hardware, operating system software, and other software to ensure that the hardware and software function as expected, and that a historical record is maintained of application changes. These controls may also be used to ensure that only authorized software is installed on the system. Such controls may include a hardware and software configuration policy that grants managerial approval (re-authorize processing) to modifications and requires that changes be documented. Other controls include products and procedures used in auditing for, or preventing, illegal use of shareware or copyrighted software. In this section, provide several paragraphs on the hardware and system software maintenance controls in place or planned.

5.GSS.6 Integrity Controls

Integrity controls are used to protect the operating system, applications, and information in the system from accidental or malicious alteration or destruction and to provide assurance to the user that the information meets expectations about its quality and that it has not been altered. In this section, describe any controls that provide assurance to users that the information has not been altered and that the system functions as expected.

5.GSS.7 Documentation

Documentation is a security control in that it explains how software/hardware is to be used and formalizes security and operational procedures specific to the system. Documentation for a system includes descriptions of the hardware and software, policies, standards, procedures, and approvals related to automated information system security on the support system, including backup and contingency activities, as well as descriptions of user and operator procedures.

5.GSS.8 Security Awareness and Training

The Computer Security Act requires federal agencies to provide mandatory periodic training in computer security awareness and accepted computer security practice for all employees who are involved with the management, use, or operation of a federal computer system within or under the supervision of the federal agency. This includes contractors as well as employees of the agency.

5.GSS.9 Incident Response Capability

A computer security incident is an adverse event in a computer system or network caused by a failure of a security mechanism or an attempted or threatened breach of these mechanisms³. Computer security incidents are becoming more common and their impact far-reaching. When faced with an incident, an organization should be able to respond quickly in a manner that both protects its own information and helps to protect the information of others that might be affected by the incident.

6.GSS General Support System - Technical Controls

Technical controls focus on security controls that the computer system executes. The controls can provide automated protection from unauthorized access or misuse, facilitate detection of security violations, and support security requirements for applications and data. The implementation of technical controls, however, always requires significant operational considerations – and should be consistent with the management of security within the organization. In this section, describe the technical control measures (in place or planned) that are intended to meet the protection requirements of the general support system.

6.GSS.1.1 Identification

Identification and Authentication is a technical measure that prevents unauthorized people (or unauthorized processes) from entering an IT system. Access control usually requires that the system be able to identify and differentiate among users. For example, access control is often based on least privilege, which refers to the granting to users of only those accesses minimally required to perform their duties. User accountability requires the linking of activities on an IT system to specific individuals and, therefore, requires the system to identify users.

6.GSS.1.1 Identification – Identification is the means by which a user provides a claimed identity to the system. The most common form of identification is the user ID. In this section of the plan, describe how the general support system identifies access to the system.

6.GSS.1.2 Authentication – Authentication is the means of establishing the validity of a user's claimed identity to the system. There are three means of authenticating a user's identity which can be used alone or in combination: something the individual knows (a secret -- e.g., a password, Personal Identification Number (PIN), or cryptographic key); something the individual possesses (a token -- e.g., an ATM card or a smart card); and something the individual is (a biometrics -- e.g., characteristics such as a voice pattern, handwriting dynamics, or a fingerprint). In this section, describe the general support system's authentication control mechanisms.

6.GSS.2 Logical Access Controls (Authorization/Access Controls)

Logical access controls are the system-based mechanisms used to specify who or what (e.g., in the case of a process) is to have access to a specific system resource and the type of access that is permitted.

In this section, discuss the controls in place to authorize or restrict the activities of users and system personnel within the general support system. Describe hardware or software features that are designed to permit only authorized access to or within the system, to restrict users to authorized transactions and functions, and/or to detect unauthorized activities (e.g., access control lists).

6.GSS.3 Audit Trails

Audit trails maintain a record of system activity by system or application processes and by user activity. In conjunction with appropriate tools and procedures, audit trails can provide a means to help accomplish several security-related objectives, including individual accountability, reconstruction of events, intrusion detection, and problem identification. In this section, describe the audit trail mechanisms in place.

The Standard of Good Practice for Information Security

SM Security Management (enterprise-wide)

SM1 HIGH-LEVEL DIRECTION

Achieving an effective and consistent standard of good practice for information security throughout the enterprise requires clear direction from the top. Accordingly, this area covers top management's direction on, and commitment to, information security. It specifies an information security policy and a set of staff agreements that should be applied to all individuals who have access to the information and systems of the enterprise.

SM1.1 Management commitment

Principle: Top management's direction on information security should be established, and commitment demonstrated.

Objective: To establish top management's direction on, and commitment to, information security.

SM1.2 Security policy

Principle: A comprehensive, documented information security policy should be produced and communicated to all individuals with access to the enterprise's information and systems.

Objective: To document top management's direction on and commitment to information security, and communicate it to all relevant individuals.

SM1.3 Staff agreements

Principle: Staff agreements should be established that specify information security responsibilities, are incorporated into staff agreements and are taken into account when screening applicants for employment.

Objective: To document top management's direction on and commitment to information security, and communicate it to all relevant individuals.

SM2 SECURITY ORGANISATION

Safeguarding information and systems requires information security activity to be organised effectively throughout the enterprise. Accordingly, this area covers the organisational arrangements for managing information security throughout the enterprise, raising security awareness amongst staff and ensuring they have the skills required to run systems correctly and securely.

SM2.1 High-level control

Principle: Control over information security should be provided by a high-level working group, committee or equivalent body, supported by a top-level executive.

Objective: To provide a top-down management structure and a practical mechanism for co-ordinating information security activity throughout the enterprise.

SM2.2 Information security function

Principle: A specialist information security function should be established, which has enterprise-wide responsibility for promoting information security.

Objective: To ensure good practice in information security is applied effectively throughout the enterprise.

SM2.3 Local security co-ordination

Principle: Arrangements should be made to co-ordinate information security activity in business units/departments.

Objective: To ensure that security activities are carried out in a timely and accurate manner, enterprise-wide, and that security issues are resolved effectively.

SM2.4 Security awareness

Principle: Specific activities should be undertaken, such as a security awareness programme, to promote security awareness to all individuals who have access to the information and systems of the enterprise.

Objective: To ensure all relevant individuals understand the key elements of information security and why it is needed, and understand their personal information security responsibilities.

SM2.5 Security education

Principle: Staff should be educated/trained in how to run systems correctly and how to develop and apply security controls.

Objective: To provide staff with the skills required to run systems correctly and fulfil their information security responsibilities.

SM3 SECURITY REQUIREMENTS

Ensuring that the safeguards applied to information and systems are proportionate to their importance to the business is a fundamental element of good practice. Accordingly, this area covers arrangements for classifying critical information and systems, assigning ownership and identifying risk.

SM3.1 Security classification

Principle: A security classification scheme should be established that applies throughout the enterprise, based on the importance and sensitivity of information and systems in use.

Objective: To communicate how information and systems should be treated in order that attention can be focused on those that are most critical.

SM3.2 Ownership

Principle: 'Ownership' of critical information and systems should be assigned to capable individuals, with responsibilities clearly defined and accepted.

Objective: To achieve individual accountability for all information and systems throughout the enterprise and give responsible individuals a vested interest in their protection.

SM3.3 Information risk analysis

Principle: Important or critical applications, computer installations, networks and systems under development should be subject to a structured information risk analysis on a regular basis.

Objective: To enable individuals who are responsible for information and systems to identify key information risks and determine the controls required to keep those risks within acceptable limits.

SM4 SECURE ENVIRONMENT

Achieving a consistent standard of good practice in information security across an enterprise is a complex undertaking. The difficulties can be eased by introducing a common framework of disciplines and by making standard arrangements at enterprise level, rather than on an individual basis, for example by appointing an individual to manage information privacy for the whole enterprise. Accordingly, this area covers the arrangements required to build a secure environment enterprise-wide.

SM4.1 Security architecture

Principle: An 'information security architecture' should be established, which provides a framework for the application of standard security controls throughout the enterprise.

Objective: To enable system developers and administrators to implement consistent, simple-to-use security functionality across multiple computer systems throughout the enterprise.

SM4.2 Information privacy

Principle: Responsibility for managing information privacy should be established and security controls for handling personally identifiable information applied.

Objective: To prevent information about individuals being used in an inappropriate manner, and ensure compliance with legal and regulatory requirements for information privacy.

SM4.3 Asset management

Principle: Proven, reliable and approved hardware/software should be used that meet security requirements and are recorded in an inventory.

Objective: To reduce the risk of information security being compromised by weaknesses in hardware/software and ensure compliance with legal/regulatory requirements.

SM4.4 Physical protection

Principle: All buildings throughout the enterprise that house critical IT facilities (eg data centres, network facilities and key user areas) should be physically protected against accident or attack.

Objective: To restrict physical access to authorised individuals and ensure that IT facilities processing critical or sensitive information are available when required.

SM4.5 Business continuity

Principle: Documented standards/procedures should be established for developing business continuity plans and for maintaining business continuity arrangements throughout the enterprise.

Objective: To enable the enterprise to withstand the prolonged unavailability of critical information and systems.

SM5 MALICIOUS ATTACK

Organisations are often subject to malicious attack from third parties, for example by viruses or hacking. Consequently, this area covers the security controls required to protect against viruses and other malicious code, provide intrusion detection capabilities, respond to a serious attack and manage forensic investigations.

SM5.1 Virus protection

Principle: Virus protection arrangements should be established, and maintained enterprise-wide.

Objective: To protect the enterprise against virus attack and ensure it can respond to virus infection within critical timescales.

SM5.2 Malicious mobile code protection

Principle: Enterprise-wide arrangements should be established to protect against malicious mobile code, such as that downloaded from the web.

Objective: To protect the enterprise against disruption caused by the introduction of malicious mobile code.

SM5.3 Intrusion detection

Principle: Intrusion detection mechanisms should be applied to critical systems and networks.

Objective: To identify suspected or actual malicious attacks and enable the enterprise to respond before serious damage is done.

SM5.4 Emergency response

Principle: An emergency response process should be established, supported by an emergency response team, which outlines actions to be taken in the event of a serious attack.

Objective: To respond to serious attacks quickly and effectively, reducing any potential business impact.

SM5.5 Forensic investigations

Principle: A process should be established for dealing with incidents that require forensic investigation.

Objective: To identify perpetrators of malicious acts and preserve sufficient evidence to prosecute them if required.

SM5.6 Patch management

Principle: There should be a strategy for patch management that should be supported by a management framework and a documented patch management process.

Objective: To address potential vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising.

SM6 SPECIAL TOPICS

The rapid pace of change in business and technology has resulted in the emergence of special topics with particular security concerns that should be dealt with enterprise-wide. Accordingly, this area covers the special security controls that apply to the use of cryptography, public key infrastructure, e-mail, remote working, the provision of third party access, electronic commerce and outsourcing.

SM6.1 Use of cryptography

Principle: Cryptographic solutions should be approved, documented and applied enterprise-wide.

Objective: To ensure that cryptographic services are managed effectively, thereby protecting the confidentiality of sensitive information, preserving the integrity of critical information and confirming the identity of the originator of information.

SM6.2 Public key infrastructure

Principle: Where a public key infrastructure (PKI) is used, it should be protected by 'hardening' the underlying operating system(s) and restricting access to Certification Authorities.

Objective: To ensure that the public key infrastructure (PKI) operates as intended, is available when required and can be recovered in the event of an emergency.

SM6.3 E-mail

Principle: E-mail systems should be protected by a combination of policy, awareness, procedural and technical security controls.

Objective: To ensure that e-mail services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

SM6.4 Remote working

Principle: Personal computers used by staff working in remote locations should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.

Objective: To ensure that computers used by staff working in remote locations operate as intended, remain available and do not compromise the security of any facilities to which they can be connected.

SM6.5 Third party access

Principle: Connections from third parties (ie external organisations, such as customers or suppliers) should be uniquely identified, subjected to a risk analysis, approved, and supported by contracts.

Objective: To ensure that access to the enterprise's information and systems is restricted to authorised third parties.

SM6.6 Electronic commerce

Principle: A process should be established to ensure that information security is incorporated into electronic commerce initiatives enterprise-wide.

Objective: To keep the increased risks associated with the development and deployment of electronic commerce within acceptable limits.

SM6.7 Outsourcing

Principle: A process should be established to govern the selection and management of outsource providers supported by documented agreements that specify the security requirements to be met.

Objective: To ensure that security requirements are satisfied and maintained when the running of a particular environment is entrusted to an outsource provider.

SM6.8 Instant messaging

Principle: Instant messaging services should be protected by setting management policy, deploying Instant Messaging application controls and configuring the security element of an Instant Messaging infrastructure.

Objective: To ensure that Instant Messaging services are available when required, the confidentiality and integrity of messages is protected in transit, and the risk of misuse is minimised.

SM7 MANAGEMENT REVIEW

An accurate understanding of the information security condition of the enterprise is required in order to manage information security effectively. Accordingly, this area covers the arrangements needed to provide decision-makers with sound information on the security condition of information and systems throughout the enterprise.

SM7.1 Security audit/review

Principle: The information security status of critical IT environments should be subject to thorough, independent and regular security audits/reviews.

Objective: To provide individuals who are responsible for particular IT environments, and top management, with an independent assessment of the security condition of those environments.

SM7.2 Security monitoring

Principle: The information security condition of the enterprise should be monitored periodically and reported to top management.

Objective: To provide top management with an accurate, comprehensive and coherent assessment of the security condition of the enterprise.

CB Critical Business Applications

CB1 BUSINESS REQUIREMENTS FOR SECURITY

Business applications vary enormously in their importance to the business; hence the level of protection required also varies. Accordingly, this area identifies the information security requirements of the application.

CB1.1 Confidentiality requirements

Principle: The business impact of unauthorised disclosure of information associated with the application should be assessed.

Objective: To document and agree the confidentiality requirements (the need for information to be kept secret or private within a predetermined group) of the application.

CB1.2 Integrity requirements

Principle: The business impact of the accidental corruption or deliberate manipulation of business information stored in or processed by the application should be assessed.

Objective: To document and agree the integrity requirements (the need for information to be valid, accurate and complete) of the application.

CB1.3 Availability requirements

Principle: The business impact of business information stored in or processed by the application being unavailable for any length of time should be assessed.

Objective: To document and agree the availability requirements (the need for information to be accessible when required) of the application.

CB2 APPLICATION MANAGEMENT

Keeping business risks within acceptable limits requires a coherent set of information security arrangements. Accordingly, this area covers the roles and responsibilities required (including ‘business ownership’), integral application controls and additional controls for handling sensitive material or transferring sensitive information. In addition, this area covers general management controls including change management, incident management and business continuity.

CB2.1 Roles and responsibilities

Principle: An ‘owner’ should be identified for the application, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective: To assign ‘ownership’ of the application, provide a sound management structure for staff running or using it and give responsible individuals a vested interest in its protection.

CB2.2 Application controls

Principle: The full range of application controls should be considered, and required controls identified.

Objective: To build in the required application controls to protect information stored in or processed by the application.

CB2.3 Change management

Principle: Changes to the application should be tested, reviewed and applied using a change management process.

Objective: To ensure that changes are applied correctly and do not compromise the security of the application.

CB2.4 Incident management

Principle: All incidents – of any type – should be recorded, reviewed and resolved using an incident management process.

Objective: To identify and resolve incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

CB2.5 Business continuity

Principle: A business continuity plan should be developed, supported by contingency arrangements, and tested periodically.

Objective: To enable the business processes associated with the application to continue in the event of a disaster.

CB2.6 Sensitive information

Principle: Additional protection should be provided for applications that involve handling sensitive material or transferring sensitive information.

Objective: To protect the integrity and confidentiality of sensitive information.

CB3 USER ENVIRONMENT

Critical business applications can be used by internal or external business or technical users. These individuals may be sited locally or at a remote location, often with differing business and security requirements. Accordingly, this area covers the disciplines required to control access to the application, configure workstations and ensure users are aware of information security and understand their personal responsibilities.

CB3.1 Access control

Principle: Access to the application and associated information should be restricted to authorised individuals and enforced accordingly.

Objective: To ensure that only authorised individuals gain access to the application, and that individual accountability is assured.

CB3.2 Application sign-on process

Principle: Users should be subjected to a rigorous sign-on process before they can gain access to the application.

Objective: To ensure that only authorised users gain access to the application.

CB3.3 Workstation configuration

Principle: Workstations connected to the application should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.

Objective: To ensure workstations operate as intended, are available when required and do not compromise the security of the application.

CB3.4 Security awareness

Principle: Users of the application should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure users of the application apply security controls and prevent the security of information used in the application from being compromised.

CB4 SYSTEM MANAGEMENT

To enable applications to function, they have to run on one or more computers and typically make use of one or more networks. Accordingly, this area covers service agreements, the resilience of the application, external connections and the back-up of essential information and software.

CB4.1 Service agreements

Principle: Computer and network services required to support the application should only be obtained from service providers capable of providing required security controls, and be supported by documented contracts or service level agreements.

Objective: To define the business requirements for providers of any computer or network services that support the application, including those for information security, and to ensure they are met.

CB4.2 Resilience

Principle: The application should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.

Objective: To ensure that the application is available when required.

CB4.3 External connections

Principle: All external connections to the application should be individually identified, verified, recorded, and approved by the application 'owner'.

Objective: To ensure that only authorised individuals gain access to the application via external connections.

CB4.4 Back-up

Principle: Back-ups of essential information and software used by the application should be taken on a regular basis, according to a defined cycle.

Objective: To ensure that, in the event of an emergency, essential information or software required by the application can be restored within critical timescales.

CB5 LOCAL SECURITY MANAGEMENT

The security controls applied to a business application should be proportional to business risk. Accordingly, this area covers the arrangements made to identify the relative importance of the application, the associated business risks and the level of protection required. It also addresses local security co-ordination and the need for the application to be subject to thorough, independent and regular security audits/reviews.

CB5.1 Local security co-ordination

Principle: An individual should be appointed to co-ordinate the information security arrangements of the application.

Objective: To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

CB5.2 Security classification

Principle: The application should be classified according to the importance and sensitivity of information stored in or processed by the application, using a security classification scheme that applies throughout the enterprise.

Objective: To communicate the level of security controls required by the application.

CB5.3 Information risk analysis

Principle: The application should be subject to a structured information risk analysis on a regular basis, the results of which should be documented, reviewed, and agreed by the application 'owner'.

Objective: To identify key information risks associated with the application and determine the security controls required in order to keep those risks within acceptable limits.

CB5.4 Security audit/review

Principle: The information security status of the application should be subject to thorough, independent and regular security audits/reviews.

Objective: To ensure that security controls have been implemented effectively, that risk is being managed and to provide the application 'owner', and top management, with an independent assessment of the security status of the application.

CB6 SPECIAL TOPICS

The rapid pace of change in business and technology has resulted in the emergence of special topics with particular security concerns. Where these topics apply to a critical business application, special security arrangements are required. Accordingly, this area covers the additional security controls required by applications that provide third party access, employ cryptographic key management, use a public key infrastructure (PKI) or are based on web-enabled technology.

CB6.1 Third party agreements

Principle: Connections from third parties (ie external organisations, such as customers, suppliers and members of the public) should be subject to a risk assessment, approved by the application 'owner' and agreed by both parties in a documented agreement, such as a contract.

Objective: To ensure that only agreed and approved third parties gain access to the application.

CB6.2 Cryptographic key management

Principle: Cryptographic keys should be managed tightly, in accordance with documented standards/procedures, and protected against unauthorised access or destruction.

Objective: To ensure that cryptographic keys are not compromised, for example through loss or disclosure.

CB6.3 Public key infrastructure

Principle: Any public key infrastructure (PKI) used by the application should be protected by ‘hardening’ the underlying operating system(s) and restricting access to Certification Authorities.

Objective: To ensure that the public key infrastructure (PKI) operates as intended, is available when required and can be recovered in the event of an emergency.

CB6.4 Web-enabled applications

Principle: Specialised technical controls should be applied to web-enabled applications.

Objective: To ensure that the increased risks associated with web-enabled applications are minimised.

CI Computer Installations

CII INSTALLATION MANAGEMENT

Computer installations used for processing information need to be well managed. Accordingly, this area covers the roles and responsibilities of the staff involved in running computer installations, agreements made with business users, management of key assets (eg hardware and software) and monitoring of the systems associated with the installation.

CII.1 Roles and responsibilities

Principle: An ‘owner’ should be identified for the computer installation, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective: To achieve individual accountability for the computer installation, provide a sound management structure for staff running it and give responsible individuals a vested interest in its protection.

CII.2 Service agreements

Principle: Users’ service requirements should be classified in a way that identifies their criticality to the business and documented in agreements, such as contracts or service level agreements.

Objective: To define the business requirements, including information security requirements, for services provided by the computer installation.

CII.3 Asset management

Principle: Essential information about hardware and software (eg unique identifiers, version numbers and physical locations) should be recorded in inventories, and software licensing requirements met.

Objective: To protect information stored in or processed by the installation and meet legal/regulatory requirements.

CII.4 System monitoring

Principle: Systems associated with the computer installation should be monitored continuously, and from a business user’s perspective.

Objective: To assess the performance of the computer installation, reduce the likelihood of system overload and detect potential or actual malicious intrusions.

CI2 LIVE ENVIRONMENT

Service targets are more likely to be achieved if computer installations are designed well. Accordingly, this area covers the design of the installation, logging of key events and the configuration of host systems and workstations. It also covers the resilience of the installation and its protection from physical loss or damage.

CI2.1 Installation design

Principle: Computer installations should be designed to cope with current and predicted information processing requirements and be protected using a range of in-built security controls.

Objective: To produce a computer installation that has security functionality built-in and enables additional controls to be incorporated easily.

CI2.2 Event logging

Principle: Logs of all key events within the computer installation should be maintained (preferably using automated tools), reviewed periodically and protected against unauthorised change.

Objective: To ensure individual accountability and to enable incidents, such as access violations, to be investigated and resolved.

CI2.3 Host system configuration

Principle: Host systems should be configured to function as required, and to prevent unauthorised or incorrect updates.

Objective: To ensure host systems operate as intended and do not compromise the security of the computer installation.

CI2.4 Workstation configuration

Principle: Workstations connected to systems within the computer installation should be purchased from a list of approved suppliers, tested prior to use, supported by maintenance arrangements and protected by physical controls.

Objective: To ensure workstations operate as intended and do not compromise the security of the systems to which they are connected.

CI2.5 Resilience

Principle: The computer installation should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.

Objective: To ensure that the systems supported by the computer installation are available when required.

CI2.6 Hazard protection

Principle: Computer equipment and facilities should be protected against fire, flood, environmental and other natural hazards.

Objective: To prevent services being disrupted by damage to computer equipment or facilities.

CI2.7 Power supplies

Principle: Critical computer equipment and facilities should be protected against power outages.

Objective: To prevent services provided by the computer installation from being disrupted by loss of power.

CI2.8 Physical access

Principle: Physical access to critical computer installation facilities should be restricted to authorised individuals.

Objective: To prevent services being disrupted by loss of or damage to equipment or facilities.

CI3 SYSTEM OPERATION

Achieving service targets requires computer installations to be run in accordance with sound disciplines. Accordingly this area covers basic controls over system operation (ie handling computer media, back-up and change management) and arrangements for identifying and resolving incidents (ie incident management and emergency fixes).

CI3.1 Handling computer media

Principle: Information held on data storage media (including magnetic tapes, disks, printed results, and stationery) should be protected against corruption, loss or disclosure and additional security controls applied to media containing sensitive information.

Objective: To protect computer media in accordance with their information security requirements.

CI3.2 Back-up

Principle: Back-ups of essential information and software used by the computer installation should be taken on a regular basis, according to a defined cycle.

Objective: To ensure that, in the event of an emergency, essential information and software required by the installation can be restored within critical timescales.

CI3.3 Change management

Principle: Changes to any part of the computer installation should be tested, reviewed and applied using a change management process.

Objective: To ensure that changes are applied correctly and do not compromise the security of the installation.

CI3.4 Incident management

Principle: All incidents – of any type – should be recorded, reviewed and resolved using an incident management process.

Objective: To identify and resolve incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

CI3.5 Emergency fixes

Principle: Emergency fixes to computer equipment, business applications, systems software and business information should be tested, reviewed and applied in accordance with documented standards/procedures.

Objective: To respond to emergencies quickly and effectively, reducing any potential business impact.

CI3.6 Patch management

Principle: There should be a strategy for patch management that should be supported by a management framework and a documented patch management process.

Objective: To address potential vulnerabilities quickly and effectively in order to reduce the likelihood of a serious business impact arising.

CI4 ACCESS CONTROL

Effective access control mechanisms can reduce the risk of unauthorised access to information and systems. Accordingly, this area covers the access control disciplines applied to users and the steps taken to control access to information and systems within the computer installation.

CI4.1 Access control arrangements

Principle: Access control arrangements should be established to restrict access by all types of user to approved system capabilities of the computer installation.

Objective: To ensure that only authorised individuals gain access to information or systems within the computer installation, and that individual accountability is assured.

CI4.2 User authorisation

Principle: All users of the computer installation should be authorised before they are granted access privileges.

Objective: To restrict access to any information or systems within the computer installation to authorised users.

CI4.3 Access privileges

Principle: All users of the computer installation should be assigned specific privileges to allow them to access particular information or systems.

Objective: To provide authorised users with access privileges which are sufficient to enable them to perform their duties but do not permit them to exceed their authority.

CI4.4 Sign-on process

Principle: Users should follow a rigorous system sign-on process before they can gain access to target systems.

Objective: To ensure that only authorised users gain access to any information or systems within the computer installation.

CI4.5 User authentication

Principle: All users should be authenticated by using UserIDs and passwords or by strong authentication mechanisms (eg smartcards or biometric devices, such as fingerprint recognition) before they can gain access to target systems.

Objective: To ensure that only authorised users gain access to any information or systems within the computer installation.

CI5 LOCAL SECURITY MANAGEMENT

A computer installation typically supports one or more critical business applications, holds information that needs to be protected, and is an important asset in its own right. Each of these perspectives needs to be considered in order to provide appropriate protection. Accordingly, this area covers the arrangements made to identify the relative importance of the computer installation, the associated business risks and the level of protection required. It also covers the arrangements made to ensure that information security is co-ordinated locally, staff are aware of information security and understand their personal responsibilities, and the need for the installation to be subject to thorough, independent and regular security audits/reviews.

CI5.1 Local security co-ordination

Principle: An individual should be appointed to co-ordinate the information security arrangements of the computer installation.

Objective: To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

CI5.2 Security awareness

Principle: Staff running the installation should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure that staff running the installation apply security controls and prevent the security of information used in the computer installation from being compromised.

CI5.3 Security classification

Principle: The computer installation should be classified according to the importance and sensitivity of information stored in or processed by the installation, using a security classification scheme that applies throughout the enterprise.

Objective: To communicate the level of security controls required by the computer installation.

CI5.4 Information risk analysis

Principle: The computer installation should be subject to a structured information risk analysis on a regular basis, the results of which should be documented, reviewed, and agreed by the installation 'owner'.

Objective: To identify key information risks associated with the computer installation and determine the security controls required in order to keep those risks within acceptable limits.

CI5.5 Security audit/review

Principle: The information security status of the computer installation should be subject to thorough, independent and regular security audits/reviews.

Objective: To ensure that security controls have been implemented effectively, that risk is being managed and to provide the installation ‘owner’, and top management, with an independent assessment of the security status of the installation.

CI6 SERVICE CONTINUITY

If there is a serious interruption to information processing, for example if a disaster occurs, the computer installation may be unavailable for a prolonged period. Considerable forethought is required to enable information processing to continue in these circumstances and to keep the business impact to a minimum. Accordingly, this area covers the development of contingency plans and arrangements, and their validation.

CI6.1 Contingency plan

Principle: A business continuity plan should be developed and documented.

Objective: To provide individuals with a documented set of actions to perform in the event of a disaster, enabling information processing to be resumed within critical timescales.

CI6.2 Contingency arrangements

Principle: Alternative processing arrangements should be established, and made available when required.

Objective: To enable information processing to resume within critical timescales, using alternative facilities.

CI6.3 Validation and maintenance

Principle: Contingency plans and arrangements should be tested on a periodic basis.

Objective: To ensure that information processing can resume within critical timescales, using alternative facilities.

NW Networks

NW1 NETWORK MANAGEMENT

Computer networks are complex. They have to link different systems together, are subject to constant change and often rely on services provided by external parties. Orchestrating the technical and organisational issues involved requires sound management. Accordingly, this area covers the organisational arrangements for running a network, its design, resilience and documentation, and the management of relationships with service providers.

NW1.1 Roles and responsibilities

Principle: An ‘owner’ should be identified for the network, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective: To achieve individual accountability for the network, provide a sound management structure for staff running it and give responsible individuals a vested interest in its protection.

NW1.2 Network design

Principle: The network should be designed to cope with current and predicted levels of traffic and be protected using a range of in-built security controls.

Objective: To produce an operational network that has security functionality built-in and enables additional controls to be incorporated easily.

NW1.3 Network resilience

Principle: The network should be run on robust, reliable hardware and software, supported by alternative or duplicate facilities.

Objective: To ensure that the network is available when required.

NW1.4 Network documentation

Principle: Networks should be supported by accurate, up-to-date documentation.

Objective: To ensure that the network is configured accurately and securely.

NW1.5 Service providers

Principle: Network services should only be obtained from service providers capable of providing relevant security controls, and be supported by documented contracts or service level agreements.

Objective: To define the business requirements for network service providers, including those for security, and ensure they are met.

NW2 TRAFFIC MANAGEMENT

Computer networks can handle many types of traffic from a wide variety of sources. To manage network traffic effectively, network devices have to be configured correctly and particular types of network traffic denied access. Accordingly, this area covers the disciplines required to ensure undesirable network traffic and unauthorised external or wireless users are prevented from gaining access to the network.

NW2.1 Configuring network devices

Principle: Network devices should be configured to function as required, and to prevent unauthorised or incorrect updates.

Objective: To ensure that the configuration of network devices is accurate and does not compromise the security of the network.

NW2.2 Firewalls

Principle: Network traffic should be routed through a firewall, prior to being allowed access to the network.

Objective: To ensure unauthorised network traffic is not allowed to gain access to specified parts of the network.

NW2.3 External access

Principle: All external connections to the network should be individually identified, verified, recorded, and approved by the network 'owner'.

Objective: To ensure that only authorised external users gain access to the network.

NW2.4 Wireless access

Principle: Wireless access should be authorised, authenticated, encrypted and permitted only from approved locations.

Objective: To ensure that only authorised individuals gain wireless access to the network and that wireless transmissions cannot be monitored.

NW3 NETWORK OPERATIONS

Maintaining continuity of service to users requires computer networks to be run in accordance with sound disciplines. Accordingly this area covers the arrangements needed to monitor network performance and to manage changes and incidents. In addition, the area covers the arrangements required to provide physical security, take back-ups and ensure service continuity.

NW3.1 Network monitoring

Principle: Key network activities should be monitored.

Objective: To assess the performance of the network, reduce the likelihood of network overload and detect potential or actual malicious intrusions.

NW3.2 Change management

Principle: Changes to the network should be tested, reviewed and applied using a change management process.

Objective: To ensure that changes are applied correctly and do not compromise the security of the network.

NW3.3 Incident management

Principle: All network incidents – of any type – should be recorded, reviewed and resolved using an incident management process.

Objective: To identify and resolve network incidents effectively, minimise their business impact and reduce the risk of similar incidents occurring.

NW3.4 Physical security

Principle: Physical access to critical network facilities should be restricted to authorised individuals.

Objective: To prevent services being disrupted by loss of or damage to communications equipment, power or facilities.

NW3.5 Back-up

Principle: Back-ups of essential information and software used by the network should be taken on a regular basis, according to a defined cycle.

Objective: To ensure that, in the event of an emergency, essential network information or software required by the network can be restored within critical timescales.

NW3.6 Service continuity

Principle: A service continuity plan should be developed, supported by effective contingency arrangements, and tested periodically.

Objective: To enable critical network services to continue in the event of a disaster.

NW3.7 Remote maintenance

Principle: Remote maintenance of the network should be restricted to authorised individuals, confined to individual sessions, and subject to review.

Objective: To prevent unauthorised access to the network through the misuse of remote maintenance facilities.

NW4 LOCAL SECURITY MANAGEMENT

Computer networks play an essential role in the functioning of many critical business applications. They convey information that needs to be protected, and are valuable assets in their own right. Accordingly, this area covers the arrangements made to identify the relative importance of the network, the associated business risks and the level of protection required. It also covers the arrangements made to ensure that information security is co-ordinated locally, network staff are aware of information security and understand their personal responsibilities, and the need for the network to be subject to thorough, independent and regular security audits/reviews.

NW4.1 Local security co-ordination

Principle: An individual should be appointed to co-ordinate the information security arrangements of the network.

Objective: To ensure that security activities are carried out in a timely and accurate manner, and that security issues are resolved effectively.

NW4.2 Security awareness

Principle: Network staff should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure network staff apply security controls and prevent the security of information transmitted across the network from being compromised.

NW4.3 Security classification

Principle: The network should be classified according to the importance and sensitivity of information transmitted across it, using a security classification scheme that applies throughout the enterprise.

Objective: To communicate the level of security controls required by the network.

NW4.4 Information risk analysis

Principle: The network should be subject to a structured information risk analysis on a regular basis, the results of which should be documented, reviewed, and agreed by the network 'owner'.

Objective: To identify key information risks associated with the network and determine the security controls required in order to keep those risks within acceptable limits.

NW4.5 Security audit/review

Principle: The information security status of the network should be subject to thorough, independent and regular security audits/reviews.

Objective: To ensure that security controls have been implemented effectively, that risk is being managed and to provide the network 'owner', and top management, with an independent assessment of the security status of the network.

NW5 VOICE NETWORKS

Business processes can be disrupted if voice networks, such as telephone systems, are unavailable or overloaded. Harm can also be caused if voice networks are subject to unauthorised use by outsiders, or sensitive conversations are overheard. Accordingly, this area covers the security arrangements applied to voice networks.

NW5.1 Voice network documentation

Principle: Voice networks should include documentation of essential components and be supported by documented standards/procedures.

Objective: To provide employees with a clear statement of the security disciplines they are expected to follow in relation to voice networks.

NW5.2 Resilience of voice networks

Principle: Voice networks should be supported by a robust and reliable set of hardware and software, with alternative facilities available when required.

Objective: To ensure that voice network facilities (eg telephone exchanges) are available when required.

NW5.3 Special voice network controls

Principle: Voice network facilities (eg telephone exchanges) should be monitored regularly and access to them restricted.

Objective: To prevent and detect the misuse of voice network facilities.

SD Systems Development

SD1 DEVELOPMENT MANAGEMENT

Producing robust systems, on which the enterprise can depend, requires a sound approach to systems development. Accordingly, this area covers the organisation of systems development staff, the methodology used in developing systems, quality assurance and the security of development environments.

SD1.1 Roles and responsibilities

Principle: An individual with overall responsibility for the development activity, together with business 'owners', should be appointed to manage system development activities, and responsibilities for key tasks assigned to individuals who are capable of performing them.

Objective: To achieve individual accountability for system development activities, provide a sound management structure for staff performing them and give responsible individuals a vested interest in their protection.

SD1.2 Development methodology

Principle: Development activities should be carried out in accordance with a documented system development methodology.

Objective: To ensure that systems under development meet business requirements, including those for information security.

SD1.3 Quality assurance

Principle: Quality assurance of key security activities should be performed during the development lifecycle.

Objective: To provide assurance that security requirements are defined adequately, agreed security controls are developed and security requirements are met.

SD1.4 Development environments

Principle: System development activities should be performed in specialised development environments, isolated from the live environment, and protected against disruption and disclosure of information.

Objective: To provide a secure environment for system development activities.

SD2 LOCAL SECURITY MANAGEMENT

In common with live systems, systems under development need to be supported by a sound organisational structure and run by staff who are aware of information security and know how to apply security controls effectively. Accordingly, this area covers the arrangements made to ensure that information security is co-ordinated locally, systems development staff are aware of information security and understand their personal responsibilities, and the need for systems development activities to be subject to thorough, independent and regular security audits/reviews.

SD2.1 Local security co-ordination

Principle: An individual should be appointed to co-ordinate the information security arrangements of system development activities.

Objective: To ensure that security activities associated with systems development are carried out in a timely and accurate manner, and that information security issues are resolved effectively.

SD2.2 Security awareness

Principle: Systems development staff should be made aware of the key elements of information security and why it is needed, and understand their personal information security responsibilities.

Objective: To ensure systems development staff apply security controls and prevent the security of information used in development activities from being compromised.

SD2.3 Security audit/review

Principle: The information security status of systems development activity should be subject to thorough, independent and regular security audits/reviews.

Objective: To ensure that security controls are designed effectively, that risk is managed, and to provide the business 'owner', and top management, with an independent assessment of the security status of system development activities.

SD3 BUSINESS REQUIREMENTS

A thorough understanding of business requirements (including those for the confidentiality, integrity and availability of information) is essential if systems are to fulfil their intended purpose. Accordingly, this area covers the arrangements made for specifying business requirements, determining security requirements and conducting risk assessments.

SD3.1 Specification of requirements

Principle: Business requirements (including those for information security) should be documented and agreed before detailed design commences.

Objective: To ensure that information security requirements are treated as an integral part of business requirements, are fully considered and approved.

SD3.2 Confidentiality requirements

Principle: The business impact of unauthorised disclosure of information associated with the system under development should be assessed.

Objective: To document and agree the confidentiality requirements (the need for information to be kept secret or private within a predetermined group) of the system under development.

SD3.3 Integrity requirements

Principle: The business impact of the accidental corruption or deliberate manipulation of business information stored in or processed by the system under development should be assessed.

Objective: To document and agree the integrity requirements (the need for information to be valid, accurate and complete) of the system under development.

SD3.4 Availability requirements

Principle: The business impact of business information stored in or processed by the system under development being unavailable for any length of time should be assessed.

Objective: To document and agree the availability requirements (the need for information to be accessible when required) of the system under development.

SD3.5 Information risk analysis

Principle: Systems under development should be subject to a structured information risk analysis, the results of which should be documented, reviewed and agreed by the business owner.

Objective: To identify key risks associated with systems under development and determine the security controls required in order to keep those risks within acceptable limits.

SD4 DESIGN AND BUILD

Building systems that function as intended requires the use of sound disciplines throughout the design and build stage of development. Accordingly, this area covers the arrangements needed to address information security during design, acquisition and system build, and the identification of required application, general and web-specific security controls.

SD4.1 System design

Principle: Information security requirements for the system under development should be considered when designing the system.

Objective: To produce an operational system based on sound design principles which has security functionality built-in and enables controls to be incorporated easily.

SD4.2 Application controls

Principle: The full range of application controls should be considered when designing the system under development.

Objective: To ensure that required application controls are built-in to the system under development.

SD4.3 General security controls

Principle: The full range of general security controls should be considered when designing the system under development.

Objective: To ensure that required general security controls are built-in to the system under development.

SD4.4 Acquisition

Principle: Robust, reliable hardware and software should be acquired, following consideration of security requirements and identification of any security deficiencies.

Objective: To ensure that hardware and software acquired from third parties provides the required functionality and does not compromise the security of systems under development.

SD4.5 System build

Principle: System build activities (including coding and package customisation) should be carried out in accordance with industry good practice, performed by individuals provided with adequate skills/tools and inspected to identify unauthorised modifications or changes which may compromise security controls.

Objective: To ensure that systems are built correctly and that no security weaknesses are introduced during the build process.

SD4.6 Web-enabled development

Principle: Specialised technical controls should be applied to the development of web-enabled applications.

Objective: To ensure that the increased risks associated with the development of web-enabled applications are minimised.

SD5 TESTING

Testing is a fundamental element of good practice in systems development. Planned well and performed correctly, it provides assurance that systems, including security controls, function as intended and reduces the likelihood of system malfunctions occurring. Accordingly, this area covers the arrangements needed to carry out testing thoroughly, without disrupting other activities.

SD5.1 Testing process

Principle: All elements of a system (ie application software packages, system software, hardware and services) should be tested before the system is promoted to the live environment.

Objective: To ensure systems function correctly and meet security requirements.

SD5.2 Acceptance testing

Principle: Systems under development should be subject to rigorous acceptance testing in an isolated area that simulates the live environment.

Objective: To ensure that only systems that have been tested rigorously and satisfy user requirements (including those for information security), are promoted to the live environment.

SD6 IMPLEMENTATION

Sound disciplines are required when new systems are promoted from the development into the live environment. Accordingly, this area covers system promotion criteria, the installation of new systems in the live environment and post-implementation reviews.

SD6.1 System promotion criteria

Principle: Rigorous criteria should be met before new systems are promoted into the live environment.

Objective: To ensure that only tested and approved versions of hardware and software are promoted into the live environment.

SD6.2 Installation process

Principle: New systems should be installed in the live environment in accordance with a documented installation process.

Objective: To ensure that new systems are installed in the live environment without disruption.

SD6.3 Post-implementation review

Principle: Post-implementation reviews should be conducted for all new systems.

Objective: To check that systems – and information security controls – function as intended.

OECD Guidelines for the Security of Information Systems and Networks – Towards a Culture of Security

The following nine principles are complementary and should be read as a whole. They concern participants at all levels, including policy and operational levels. Under these Guidelines, the responsibilities of participants vary according to their roles. All participants will be aided by awareness, education, information sharing and training that can lead to adoption of better security understanding and practices. Efforts to enhance the security of information systems and networks should be consistent with the values of a democratic society, particularly the need for an open and free flow of information and basic concerns for personal privacy.

1) Awareness

Participants should be aware of the need for security of information systems and networks and what they can do to enhance security.

Awareness of the risks and available safeguards is the first line of defence for the security of information systems and networks. Information systems and networks can be affected by both internal and external risks. Participants should understand that security failures may significantly harm systems and networks under their control. They should also be aware of the potential harm to others arising from interconnectivity and interdependency. Participants should be aware of the configuration of, and available updates for, their system, its place within networks, good practices that they can implement to enhance security, and the needs of other participants.

2) Responsibility

All participants are responsible for the security of information systems and networks.

Participants depend upon interconnected local and global information systems and networks and should understand their responsibility for the security of those information systems and networks. They should be accountable in a manner appropriate to their individual roles. Participants should review their own policies, practices, measures, and procedures regularly and assess whether these are appropriate to their environment. Those who develop, design and supply products and services should address system and network security and distribute appropriate information including updates in a timely manner so that users are better able to understand the security functionality of products and services and their responsibilities related to security.

3) Response

Participants should respect the legitimate interests of others.

Recognising the interconnectivity of information systems and networks and the potential for rapid and widespread damage, participants should act in a timely and co-operative manner to address security incidents. They should share information about threats and vulnerabilities, as appropriate, and implement procedures for rapid and effective co-operation to prevent, detect and respond to security incidents. Where permissible, this may involve cross-border information sharing and co-operation.

4) Ethics

All participants are responsible for the security of information systems and networks.

Given the pervasiveness of information systems and networks in our societies, participants need to recognise that their action or inaction may harm others. Ethical conduct is therefore crucial and participants should strive to develop and adopt best practices and to promote conduct that recognises security needs and respects the legitimate interests of others.

5) Democracy

The security of information systems and networks should be compatible with essential values of a democratic society.

Security should be implemented in a manner consistent with the values recognised by democratic societies including the freedom to exchange thoughts and ideas, the free flow of information, the confidentiality of information and communication, the appropriate protection of personal information, openness and transparency.

6) Risk assessment

Participants should conduct risk assessments.

Risk assessment identifies threats and vulnerabilities and should be sufficiently broad-based to encompass key internal and external factors, such as technology, physical and human factors, policies and third-party services with security implications. Risk assessment will allow determination of the acceptable level of risk and assist the selection of appropriate controls to manage the risk of potential harm to information systems and networks in light of the nature and importance of the information to be protected. Because of the growing interconnectivity of information systems, risk assessment should include consideration of the potential harm that may originate from others or be caused to others.

7) Security design and implementation

Participants should incorporate security as an essential element of information systems and networks.

Systems, networks and policies need to be properly designed, implemented and co-ordinated to optimise security. A major, but not exclusive, focus of this effort is the design and adoption of appropriate safeguards and solutions to avoid or limit potential harm from identified threats and vulnerabilities. Both technical and non-technical safeguards and solutions are required and should be proportionate to the value of the information on the organisation's systems and networks. Security should be a fundamental element of all products, services, systems and networks, and an integral part of system design and architecture. For end users, security design and implementation consists largely of selecting and configuring products and services for their system.

8) Security management

Participants should adopt a comprehensive approach to security management.

Security management should be based on risk assessment and should be dynamic, encompassing all levels of participants' activities and all aspects of their operations. It should include forward-looking responses to emerging threats and address prevention, detection and response to incidents, systems recovery, ongoing maintenance, review and audit. Information system and network security policies, practices, measures and procedures should be co-ordinated and integrated to create a coherent system of security. The requirements of security management depend upon the level of involvement, the role of the participant, the risk involved and system requirements.

9) Reassessment

Participants should review and reassess the security of information systems and networks, and make appropriate modifications to security policies, practices, measures and procedures.

New and changing threats and vulnerabilities are continuously discovered. Participants should continually review, reassess and modify all aspects of security to deal with these evolving risks.

Control Objectives for Information and related Technology (COBIT)

Plan and Organise

This domain covers strategy and tactics, and concerns the identification of the way IT can best contribute to the achievement of the business objectives. Furthermore, the realisation of the strategic vision needs to be planned, communicated and managed for different perspectives. Finally, a proper organisation as well as technological infrastructure should be put in place. This domain typically addresses the following management questions:

- Are IT and the business strategy aligned?
- Is the enterprise achieving optimum use of its resources?
- Does everyone in the organisation understand the IT objectives?
- Are IT risks understood and being managed?
- Is the quality of IT systems appropriate for business needs?

PO1 Define a Strategic IT Plan

IT strategic planning is required to manage and direct all IT resources in line with the business strategy and priorities. The IT function and business stakeholders are responsible for ensuring that optimal value is realised from project and service portfolios. The strategic plan should improve key stakeholders' understanding of IT opportunities and limitations, assess current performance and clarify the level of investment required. The business strategy and priorities are to be reflected in portfolios and executed by the IT tactical plan(s), which establishes concise objectives, plans and tasks understood and accepted by both business and IT.

Control over the IT process of

Define a strategic IT plan

that satisfies the business requirement for IT of

sustaining or extending the business strategy and governance requirements while being transparent about benefits, costs and risks

by focusing on

incorporating IT and business management in the translation of business requirements into service offerings, and the development of strategies to deliver these services in a transparent and effective manner

is achieved by

- Engaging with business and senior management in aligning IT strategic planning with current and future business needs
- Understanding current IT capabilities
- Providing for a prioritisation scheme for the business objectives that quantifies the business requirements

and is measured by

- Percent of IT objectives in the IT strategic plan that support the strategic business plan
- Percent of IT projects in the IT project portfolio that can be directly traced back to the IT tactical plan
- Delay between updates of IT strategic plan and updates of IT tactical plans

PO1.1 IT Value Management

PO1.2 Business-IT Alignment

PO1.3 Assessment of Current Performance

PO1.4 IT Strategic Plan

PO1.5 IT Tactical Plans

PO1.6 IT Portfolio Management

PO2 Define the Information Architecture

The information systems function should create and regularly update a business information model and define the appropriate systems to optimise the use of this information. This encompasses the development of a corporate data dictionary with the organisation's data syntax rules, data classification scheme and security levels. This process improves the quality of management decision making by making sure that reliable and secure information is provided, and it enables rationalising information systems resources to appropriately match business strategies. This IT process is also needed to increase accountability for the integrity and security of data and to enhance the effectiveness and control of sharing information across applications and entities.

Control over the IT process of

Define the information architecture

that satisfies the business requirement for IT of

to be agile in responding to requirements, to provide reliable and consistent information and to seamlessly integrate applications into business processes

by focusing on

the establishment of an enterprise data model that incorporates a data classification scheme to ensure integrity and consistency of all data

is achieved by

- Assuring the accuracy of the information architecture and data model
- Assigning data ownership
- Classifying information using an agreed classification scheme

and is measured by

- Percent of redundant/duplicate data elements
- Percent of applications not complying with the information architecture
- Frequency of data validation activities

PO2.1 Enterprise Information Architecture Model

PO2.2 Enterprise Data Dictionary and Data Syntax Rules

PO2.3 Data Classification Scheme

PO2.4 Integrity Management

PO3 Determine Technological Direction

The information services function should determine the technology direction to support the business. This requires the creation of a technological infrastructure plan and an architecture board that sets and manages clear and realistic expectations of what technology can offer in terms of products, services and delivery mechanisms. The plan should be regularly updated and encompasses aspects such as systems architecture, technological direction, acquisitions plans, standards, migration strategies and contingency. This enables timely responses to changes in the competitive environment, economies of scale for information systems staffing and investments as well as improved interoperability of platforms and applications.

Control over the IT process of

Determine technological direction

that satisfies the business requirement for IT of

having stable and cost-effective integrated and standard application systems, resources and capabilities that meet current and future business requirements

by focusing on

defining and implementing a technology infrastructure plan, architecture and standards that recognise and leverage technology opportunities

is achieved by

- Establishing a forum to guide architecture and verify compliance
- Establishing the technical infrastructure plan balanced against cost, risk and requirements
- Defining the technical infrastructure standards based on information architecture requirements

and is measured by

- Number and type of deviations from the technology infrastructure plan
- Frequency of technology infrastructure plan review/update
- Number of technology platforms by function across the enterprise

PO3.1 Technological Direction Planning

PO3.2 Technological Infrastructure Plan

PO3.3 Monitoring of Future Trends and Regulations

PO3.4 Technology Standards

PO3.5 IT Architecture Board

PO4 Define the IT Processes, Organisation and Relationships

An IT organisation must be defined considering requirements for staff, skills, functions, accountability, authority, roles and responsibilities, and supervision. This organisation is to be embedded into an IT process framework that ensures transparency and control as well as the involvement of senior executives and business management. A strategy committee should ensure board oversight of IT and one or more steering committees, in which business and IT participate, should determine prioritisation of IT resources in line with business needs. Processes, administrative policies and procedures need to be in place for all functions, with specific attention to control, quality assurance, risk management, information security, data and systems ownership, and segregation of duties. To ensure timely support of business requirements, IT is to be involved in relevant decision processes.

Control over the IT process of

Define the IT processes, organisation and relationships

that satisfies the business requirement for IT of

being agile in responding to the business strategy while complying with governance requirements and providing defined and competent points of contact

by focusing on

establishing transparent, flexible and responsive IT organisational structures and defining and implementing IT processes with owners, roles and responsibilities integrated into business and decision processes

is achieved by

- Defining an IT process framework
- Establishing appropriate organisational bodies and structure
- Defining roles and responsibilities

and is measured by

- Percent of roles with documented position and authority descriptions
- Number of business units/processes not supported by the IT organisation that should be supported, according to the strategy
- Number of core IT activities outside of the IT organisation that are not approved or are not subject to IT organisational standards

PO4.1 IT Process Framework

PO4.2 IT Strategy Committee

PO4.3 IT Steering Committee

PO4.4 Organisational Placement of the IT Function

- PO4.5 IT Organisational Structure
- PO4.6 Roles and Responsibilities
- PO4.7 Responsibility for IT Quality Assurance
- PO4.8 Responsibility for Risk, Security and Compliance
- PO4.9 Data and System Ownership
- PO4.10 Supervision
- PO4.11 Segregation of Duties
- PO4.12 IT Staffing
- PO4.13 Key IT Personnel
- PO4.14 Contracted Staff Policies and Procedures
- PO4.15 Relationships

PO5 Manage the IT Investment

Establish and maintain a framework to manage IT-enabled investment programmes that encompasses cost, benefits, prioritisation within budget, a formal budgeting process and management against the budget. Work with stakeholders to identify and control the total costs and benefits within the context of the IT strategic and tactical plans, and initiate corrective action where needed. The process fosters partnership between IT and business stakeholders, enables the effective and efficient use of IT resources, and provides transparency and accountability into the total cost of ownership, the realisation of business benefits and the return on investment of IT-enabled investments.

Control over the IT process of

Manage the IT investment

that satisfies the business requirement for IT of

continuously and demonstrably improving IT's cost-efficiency and its contribution to business profitability with integrated and standardised services that satisfy end-user expectations

by focusing on

effective and efficient IT investment and portfolio decisions, and by setting and tracking IT budgets in line with IT strategy and investment decisions

is achieved by

- Forecasting and allocating budgets
- Defining formal investment criteria (ROI, payback period, NPV)
- Measuring and assessing business value against forecast

and is measured by

- Percent reduction of the unit cost of the delivered IT services
- Percent of budget deviation value compared to the total budget
- Percent of IT spend expressed in business value drivers (e.g., sales/services increase due to increased connectivity)

- PO5.1 Financial Management Framework
- PO5.2 Prioritisation Within IT Budget
- PO5.3 IT Budgeting Process
- PO5.4 Cost Management
- PO5.5 Benefit Management

PO6 Communicate Management Aims and Direction

Management should develop an enterprise IT control framework and define and communicate policies. An ongoing communication programme should be implemented to articulate the mission, service objectives, policies and procedures, etc., approved and supported by management. The communication supports achievement of IT objectives and ensures awareness and understanding of business and IT risks, objectives and direction. The process should ensure compliance with relevant laws and regulations.

Control over the IT process of

Communicate management aims and direction

that satisfies the business requirement for IT of

accurate and timely information on the current and future IT services,
associated risks and responsibilities

by focusing on

providing accurate, understandable and approved policies, procedures,
guidelines and other documentation to stakeholders, embedded in an IT control
framework

is achieved by

- Defining an IT control framework
- Developing and rolling out IT policies
- Enforcing IT policies

and is measured by

- Number of business disruptions due to IT service disruption
- Percent of stakeholders who understand the enterprise IT control framework
- Percent of stakeholders who are noncompliant with policy

PO6.1 IT Policy and Control Environment

PO6.2 Enterprise IT Risk and Internal Control Framework

PO6.3 IT Policies Management

PO6.4 Policy Rollout

PO6.5 Communication of IT Objectives and Direction

PO7 Manage IT Human Resources

Acquire, maintain and motivate a competent workforce for creation and delivery of IT services to the business. This is achieved by following defined and agreed practices supporting recruiting, training, evaluating performance, promoting and terminating. This process is critical as people are important assets and governance and the internal control environment are heavily dependent on the motivation and competence of personnel.

Control over the IT process of

Manage IT human resources

that satisfies the business requirement for IT of

competent and motivated people to create and deliver IT services

by focusing on

hiring and training personnel, motivating through clear career paths, assigning
roles that correspond with skills, establishing a defined review process, creating
position descriptions and ensuring awareness of dependency on individuals

is achieved by

- Reviewing staff performance
- Hiring and training IT personnel to support IT tactical plans
- Mitigating risk of overdependence on key resources

and is measured by

- Satisfaction level of stakeholders with IT personnel expertise and skills
- IT personnel turnover
- Percent of IT people certified according to job needs

PO7.1 Personnel Recruitment and Retention

PO7.2 Personnel Competencies

PO7.3 Staffing of Roles

PO7.4 Personnel Training

- PO7.5 Dependence Upon Individuals
- PO7.6 Personnel Clearance Procedures
- PO7.7 Employee Job Performance Evaluation
- PO7.8 Job Change and Termination

PO8 Manage Quality

A quality management system should be developed and maintained, which includes proven development and acquisition processes and standards. This is enabled by planning, implementing and maintaining the quality management system by providing clear quality requirements, procedures and policies. Quality requirements should be stated and communicated in quantifiable and achievable indicators. Continuous improvement is achieved by ongoing monitoring, analysing and acting upon deviations, and communicating results to stakeholders. Quality management is essential to ensure that IT is delivering value to the business, continuous improvement and transparency for stakeholders.

Control over the IT process of
Manage quality

that satisfies the business requirement for IT of

continuous and measurable improvement of the quality of IT services delivered

by focusing on

the definition of a quality management system (QMS), ongoing performance monitoring against predefined objectives, and implementation of a programme for continuous improvement of IT services

is achieved by

- Defining quality standards and practices
- Monitoring and reviewing internal and external performance against the defined quality standards and practices
- Improving the QMS in a continuous manner

and is measured by

- Percent of stakeholders satisfied with IT quality (weighted by importance)
- Percent of IT processes formally reviewed by quality assurance on a periodic basis that meet target quality goals and objectives
- Percent of processes receiving quality assurance (QA) review

- PO8.1 Quality Management System
- PO8.2 IT Standards and Quality Practices
- PO8.3 Development and Acquisition Standards
- PO8.4 Customer Focus
- PO8.5 Continuous Improvement
- PO8.6 Quality Measurement, Monitoring and Review

PO9 Assess and Manage IT Risks

Create and maintain a risk management framework. The framework documents a common and agreed level of IT risks, mitigation strategies and agreed-upon residual risks. Any potential impact on the goals of the organisation caused by an unplanned event should be identified, analysed and assessed. Risk mitigation strategies should be adopted to minimise residual risk to an accepted level. The result of the assessment should be understandable to the stakeholders and expressed in financial terms, to enable stakeholders to align risk to an acceptable level of tolerance.

Control over the IT process of

Assess and manage IT risks

that satisfies the business requirement for IT of

analysing and communicating IT risks and their potential impact on business

processes and goals

by focusing on

development of a risk management framework that is integrated in business and operational risk management frameworks, risk assessment, risk mitigation and communication of residual risk

is achieved by

- Ensuring that risk management is fully embedded in management processes, internally and externally, and consistently applied
- Performing risk assessments
- Recommending and communicating risk remedial action plans

and is measured by

- Percent of critical IT objectives covered by risk assessment
- Percent of identified critical IT risks with action plans developed
- Percent of risk management action plans approved for implementation

PO9.1 IT and Business Risk Management Alignment

PO9.2 Establishment of Risk Context

PO9.3 Event Identification

PO9.4 Risk Assessment

PO9.5 Risk Response

PO9.6 Maintenance and Monitoring of a Risk Action Plan

PO10 Manage Projects

Establish a programme and project management framework for the management of all IT projects. The framework should ensure the correct prioritisation and co-ordination of all projects. The framework should include a master plan, assignment of resources, definition of deliverables, approval by users, a phased approach to delivery, quality assurance, a formal test plan, and testing and post-implementation review after installation to ensure project risk management and value delivery to the business. This approach reduces the risk of unexpected costs and project cancellations, improves communications to and involvement of business and end users, ensures the value and quality of project deliverables, and maximises their contribution to IT-enabled investment programmes.

Control over the IT process of

Manage projects

that satisfies the business requirement for IT of

delivery of project results within agreed time frames, budget and quality

by focusing on

a defined programme and project management approach that is applied to IT projects, which enables stakeholder participation in and monitoring of project risks and progress

is achieved by

- Defining and enforcing programme and project frameworks and approach
- Issuing project management guidelines
- Performing project planning for each project detailed in the project portfolio

and is measured by

- Percent of projects meeting stakeholders expectations (on time, on budget and meeting requirements—weighted by importance)
- Percent of projects receiving post-implementation reviews
- Percent of projects following project management standards and practices

PO10.1 Programme Management Framework

PO10.2 Project Management Framework

PO10.3 Project Management Approach
PO10.4 Stakeholder Commitment
PO10.5 Project Scope Statement
PO10.6 Project Phase Initiation
PO10.7 Integrated Project Plan
PO10.8 Project Resources
PO10.9 Project Risk Management
PO10.10 Project Quality Plan
PO10.11 Project Change Control
PO10.12 Project Planning of Assurance Methods
PO10.13 Project Performance Measurement, Reporting and Monitoring
PO10.14 Project Closure

Acquire and Implement

To realise the IT strategy, IT solutions need to be identified, developed or acquired, as well as implemented and integrated into the business process. In addition, changes in and maintenance of existing systems are covered by this domain to make sure the solutions continue to meet business objectives. This domain typically addresses the following management questions:

- Are new projects likely to deliver solutions that meet business needs?
- Are new projects likely to be delivered on time and within budget?
- Will the new systems work properly when implemented?
- Will changes be made without upsetting current business operations?

AI1 Identify Automated Solutions

The need for a new application or function requires analysis before acquisition or creation to ensure that business requirements are satisfied in an effective and efficient approach. This process covers the definition of the needs, consideration of alternative sources, review of technological and economic feasibility, execution of a risk analysis and cost-benefit analysis, and conclusion of a final decision to 'make' or 'buy'. All these steps enable organisations to minimise the cost to acquire and implement solutions whilst ensuring they enable the business to achieve its objectives.

Control over the IT process of

Identify automated solutions

that satisfies the business requirement for IT of

translating business functional and control requirements into an effective and efficient design of automated solutions

by focusing on

identifying technically feasible and cost-effective solutions

is achieved by

- Defining business and technical requirements
- Undertaking feasibility studies as defined in the development standards
- Approving (or rejecting) requirements and feasibility study results

and is measured by

- Number of projects where stated benefits were not achieved due to incorrect feasibility assumptions
- Percent of feasibility studies signed off by the business process owner
- Percent of users satisfied with functionality delivered

AI1.1 Definition and Maintenance of Business Functional and Technical Requirements
AI1.2 Risk Analysis Report
AI1.3 Feasibility Study and Formulation of Alternative Courses of Action
AI1.4 Requirements and Feasibility Decision and Approval

AI2 Acquire and Maintain Application Software

Applications have to be made available in line with business requirements. This process covers the design of the applications, the proper inclusion of application controls and security requirements, and the actual development and configuration according to standards. This allows organisations to properly support business operations with the correct automated applications.

Control over the IT process of

Acquire and maintain application software

that satisfies the business requirement for IT of

making available applications in line with business requirements, and doing so in time and at a reasonable cost

by focusing on

ensuring there is a timely and cost-effective development process

is achieved by

- Translating business requirements into design specifications
- Adhering to development standards for all modifications
- Separating development, testing and operational activities

and is measured by

- Number of production problems per application causing visible down time
- Percentage of users satisfied with functionality delivered

AI2.1 High-level Design

AI2.2 Detailed Design

AI2.3 Application Control and Auditability

AI2.4 Application Security and Availability

AI2.5 Configuration and Implementation of Acquired Application Software

AI2.6 Major Upgrades to Existing Systems

AI2.7 Development of Application Software

AI2.8 Software Quality Assurance

AI2.9 Applications Requirements Management

AI2.10 Application Software Maintenance

AI3 Acquire and Maintain Technology Infrastructure

Organisations should have processes for the acquisition, implementation and upgrade of the technology infrastructure. This requires a planned approach to acquisition, maintenance and protection of infrastructure in line with agreed technology strategies and the provision of development and test environments. This ensures that there is ongoing technological support for business applications.

Control over the IT process of

Acquire and maintain technology infrastructure

that satisfies the business requirement for IT of

acquiring and maintaining an integrated and standardised IT infrastructure

by focusing on

providing appropriate platforms for the business applications in line with the defined IT architecture and technology standards

is achieved by

- Producing a technology acquisition plan that aligns to the technology infrastructure plan
- Planning infrastructure maintenance
- Implementing internal control, security and auditability measures

and is measured by

- Percent of platforms that are not in line with the defined IT architecture and technology standards
- Number of critical business processes supported by obsolete (or soon to be) infrastructure
- Number of infrastructure components that are no longer supportable (or will not be in the near future)

AI3.1 Technological Infrastructure Acquisition Plan

AI3.2 Infrastructure Resource Protection and Availability

AI3.3 Infrastructure Maintenance

AI3.4 Feasibility Test Environment

AI4 Enable Operation and Use

Knowledge about new systems needs to be made available. This process requires the production of documentation and manuals for users and IT, and provides training to ensure proper use and operations of applications and infrastructure.

Control over the IT process of

Enable operation and use

that satisfies the business requirement for IT of

ensuring satisfaction of end users with service offerings and service levels, and seamlessly integrating applications and technology solutions into business processes

by focusing on

providing effective user and operational manuals and training materials to transfer the knowledge necessary for successful system operation and use

is achieved by

- Developing and making available knowledge transfer documentation
- Communicating and training users and business management, support staff and operational staff
- Producing training materials

and is measured by

- Number of applications where IT procedures are seamlessly integrated into business processes
- Percent of business owners satisfied with application training and support materials
- Number of applications with adequate user and operational support training

AI4.1 Planning for Operational Solutions

AI4.2 Knowledge Transfer to Business Management

AI4.3 Knowledge Transfer to End Users

AI4.4 Knowledge Transfer to Operations and Support Staff

AI5 Procure IT Resources

IT resources, including people, hardware, software and services need to be procured. This requires the definition and enforcement of procurement procedures, the selection of vendors, the setup of contractual arrangements and the actual acquisition itself. Doing so ensures that the organisation has all required IT resources in a timely and cost-effective manner.

Control over the IT process of

Procure IT resources

that satisfies the business requirement for IT of

improving IT's cost-efficiency and its contribution to business profitability

by focusing on

acquiring and maintaining IT skills that respond to the delivery strategy, an integrated and standardised IT infrastructure, and reducing IT procurement risk

is achieved by

- Obtaining professional legal and contractual advice
- Defining procurement procedures and standards
- Procuring requested hardware, software and services in line with defined procedures

and is measured by

- Number of disputes related to procurement contracts
- Reduced purchasing cost
- Percent of key stakeholders satisfied with suppliers

AI5.1 Procurement Control

AI5.2 Supplier Contract Management

AI5.3 Supplier Selection

AI5.4 Software Acquisition

AI5.5 Acquisition of Development Resources

AI5.6 Acquisition of Infrastructure, Facilities and Related Services

AI6 Manage Changes

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment must be formally managed in a controlled manner. Changes (including procedures, processes, system and service parameters) must be logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

Control over the IT process of

Manage changes

that satisfies the business requirement for IT of

responding to business requirements in alignment with the business strategy, whilst reducing solution and service delivery defects and rework

by focusing on

controlling impact assessment, authorisation and implementation of all changes to the IT infrastructure, applications and technical solutions, minimising errors due to incomplete request specifications and halting implementation of unauthorised changes

is achieved by

- Defining and communicating change procedures, including emergency changes
- Assessing, prioritising and authorising changes
- Tracking status and reporting on changes

and is measured by

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Application or infrastructure rework caused by inadequate change specifications
- Percent of changes that follow formal change control processes

AI6.1 Change Standards and Procedures

AI6.2 Impact Assessment, Prioritisation and Authorisation

AI6.3 Emergency Changes

AI6.4 Change Status Tracking and Reporting

AI6.5 Change Closure and Documentation

AI7 Install and Accredite Solutions and Changes

New systems need to be made operational once development is complete. This requires proper testing in a dedicated environment with relevant test data, definition of rollout and migration instructions, release planning and actual promotion to production, and a post-implementation review. This assures that operational systems are in line with the agreed expectations and outcomes.

Control over the IT process of

Install and accredit solutions and changes

that satisfies the business requirement for IT of

new or changed systems working without major problems after installation

by focusing on

testing that applications and infrastructure solutions are fit for the intended purpose and free from errors, and planning releases to production

is achieved by

- Establishing test methodology
- Undertaking release planning
- Evaluating and approving test results by business management
- Performing post-implementation reviews

and is measured by

- Application down time or data fixes caused by inadequate testing
- Percent of systems that meet expected benefits as measured by post-implementation process
- Percent of projects with documented and approved testing plan

AI7.1 Training

AI7.2 Test Plan

AI7.3 Implementation Plan

AI7.4 Test Environment

AI7.5 System and Data Conversion

AI7.6 Testing of Changes

AI7.7 Final Acceptance Test

AI7.8 Promotion to Production

AI7.9 Software Release

AI7.10 System Distribution

AI7.11 Recording and Tracking of Changes

AI7.12 Post-implementation Review

Deliver and Support

This domain is concerned with the actual delivery of required services, which includes service delivery, management of security and continuity, service support for users, and management of data and the operational facilities. It typically addresses the following management questions:

- Are IT services being delivered in line with business priorities?
- Are IT costs optimised?
- Is the workforce able to use the IT systems productively and safely?
- Are adequate confidentiality, integrity and availability in place?

DS1 Define and Manage Service Levels

Effective communication between IT management and business customers regarding services required is enabled by a documented definition and agreement of IT services and service

levels. This process also includes monitoring and timely reporting to stakeholders on the accomplishment of service levels. This process enables alignment between IT services and the related business requirements.

Control over the IT process of

Define and manage service levels

that satisfies the business requirement for IT of

ensuring the alignment of key IT services with business strategy

by focusing on

identifying service requirements, agreeing on service levels and monitoring the achievement of service levels

is achieved by

- Formalising internal and external agreements in line with requirements and delivery capabilities
- Reporting on service level achievements (reports and meetings)
- Identifying and communicating new and updated service requirements to strategic planning

and is measured by

- Percent of business stakeholders satisfied that service delivery meets agreed-upon levels
- Number of delivered services not in the catalogue
- Number of formal SLA review meetings with business per year

DS1.1 Service Level Management Framework

DS1.2 Definition of Services

DS1.3 Service Level Agreements

DS1.4 Operating Level Agreements

DS1.5 Monitoring and Reporting of Service Level Achievements

DS1.6 Review of Service Level Agreements and Contracts

DS2 Manage Third-party Services

The need to assure that services provided by third parties meet business requirements requires an effective third-party management process. This process is accomplished by clearly defining the roles, responsibilities and expectations in third-party agreements as well as reviewing and monitoring such agreements for effectiveness and compliance. Effective management of third-party services minimises business risk associated with non-performing suppliers.

Control over the IT process of

Manage third-party services

that satisfies the business requirement for IT of

providing satisfactory third-party services while being transparent about benefits, costs and risks

by focusing on

establishing relationships and bilateral responsibilities with qualified third-party service providers and monitoring the service delivery to verify and ensure adherence to agreements

is achieved by

- Identifying and categorising supplier services
- Identifying and mitigating supplier risk
- Monitoring and measuring supplier performance

and is measured by

- Number of user complaints due to contracted services

- Percent of major suppliers meeting clearly defined requirements and service levels
- Percent of major suppliers subject to monitoring

DS2.1 Identification of All Supplier Relationships

DS2.2 Supplier Relationship Management

DS2.3 Supplier Risk Management

DS2.4 Supplier Performance Monitoring

DS3 Manage Performance and Capacity

The need to manage performance and capacity of IT resources requires a process to periodically review current performance and capacity of IT resources. This process includes forecasting future needs based on workload, storage and contingency requirements. This process provides assurance that information resources supporting business requirements are continually available.

Control over the IT process of

Manage performance and capacity

that satisfies the business requirement for IT of

optimising the performance of IT infrastructure, resources and capabilities in response to business needs

by focusing on

meeting response time requirements of service level agreements, minimising down time and making continuous IT performance and capacity improvements through monitoring and measurement

is achieved by

- Planning and providing system capacity and availability
- Monitoring and reporting system performance
- Modelling and forecasting system performance

and is measured by

- Number of hours lost per user per month due to insufficient capacity planning
- Percent of peaks where target utilisation is exceeded
- Percent of response time SLAs not met

DS3.1 Performance and Capacity Planning

DS3.2 Current Capacity and Performance

DS3.3 Future Capacity and Performance

DS3.4 IT Resources Availability

DS3.5 Monitoring and Reporting

DS4 Ensure Continuous Service

The need for providing continuous IT services requires developing, maintaining and testing IT continuity plans, offsite backup storage and periodic continuity plan training. An effective continuous service process minimises the probability and impact of a major IT service interruption on key business functions and processes.

Control over the IT process of

Ensure continuous service

that satisfies the business requirement for IT of

ensuring minimum business impact in the event of an IT service interruption

by focusing on

building resilience into automated solutions and developing, maintaining and testing IT continuity planst

is achieved by

- Developing and maintaining (improving) IT contingency
- Training on and testing IT contingency plans
- Storing copies of contingency plans and data at offsite locations

and is measured by

- Number of hours lost per user per month due to unplanned outages
- Number of business-critical processes relying on IT not covered by the IT continuity plan

DS4.1 IT Continuity Framework

DS4.2 IT Continuity Plans

DS4.3 Critical IT Resources

DS4.4 Maintenance of the IT Continuity Plan

DS4.5 Testing of the IT Continuity Plan

DS4.6 IT Continuity Plan Training

DS4.7 Distribution of the IT Continuity Plan

DS4.8 IT Services Recovery and Resumption

DS4.9 Offsite Backup Storage

DS4.10 Post-resumption Review

DS5 Ensure Systems Security

The need to maintain the integrity of information and protect IT assets requires a security management process. This process includes establishing and maintaining IT security roles and responsibilities, policies, standards and procedures. Security management also includes performing security monitoring and periodic testing and implementing corrective actions for identified security weaknesses or incidents. Effective security management protects all IT assets to minimise the business impact of security vulnerabilities and incidents.

Control over the IT process of

Ensure systems security

that satisfies the business requirement for IT of

maintaining the integrity of information and processing infrastructure and minimising the impact of security vulnerabilities and incidents

by focusing on

defining IT security policies, procedures and standards, and monitoring, detecting, reporting and resolving security vulnerabilities and incidents

is achieved by

- Understanding security requirements, vulnerabilities and threats
- Managing user identities and authorisations in a standardised manner
- Testing security regularly

and is measured by

- Number of incidents damaging reputation with the public
- Number of systems where security requirements are not met
- Number of violations in segregation of duties

DS5.1 Management of IT Security

DS5.2 IT Security Plan

DS5.3 Identity Management

DS5.4 User Account Management

DS5.5 Security Testing, Surveillance and Monitoring

DS5.6 Security Incident Definition

DS5.7 Protection of Security Technology

DS5.8 Cryptographic Key Management

DS5.9 Malicious Software Prevention, Detection and Correction

DS5.10 Network Security
DS5.11 Exchange of Sensitive Data

DS6 Identify and Allocate Costs

The need for a fair and equitable system of allocating IT costs to the business requires accurate measurement of IT costs and agreement with business users on fair allocation. This process includes building and operating a system to capture, allocate and report IT costs to the users of services. A fair system of allocation enables the business to make more informed decisions regarding use of IT services.

Control over the IT process of

Identify and allocate costs

that satisfies the business requirement for IT of

transparency and understanding of IT costs and improving cost-efficiency through well-informed use of IT services

by focusing on

complete and accurate capture of IT costs, a fair system of allocation agreed-upon by business users, and a system for timely reporting of IT use and costs allocated

is achieved by

- Aligning charges to the quality and quantity of services provided
- Building and agreeing a complete cost model
- Implementing charging as per the agreed-upon policy

and is measured by

- Percent of IT service bills accepted/paid by business management
- Percent of variance amongst budgets, forecasts and actual costs
- Percent of overall IT costs that are allocated according to the agreed-upon cost models

DS6.1 Definition of Services
DS6.2 IT Accounting
DS6.3 Cost Modelling and Charging
DS6.4 Cost Model Maintenance

DS7 Educate and Train Users

Effective education of all users of IT systems, including those within IT, requires identifying the training needs of each user group. In addition to identifying needs, this process includes defining and executing a strategy for effective training and measuring the results. An effective training programme increases effective use of technology by reducing user errors, increasing productivity and increasing compliance with key controls such as user security measures.

Control over the IT process of

Educate and train users

that satisfies the business requirement for IT of

effective and efficient use of applications and technology solutions and user compliance with policies and procedures

by focusing on

a clear understanding of IT user training needs, execution of an effective training strategy and measurement of the results

is achieved by

- Establishing training curricula
- Organising training
- Delivering training

- Monitoring and reporting on training effectiveness
- and is measured by**
 - Number of service desk calls due to lack of user training
 - Percent of stakeholder satisfaction with training provided
 - Time lag between identification of training need and the delivery of the training

DS7.1 Identification of Education and Training Needs

DS7.2 Delivery of Training and Education

DS7.3 Evaluation of Training Received

DS8 Manage Service Desk and Incidents

Timely and effective response to IT user queries and problems requires a well-designed and well-executed service desk and incident management process. This process includes setting up a service desk function with registration, incident escalation, trend and root cause analysis, and resolution. The business benefits include increased productivity through quick resolution of user queries. In addition, the business can address root causes (such as poor user training) through effective reporting.

Control over the IT process of

Manage service desk and incidents

that satisfies the business requirement for IT of

enabling effective use of IT systems by ensuring resolution and analysis of end-user queries, questions and incidents

by focusing on

a professional service desk function with quick response, clear escalation procedures, and resolution and trend analysis

is achieved by

- Installing and operating a service desk
- Monitoring and reporting trends
- Defining clear escalation criteria and procedures

and is measured by

- User satisfaction with first-line support
- Percent of incidents resolved within agreed/acceptable period of time
- Call abandonment rate

DS8.1 Service Desk

DS8.2 Registration of Customer Queries

DS8.3 Incident Escalation

DS8.4 Incident Closure

DS8.5 Trend Analysis

DS9 Manage the Configuration

Ensuring the integrity of hardware and software configurations requires establishment and maintenance of an accurate and complete configuration repository. This process includes collecting initial configuration information, establishing baselines, verifying and auditing configuration information, and updating the configuration repository as needed. Effective configuration management facilitates greater system availability, minimises production issues and resolves issues faster.

Control over the IT process of

Manage the configuration

that satisfies the business requirement for IT of

optimising the IT infrastructure, resources and capabilities, and accounting for

IT assets

by focusing on

establishing and maintaining an accurate and complete repository of asset configuration attributes and baselines, and comparing against actual asset configuration

is achieved by

- Establishing a central repository of all configuration items
- Identifying configuration items and maintaining them
- Reviewing integrity of configuration data

and is measured by

- Number of business compliance issues caused by improper configuration of assets
- Number of deviations identified between configuration repository and actual asset configurations
- Percent of licences purchased and not accounted for in repository

DS9.1 Configuration Repository and Baseline

DS9.2 Identification and Maintenance of Configuration Items

DS9.3 Configuration Integrity Review

DS10 Manage Problems

Effective problem management requires the identification and classification of problems, root cause analysis and resolution of problems. The problem management process also includes identification of recommendations for improvement, maintenance of problem records and review of the status of corrective actions. An effective problem management process improves service levels, reduces costs and improves customer convenience and satisfaction.

Control over the IT process of

Manage problems

that satisfies the business requirement for IT of

ensuring end users' satisfaction with service offerings and service levels, and reducing solution and service delivery defects and rework

by focusing on

recording, tracking and resolving operational problems; investigating the root cause of all significant problems; and defining solutions for identified operations problems

is achieved by

- Performing root cause analysis of reported problems
- Analysing trends
- Taking ownership of problems and progressing problem resolution

and is measured by

- Number of recurring problems with impact on business
- Percent of problems resolved within required time period
- The frequency of reports or updates to an ongoing problem, based on the problem severity

DS10.1 Identification and Classification of Problems

DS10.2 Problem Tracking and Resolution

DS10.3 Problem Closure

DS10.4 Integration of Change, Configuration and Problem Management

DS11 Manage Data

Effective data management requires identifying data requirements. The data management process also includes establishing effective procedures to manage the media library, backup

and recovery of data, and proper disposal of media. Effective data management helps ensure the quality, timeliness and availability of business data.

Control over the IT process of

Manage data

that satisfies the business requirement for IT of

optimising the use of information and ensuring information is available as required

by focusing on

maintaining the completeness, accuracy, availability and protection of data

is achieved by

- Backing up data and testing restoration
- Managing onsite and offsite storage of data
- Securely disposing of data and equipment

and is measured by

- User satisfaction with availability of data
- Percent of successful data restorations
- Number of incidents where sensitive data were retrieved after media were disposed of

DS11.1 Business Requirements for Data Management

DS11.2 Storage and Retention Arrangements

DS11.3 Media Library Management System

DS11.4 Disposal

DS11.5 Backup and Restoration

DS11.6 Security Requirements for Data Management

DS12 Manage the Physical Environment

Protection for computer equipment and personnel requires well-designed and well-managed physical facilities. The process of managing the physical environment includes defining the physical site requirements, selecting appropriate facilities and designing effective processes for monitoring environmental factors and managing physical access. Effective management of the physical environment reduces business interruptions from damage to computer equipment and personnel.

Control over the IT process of

Manage the physical environment

that satisfies the business requirement for IT of

protecting computer assets and business data and minimising the risk of business disruption

by focusing on

providing and maintaining a suitable physical environment to protect IT assets from access, damage or theft

is achieved by

- Implementing physical security measures
- Selecting and managing facilities

and is measured by

- Down time arising from physical environment incidents
- Number of incidents due to physical security breaches or failures
- Frequency of physical risk assessment and reviews

DS12.1 Site Selection and Layout

DS12.2 Physical Security Measures

- DS12.3 Physical Access
- DS12.4 Protection Against Environmental Factors
- DS12.5 Physical Facilities Management

DS13 Manage Operations

Complete and accurate processing of data requires effective management of data processing and maintenance of hardware. This process includes defining operations' policies and procedures for effective management of scheduled processing, protection of sensitive output, monitoring infrastructure and preventative maintenance of hardware. Effective operations management helps maintain data integrity and reduces business delays and IT operating costs.

Control over the IT process of

Manage operations

that satisfies the business requirement for IT of

maintaining data integrity and ensuring IT infrastructure can resist and recover from errors and failures

by focusing on

meeting operational service levels for scheduled data processing, protecting sensitive output, and monitoring and maintaining infrastructure

is achieved by

- Operating the IT environment in line with agreed-upon service levels and defined instructions
- Maintaining the IT infrastructure

and is measured by

- Number of service levels impacted by operational incidents
- Hours of unplanned downtime caused by operational incidents
- Percent of hardware assets included in preventive maintenance schedules

- DS13.1 Operations Procedures and Instructions
- DS13.2 Job Scheduling
- DS13.3 IT Infrastructure Monitoring
- DS13.4 Sensitive Documents and Output Devices
- DS13.5 Preventive Maintenance for Hardware

Monitor and Evaluate

All IT processes need to be regularly assessed over time for their quality and compliance with control requirements. This domain addresses performance management, monitoring of internal control, regulatory compliance and providing governance. It typically addresses the following management questions:

- Is IT's performance measured to detect problems before it is too late?
- Does management ensure that internal controls are effective and efficient?
- Can IT performance be linked back to business goals?
- Are risk, control, compliance and performance measured and reported?

ME1 Monitor and Evaluate IT Performance

Effective IT performance management requires a monitoring process. This process includes defining relevant performance indicators, a systematic and timely reporting of performance, and prompt acting upon deviations. Monitoring is needed to make sure that the right things are done and are in line with the set directions and policies.

Control over the IT process of

Monitor and evaluate IT performance

that satisfies the business requirement for IT of

transparency and understanding of IT cost, benefits, strategy, policies and service levels in accordance with governance requirements

by focusing on

monitoring and reporting process metrics and identifying and implementing performance improvements actions

is achieved by

- Collating and translating process performance reports into management reports
- Reviewing performance against agreed-upon targets and initiating necessary remedial action

and is measured by

- Satisfaction of management and the governance entity with the performance reporting
- Number of improvement actions driven by monitoring activities
- Percent of critical processes monitored

ME1.1 Monitoring Approach

ME1.2 Definition and Collection of Monitoring Data

ME1.3 Monitoring Method

ME1.4 Performance Assessment

ME1.5 Board and Executive Reporting

ME1.6 Remedial Actions

ME2 Monitor and Evaluate Internal Control

Establishing an effective internal control programme for IT requires a well-defined monitoring process. This process includes the monitoring and reporting of control exceptions, results of self-assessments and third-party reviews. A key benefit of internal control monitoring is to provide assurance regarding effective and efficient operations and compliance with applicable laws and regulations.

Control over the IT process of

Monitor and evaluate internal control

that satisfies the business requirement for IT of

protecting the achievement of IT objectives and complying with IT-related laws and regulations

by focusing on

monitoring the internal control processes for IT-related activities and identifying improvement actions

is achieved by

- Defining a system of internal controls embedded in the IT process framework
- Monitoring and reporting on the effectiveness of the internal controls over IT
- Reporting control exceptions to management for action

and is measured by

- Number of major internal control breaches
- Number of control improvement initiatives
- Number and coverage of control self-assessments

ME2.1 Monitoring of Internal Control Framework

ME2.2 Supervisory Review

ME2.3 Control Exceptions

ME2.4 Control Self-assessment

ME2.5 Assurance of Internal Control

ME2.6 Internal Control at Third Parties

ME2.7 Remedial Actions

ME3 Ensure Regulatory Compliance

Effective regulatory oversight requires the establishment of an independent review process to ensure compliance with laws and regulations. This process includes defining an audit charter, auditor independence, professional ethics and standards, planning, performance of audit work, and reporting and follow-up of audit activities. The purpose of this process is to provide positive assurance related to IT compliance with laws and regulations.

Control over the IT process of

Ensure regulatory compliance

that satisfies the business requirement for IT of

compliance with laws and regulations

by focusing on

identifying all applicable laws and regulations and the corresponding level of IT compliance and optimising IT processes to reduce the risk of non-compliance

is achieved by

- Identifying legal and regulatory requirements related to IT
- Assessing the impact of regulatory requirements
- Monitoring and reporting on compliance with regulatory requirements

and is measured by

- Cost of IT non-compliance, including settlements and fines
- Average time lag between identification of external compliance issues and resolution
- Frequency of compliance reviews

ME3.1 Identification of Laws and Regulations Having Potential Impact on IT

ME3.2 Optimisation of Response to Regulatory Requirements

ME3.3 Evaluation of Compliance With Regulatory Requirements

ME3.4 Positive Assurance of Compliance

ME3.5 Integrated Reporting

ME4 Provide IT Governance

Establishing an effective governance framework includes defining organisational structures, processes, leadership, roles and responsibilities to ensure that enterprise IT investments are aligned and delivered in accordance with enterprise strategies and objectives.

Control over the IT process of

Provide IT governance

that satisfies the business requirement for IT of

integrating IT governance with corporate governance objectives and complying with laws and regulations

by focusing on

preparing board reports on IT strategy, performance and risks, and responding to governance requirements in line with board directions

is achieved by

- Establishing an IT governance framework integrated into corporate governance
- Obtaining independent assurance over the IT governance status

and is measured by

- Frequency of board reporting on IT to stakeholders (including maturity)
- Frequency of reporting from IT to board (including maturity)

- Frequency of independent reviews of IT compliance

ME4.1 Establishment of an IT Governance Framework

ME4.2 Strategic Alignment

ME4.3 Value Delivery

ME4.4 Resource Management

ME4.5 Risk Management

ME4.6 Performance Measurement

ME4.7 Independent Assurance

Generally Accepted Information Security Principles (GAISP)

Candidate principles are organized in a three-level hierarchy. The hierarchy is comprised of:

- Pervasive Principles - few in number, fundamental in nature, and rarely changing. Target: Governance
- Broad Functional Principles - subordinate to one or more of the Pervasive Principles, are more numerous and specific, guide the development of more Detailed Principles, and change only when reflecting major developments in technology or other affecting issues. Target: Operational Management
- Detailed Principles - subordinate to one or more of the Broad Functional Principles, numerous, specific, emergent and change frequently as technology and other affecting issues evolve. Target: the Information Security Practitioner

2.0 PERVASIVE PRINCIPLES

The Pervasive Principles provide general governance-level guidance to establish and maintain the security of information. These principles form the basis of Broad Functional Principles and Detailed Principles. Security of information is achieved through the preservation of appropriate confidentiality, integrity, and availability.

2.1 Accountability Principle

Information security accountability and responsibility must be clearly defined and acknowledged.

Accountability characterizes the ability to audit the actions of all parties and processes that interact with information. Roles and responsibilities are clearly defined, identified, and authorized at a level commensurate with the sensitivity and criticality of information. The relationship between all parties, processes, and information must be clearly defined, documented, and acknowledged by all parties. All parties must have responsibilities for which they are held accountable.

2.2 Awareness Principle

All parties, including but not limited to information owners and information security practitioners, with a need to know should have access to applied or available principles, standards, conventions, or mechanisms for the security of information and information systems, and should be informed of applicable threats to the security of information.

This principle applies between and within organizations. Awareness of information security principles, standards, conventions, and mechanisms enhances and enables controls and can help to mitigate threats. Awareness of threats and their significance also increases user acceptance of controls. Without user awareness of the necessity for particular controls, the users can pose a risk to information by ignoring, bypassing, or overcoming existing control mechanisms. The awareness principle applies to unauthorized and authorized parties.

2.3 Ethics Principle

Information should be used, and the administration of information security should be executed, in an ethical manner.

Information systems pervade our societies and cultures. Rules and expectations are evolving with regard to the appropriate provision and use of information systems and the security of information. Use of information and information systems should match the expectations established by social norms, and obligations.

2.4 Multidisciplinary Principle

Principles, standards, conventions, and mechanisms for the security of information and information systems should address the considerations and viewpoints of all interested parties.

Information security is achieved by the combined efforts of information owners, users, custodians, and information security personnel. Decisions made with due consideration of all relevant viewpoints and technical capabilities can enhance information security and receive better acceptance.

2.5 Proportionality Principle

Information security controls should be proportionate to the risks of modification, denial of use, or disclosure of the information.

Security controls should be commensurate with the value of the information assets and the vulnerability. Consider the value, sensitivity and criticality of the information, and the probability, frequency and severity of direct and indirect harm or loss. This principle recognizes the value of approaches to information security risk management, ranging from prevention to acceptance.

2.6 Integration Principle

Principles, standards, conventions, and mechanisms for the security of information should be coordinated and integrated with each other and with the organization's policies and procedures to create and maintain security throughout an information system.

Many breaches of information security involve the compromise of more than one safeguard. The most effective control measures are components of an integrated system of controls. Information security is most efficient when planned, managed, and coordinated throughout the organization's system of controls and the life of the information asset.

2.7 Timeliness Principle

All accountable parties should act in a timely, coordinated manner to prevent or respond to breaches of and threats to the security of information and information systems.

Organizations should be capable of swift coordination and action to enable threat event prevention or mitigation. This principle recognizes the need for the public and private sectors to jointly establish mechanisms and procedures for rapid and effective threat event reporting and handling. Access to threat event history could support effective response to threat events and may help to prevent future incidents.

2.8 Assessment Principle

The risks to information and information systems should be assessed periodically.

Information and the requirements for its security vary over time. Risks to the information; its value; and the probability, frequency, and severity of direct and indirect harm/loss should undergo periodic assessment. Periodic assessment identifies and measures the variances from available and established security measures and controls, such as those articulated here in the GAISP, and the risk associated with such variances. Periodic assessment enables accountable parties to make informed, information risk management decisions whether to accept, mitigate, or transfer the identified risks with due consideration of cost effectiveness.

2.9 Equity Principle

Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.

Information security measures implemented by an organization should not infringe upon the obligations, rights, and needs of legitimate users, owners, and others affected by the information when exercised within the legitimate parameters of the mission objectives.

3.0 BROAD FUNCTIONAL PRINCIPLES

The Broad Functional Principles (BFP) are derived from the Pervasive Principles (PP) that represent the broad conceptual goals of information security. By providing the guidance for operational accomplishment of the Pervasive Principles, the Broad Functional Principles are the building blocks (what to do, at a high level) that comprise the Pervasive Principles and allow

definition of the basic units of those principles. Because the Broad Functional Principles are smaller in scope, they are easier to address in terms of implementation planning, and execution.

3.1 Information Security Policy

Management shall ensure that policy and supporting standards, baselines, procedures, and guidelines are developed and maintained to address all aspects of information security. Such guidance must assign responsibility, the level of discretion, and how much risk each individual or organizational entity is authorized to assume.

In order to assure that Information assets are effectively and uniformly secured consistent with their value and associated risk factors, management must clearly articulate its security strategy and associated expectations. In the absence of this clarity, some resources will be under-secured - that is, ineffective; other resources will be oversecured - that is, inefficient.

3.2 Education and Awareness

Management shall communicate information security policy to all personnel and ensure that all are appropriately aware. Education shall include standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and consequences of failure to comply.

In order to ensure that all personnel are effectively aware of security policy, management must effectively and regularly communicate its requirements. When personnel fail to do what management expects, it is more often the result of an ineffective or imperfect communication of what management expects, rather than from the result of wrongful motive or intent on the part of the personnel. The failure to regularly and effectively communicate information security policy, standards, baselines, procedures, guidelines, responsibilities, related enforcement measures, and the consequences of failing to comply, to all relevant parties can cause the unintentional breach of policy by parties to whom the policy has not been effectively communicated. Such failure can also result in the intentional breach of policy by parties to whom the adverse consequences of such a breach have not been effectively communicated.

In both cases, the potential for harm, liability, or loss to the organization or other relevant parties can be significant. The failure to effectively communicate information security policy can also impair the ability to successfully apply enforcement measures, prosecute criminal activity, or seek civil redress.

3.3 Accountability

Management shall hold all parties accountable for their access to and use of information, e.g., additions, modifications, copying and deletions, and supporting Information Technology resources. It must be possible to affix the date, time, and responsibility, to the level of an individual, for all significant events.

In order to assure that people behave as expected, it is necessary to know who did what and when it was done.

It is essential that organizations establish and maintain a basis of control for information assets. Such a control framework requires individual and organizational accountability at all levels. The concept of "accountability" refers to the accepting of responsibility by all relevant parties or entities. Holding all parties thusly accountable is intended to assure that any use made of or actions taken on information assets and supporting Information Technology resources shall be for authorized "business/mission purposes only" and that such use or action can be reliably traced to the responsible party or parties, who will be held "accountable."

3.4 Information Management

Management shall routinely catalog and value information assets, and assign levels of sensitivity and criticality. Information, as an asset, must be uniquely identified and responsibility for it assigned.

In order to manage information assets efficiently, management must know what to protect. In order to be effectively managed, it is essential to identify and enumerate the core attributes of information as assets. These information asset attributes include:

- Identity,
- Ownership,
- Custody,
- Content,
- Value (ideally expressed in monetary terms) of the confidentiality, availability, and integrity of the information assets
- Sensitivity (which relates directly to confidentiality), and
- Criticality (which relates directly to availability and integrity).

The organizational ownership of an information asset must be established. The person or agent/custodian legitimately established as the owner of an information asset has the authority and responsibility to make - or delegate - decisions regarding the security of the information asset. It is typically the organization that will ultimately suffer liability, loss, or other harm if the confidentiality, availability, or integrity of the information asset is compromised, though others may suffer harm or loss as well.

The identity and content of the information asset must be clearly established for the owner to make informed decisions regarding its security. Knowing the value of the information asset, as related to its confidentiality, availability, and integrity, enables the owner to understand the financial risks and associated threats that must be mitigated when establishing security requirements for the information asset.

Finally, these attributes should be reviewed regularly, because most information attributes change value over time - in some cases increasing and in others, decreasing.

3.5 Environmental Management

Management shall consider and compensate for the risks inherent to the internal and external physical environment where information assets and supporting Information Technology resources and assets are stored, transmitted, processed, or used.

In order to effectively protect the organizational mission, it is necessary to identify and address environmental threats that can disrupt Information Technology functionality. There are significant threats - and vulnerabilities - associated with the location, construction, and equipping of Information Technology facilities. These threats include:

- Natural disaster threats (earthquake, flood, hurricane, tornado, landslides, etc.), and
- Unintentional or intentional physical threats (power outage, equipment failure, fire, proximity of potentially toxic or explosive industrial facilities and transportation infrastructures, local crime, and a wide array of accidents that could “exploit” unrecognized or inadequately addressed vulnerabilities of the physical environment.).

For the optimum security strategy implementation, it is essential to coordinate and integrate information security efforts with overall organizational security measures and management. Failure to recognize and effectively address local threats and associated vulnerabilities, both internal and external, can result in a potentially disastrous disruption of Information Technology functionality.

3.6 Personnel Qualifications

Management shall establish and verify the qualifications related to integrity, need-to-know, and technical competence of all parties provided access to information assets or supporting Information Technology resources.

In order to effectively implement security for information assets and supporting Information Technology resources, it is necessary that the personnel involved are competent with respect to the knowledge and technical skill needed to perform their roles reliably, that their integrity (as demonstrated by work history, academic and training certification, and

references) meets organizational requirements, and that their need-to-know is authoritatively established. Such personnel include, at a minimum:

- Owners (as representatives of the organization and its interests),
- Users,
- Contractors and supplemental staff,
- Custodians, and
- Information security personnel.

3.7 System Integrity

Management shall provide the capability to respond to and resolve information security incidents expeditiously and effectively in order to ensure that any business impact is minimized and that the likelihood of experiencing similar incidents is reduced.

Information security “incidents” are defined by the Carnegie Mellon Computer Emergency Response Team (CERT) as, essentially, the occurrence of a denial-of-service, virus, worm, Trojan horse, or other similar malefactor on the Internet that impacts a number of on-line parties. From the perspective of the individual party, such incidents can have effects from the complete corruption of data on their Internet-accessible systems to simply denying them access to the Internet. Such incidents are differentiated from the kind of disruptive event(s) addressed by the activities discussed in 3.10 Operational Continuity and Contingency Planning below and require significantly different planning and response.

3.8 Information Systems Life Cycle

Management shall ensure that security is addressed at all stages of the system life cycle.

In order for management to be able to rely upon controls, they must be continuous. In order to be efficient, controls must be comprehensive and applied early. The security function must be fully integrated with system life cycle processes. Retrofit, repair, and other late remedies are always inefficient and may be ineffective. Late application of a control may be insufficient to restore a system to a desired or required robustness.

3.9 Access Control

Management shall establish appropriate controls to balance access to information assets and supporting Information Technology resources against the risk.

In order to achieve a level of risk mitigation commensurate with the value of the information asset to be secured, access to information assets and supporting Information Technology resources should be restricted to the smallest population consistent with other business needs, based on the criteria of a clearly delineated “need-to-know.” Through this standard, the information systems-dependent workforce is facilitated in the accomplishment of assigned tasks by ensuring that all required information is available only through appropriately controlled means. Specifically, individual employees and other parties are restricted from access to information assets and supporting Information Technology resources that do not directly relate to their work requirements, assigned objectives, or legitimate, authorized need.

3.10 Operational Continuity and Contingency Planning

Management shall plan for and operate Information Technology in such a way as to preserve the continuity of organizational operations.

In order to protect information assets and supporting Information Technology resources from disruptive events, or to be able to rapidly restore their proper functioning in the case that such a disruptive event is unavoidable, it is essential that organizations establish a cohesive set of preventive, mitigative, and restorative measures, as determined to be appropriate and cost-effective by risk assessment.

Organizational entities depend on their Information Technology resource infrastructure now more than at any previous time in history to deliver mission-critical information in a timely fashion. The operational importance of information assets, whether based on cost or time

factors, is such that organizations can ill afford to endure the consequences of significantly disruptive events impacting supporting Information Technology resources or the information assets directly.

3.11 Information Risk Management

Management shall ensure that information security measures are appropriate to the value of the assets and the threats to which they are vulnerable.

In order to choose effective and efficient information security measures, management must identify the assets to be protected, the threats to the assets, and the vulnerability of the assets or their environment to the threats.

The security of information assets, with regard to the value of their confidentiality, integrity, and availability, and the security of the supporting Information Technology resources, must be assured by well-informed owners, managers, custodians, or other responsible parties. Such an approach (performed strategically, on an on-going basis, or as changes dictate) must enable well-informed decisions regarding whether to accept, mitigate, or transfer the risks associated with the information assets and supporting Information Technology resources. These decisions should be based on the monetary value of the assets, probability and consequences of direct or indirect harm or loss, related threats, effectiveness of existing safeguards and controls, and whether additional safeguards or controls could be expected to provide cost-effective incremental risk mitigation.

3.12 Network and Infrastructure Security

Management shall consider the potential impact on the shared global infrastructure, e.g., the Internet, public switched networks, and other connected systems, when establishing network security measures.

In order to compensate for the increased vulnerability from and to things outside of the organization, as created by connection to systems beyond the organization, the threat and risk model must be changed to reflect the threat from and to things outside the organization. For example, connecting a UNIX system to the public switched network puts the UNIX system at risk, and connecting the UNIX system to the Internet puts other systems at risk.

All methods for accessing Information Technology resource connectivity must contain controls and counter-measures that implement the established security policy of the organization appropriate to the sensitivity or criticality level of the Information Technology resources and supported information assets. Such controls must, at a minimum, reflect the same security level as the information itself to ensure consistency and cohesiveness of overall policy implementation. This consideration must extend to the physical as well as the logical aspect of the connectivity.

The potential to subvert access to the Information Technology resources and supported information assets is greatest in terms of connectivity through persistent connections, but increases with temporary connections. This same potential exists, however, through in-house networks, though these are inherently less flexible in their vulnerability to exploitation. Therefore, the security implementation must first identify the specific weaknesses in each access method and the potential consequences of their exploitation. Then each weakness can be addressed through the application of measures intended to achieve a level of protection commensurate with the sensitivity/criticality of the Information Technology resource and the supported information assets.

3.13 Legal, Regulatory, and Contractual Requirements of Information Security

Management shall take steps to be aware of and address all legal, regulatory, and contractual requirements pertaining to information assets.

In order for an organization to diligently comply with all legal, regulatory, and contractual requirements associated with its operations, it is necessary to ensure that no requirement exists for which compliance measures have not been put in place. As part of this effort,

plans should also be in place to address potential actions against the organization should their policy, processes, or actions be called into question.

3.14 Ethical Practices

Management shall respect the rights and dignity of individuals when setting policy and when selecting, implementing, and enforcing security measures.

In order to preserve employee morale and the perception of the organization and its management as fair and ethical, and recognizing that security measures may be or become unduly intrusive, management must be candid, fair, and conservative in developing and enforcing security policy.

Management must carefully consider employee privacy. The key to successful policy is strict observance of fairness and respect for the individual. No policy is complete proof against culpability, but careful construction and consistently unbiased execution contribute positively to the organization's overall risk management program.

Policy provisions, including consequences for non-compliance, must be understandable and enforceable, and enforcement must be fairly applied. Candor helps ensure fairness. Security measures that cannot be disclosed should not be applied.

Owner's conservative rule: Owners should assume that others would treat their assets as belonging to the public domain. Therefore, they should explicitly declare (in reasonably visible ways) the products of their efforts and their property to be either private or public.

User's conservative rule: Assume that any tangible or intangible item belongs to somebody else unless an explicit declaration or convention identifies it as being in the public domain or authorized for your use.

4.0 DETAILED SECURITY PRINCIPLES

The Detailed Security Principles specifically address methods of achieving compliance with the Broad Functional Principles with respect to existing environments and available technology. There will be many detailed information security principles supporting one or more Broad Functional Principles. The Detailed Principles will address differing technologies, environments, standards, practices, and concepts that are relevant to the Broad Functional Principles. The Detailed Principles are expected to continuously evolve to meet the challenges of emerging technology and new threats.

Information Systems Security Assessment Framework (ISSAF)

3 THE FRAMEWORK

ISSAF provides a four phase model that structures the management of security initiatives and ensures the viability of the engagement by providing the requisite know-how in the form of bite-sized work packages (referred to as activities) that can be assigned to individuals within the project team.

The four phases respectively are Planning, Assessment, Treatment, and Accreditation. Each of these phases has specific work packages that are generic to all organizations regardless of their size, their specific key result areas, and their geographical siting. Through the sequencing of their respective work packages, these phases focus on delivering specific results, be it a deliverable or a desired state of affairs. The outputs of these phases are then followed by operational activities designed to integrate the deliverable or to maintain the achieved state, feasibly and effectively.

3.1 PHASE I – PLANNING

3.1.1 Information Gathering

Information gathering therefore seeks to assemble a complete picture of the information technology infrastructure to serve as the basis for the next phase, namely risk assessment. ISSAF has assembled a set of questions that can serve as the basis for this information gathering in a document titled ISSAF – Information Gathering Questionnaire. It is recommended that the security practitioner collates this information and analyze their findings prior to moving to the next stage namely, preparing the business case to align management of security as a priority.

3.1.2 Project Chartering

We recommend identifying the critical success factors (desired outcomes) and then mapping them to all key internal business processes including revenue and expense cycles, as a starting step. This will facilitate the identification of which business processes are most critical to the business, and this in turn will help prioritize which systems are critical to these processes. Based on this analysis, it is recommended to fill out the sample Project Charter template to initiate discussions with the proposed project sponsor(s) and to document their expectations in this regard. Once the project charter is completed, use this document to obtain an internal signoff to ensure that project planning proceeds on the documented assumptions.

3.1.3 Resource Identification

Using the project charter, it is possible to identify at a high level the resources that are likely to be required to deliver the required results. Resources can range from people, products, processes, tools, knowledge and political support. The objective of this activity is to research the type and potential costs of the resources that will be required to execute this project. The key objective for this phase is to understand whether this project is feasible from a financial and human resourcing standpoint. At this point it is likely that the project charter may require further revision to narrow or broaden the scope based on the correction or validation of the many assumptions that would have driven the definition of the earlier charter.

3.1.4 Budgeting

Next a budget is prepared that identifies investments and subsequent operating costs to establish whether the required funding is likely to be feasible from an overall business perspective. The budget should consist of the following supporting schedules in addition

to the actual project budget to help the organization's financial team assess and/or integrate the project funding into the annual capital/operations budgets.

3.1.5 *Cash flow – pro forma preparation*

It's important to prepare the following: • Income statement (Profit & Loss); • Balance sheet. Unless these pro forma statements are prepared the financial team will be unable to do basic financial analysis such as the preparation of depreciation/amortization schedules, identify the increase in operating costs caused by new hires, training needs, etc.

3.1.6 *Work breakdown structure*

A work breakdown structure (WBS) essentially creates a framework that groups and integrates the individual work packages that will work in concert to deliver the project results. Work packages are a collection of related tasks usually carried out by an integral unit, such as a team or an individual or through automation. This structure is composed using a hierarchical outline that progressively breaks down activities into smaller and smaller chunks until the final chunk results in an assignable work package.

3.1.7 *Project kick-off*

The primary purpose of the Project Kick-off is to formally appoint the project manager. This ensures that the project manager has the necessary visibility and functional authority to make the decisions required to deliver the defined project results.

3.2 PHASE II – ASSESSMENT

The Assessment Phase provides a holistic approach to assessing Information Security Risks to an enterprise. This phase advocates approaching Information Security Risks to an enterprise. This phase advocates approaching Information Security Risk assessments from the perspective of the enterprise business objectives and associated risks. This would ensure the alignment of the enterprise business risks with the risks in relation to the nature and extent of usage of Information Technology for the achievement of the business objectives of an enterprise.

The assessment phase provides an overview of the ISSAF risk assessment process and addresses the different components involved. The assessment phase is divided into two categories: 1. Inherent Risk Identification and 2. Controls Assessment.

3.2.1 *Inherent Risk Assessment*

3.2.1.1 ASSESSMENT PREPARATION

Identification of Assessment entities – These could be processes, assets, facilities etc. The assessment entities constitute the basis for identifying applicable assessment parameters, threats, etc to the entities.

Identify threats and Vulnerabilities – The various vulnerabilities of the selected or identified entities for assessment are documented. Next, the threats that could exploit a single or multiple vulnerabilities are identified and listed. These threats constitute the risks for the entities. These risks can be repeatable to an entity.

3.2.1.2 THREAT ASSESSMENT

Impact Assessment – The impact to the business of an organization of a threat being realized against an asset is measured or estimated. This is done individually for each asset entity, and does not consider risk mitigating factors. It is a measure of raw risk.. The assessor can choose to average or sum the assessment parameter values for mathematical or logical reasons.

Likelihood Assessment – Here the probability of occurrence of the threat for the chosen assessment entity is measured or estimated.

3.2.2 *Controls Assessment*

Compensating controls may be in place to reduce or mitigate risks. These factors need to be accounted for in an accurate risk assessment. After obtaining the inherent risk of an

assessment entity, evaluation of controls is performed to identify the amount of risk reduction they offer, and the residual risk that remains for the assessment entity.

- Evaluation of Legal and Regulatory Compliance
- Evaluation of Enterprise Information Security Policy
- Evaluation of Enterprise Information Security Organization and Management
- Assessment of Enterprise Information Systems Security and Controls
- Evaluation of Enterprise Security Operations Management
- Evaluation of Enterprise Business Continuity Management
- Manage Residual Risks

3.3 PHASE III - TREATMENT

Risk treatment provides a platform for taking a decision for the residual risks, through the selection of safeguards, development of implementation plans, and providing accurate documentation for the implementation of, and decision making process. Risk decision is an important stage where executive management and other stakeholders review your documentation and make a decision to accept, mitigate, transfer or avoid the risk. Once this decision is made, plans for implementing the outcome are made, and approvals are sought for budgetary requirements, for project planning, for implementation and for change management.

3.4 PHASE IV - ACCREDITATION

The process of accreditation involves assessing the controls that have been selected for implementation under the scope for certification. The assessment results determine the accreditation of the ISSAF certification to an organization.

3.4.1 Context Establishment

Contact OISSG / Authorized Certification Bodies
Auditor Assignment

3.4.2 Evaluation

After the initiation is done, OISSG auditors would approach the organization for further discussions regarding the scope and coverage of the accreditation process.

3.4.3 Reporting

Auditors would then prepare a draft report based on their findings and present it to the senior management of the organization. This report highlights the level of compliance that the organization has achieved vis-à-vis ISSAF. It also consists a detailed breakdown of areas where non-compliances were found along with the severity of such non-compliance. Management feedback on the non-compliances found is considered before deciding on further course of action.

3.4.4 Certification

Based on the degree of compliance, a certification of ISSAF compliance is issued. Any outstanding issue in the form of recommendations for further action will be checked in subsequent ISSAF reviews & subject to closure of all outstanding items from previous ISSAF reviews, a recertification will be granted every two years.

3.5 PHASE V – MAINTENANCE

ISSAF certified organizations will be required to demonstrate compliance to the ISSAF accreditation on a continuing basis. To ensure this, OISSG will conduct regularly scheduled compliance assessments/reviews. The frequency for this review will be based on the size of the organization and the accreditation scope.

4 ENGAGEMENT MANAGEMENT

An engagement is grouping of activities that, when put together, achieve an objective and a goal. An engagement always has a recognizable start and an end. This document provides an overview on engagement management for security assessment engagements.

4.1 ENGAGEMENT EXECUTIVE OVERVIEW

The executive summary provides a summary of the engagement definition document. In many cases, this is a PowerPoint presentation. If it is, then a reference to the external document can be included. This section contains high-level explanation of the engagement objectives, scope, assumptions, risks, costs, timeline, approach, and organisation.

4.2 OBJECTIVE

Objectives are statements to describe what an engagement will achieve and deliver. Objectives should be “SMART”: Specific, Measurable, Achievable, Realistic, and Time-Based. To be specific and concrete, objectives should be based on deliverables (outcomes). The completion of an objective should be evident through deliverables (outcomes). The completion of an objective should be evident through the creation of one or more deliverables. If the statement is at a high level and does not imply the creation of a deliverable, it may be a goal instead. If the statement is too low-level and describes features and functions, then it may be a requirement statement instead.

4.3 APPROACH

Illustrate an overview of the methodology used for security assessment engagement. Generally the phases involved in typical security assessment engagement are:

- Planning and Preparation (Scoping & Logistics);
- Assessment (Fieldwork);
- Reporting (Conclusion / Results).

4.4 ENGAGEMENT SCOPE

In this section, you should clearly define the logical boundaries of your engagement. Scope statements are used to define what is within the boundaries of the engagement and what is outside those boundaries. Examples of areas that could be examined are data, processes, applications, or business areas.

4.5 ENGAGEMENT KICKOFF MEETING (INTERNAL)

As you win an engagement, Engagement Manager shall call a Engagement Kickoff Meeting.

- Quick look at lesson learned in previous engagement
- Declare Single Point of Contact for Engagement
- Form Engagement Team and divide their tasks
- Set deadlines on divided tasks to members responsible for Engagement Execution
- Process Administrative Tasks
- Availability of Tools (Commercial/Freeware)
- Efficient delivery capabilities of promised tasks in proposal
- Any help needed for delivery
- Inform Technical Infrastructure Management department about IP Addresses
- Engagement manager or assigned team member shall give minutes of meetings to everybody

4.6 COMMUNICATIONS PLAN

4.7 ENGAGEMENT KICKOFF DISCUSSION WITH CLIENT

- Identify access points and number of devices needs to be tested
- Deliverables
- Single Point of Contact from both end
- Team Introduction
- Engagement start and end date

- Working days/hrs
- Internet Access during onsite assessment
- Site location and contact numbers
- Update client about source IP addresses used for testing perform assessment.
- Make sure access to service is given from your company /ISP Router and Firewall

4.8 SAMPLE STATUS REPORT

If appropriate, provide background information for this report. You may wish to include the following information in your comments:

- Origins of the engagement;
- business reason for its initiation;
- anticipated value to the customer;
- and engagement increase to revenue or decrease to cost.

Engagement scope and objective.

4.9 ISSUE ESCALATION PLAN

Escalation chart in case of issue can be provided in this section. Escalation will happen both client and assessment organization. A flow chart will be of great help.

4.10 DEVELOP A ENGAGEMENT PLAN AND SEND IT TO CUSTOMER FOR UPDATE

- Send test cases which you are going to execute
- Put time for every test case
- Mention start and end date of engagement
- Time of assessment
- Contacts of each team

4.11 SET MILESTONES AND TIMELINES

Define milestones of engagements as per tasks, stick to them and achieve in defined time. Try to complete testing in office hours. It will help to minimize any down time if it occurs in any circumstances.

4.12 ENGAGEMENT SCHEDULE

4.13 DELIVERABLES PRODUCED

All engagements have deliverables. In this section, describe the deliverables of the engagement. Provide enough explanation and detail so that the reader will be able to understand what is being produced.

4.14 ENGAGEMENT ESTIMATED EFFORT/COST/DURATION (COST OPTIONAL)

The estimated effort hours and engagement costs may be depicted in many ways, including cost by team member, cost by deliverable, cost by milestone, or cost by including cost by team member, cost by deliverable, cost by milestone, or cost by category (internal labor, external labor, travel, training, supplies, etc.). Also include a chart showing the engagement start date, major milestones, and end date. The deliverables included in this milestone chart should all have been described in the scope section.

4.15 ENGAGEMENT ASSUMPTIONS

Engagement assumptions are circumstances and events that need to occur for the engagement to be successful but are outside the total control of the engagement team. They are listed as assumptions if there is a HIGH probability that they will in fact happen. The assumptions provide a historical perspective when evaluating engagement performance and determining justification for engagement-related decisions and direction.

4.16 ENGAGEMENT RISKS

Engagement risks are circumstances or events that exist outside of the control of the engagement team that will have an adverse impact on the engagement if they occur. (In other words, whereas an issue is a current problem that must be dealt with, a risk is a

potential future problem that has not yet occurred.) All engagements contain some risks. It may not be possible to eliminate risks entirely, but they can be anticipated and managed, thereby reducing the probability that they will occur.

4.17 ENGAGEMENT APPROACH

This section is used to describe how the engagement will be structured and the important techniques that will be utilized. The engagement approach is intended to encourage the engagement manager to think about the engagement from the top down instead of the traditional bottom-up method. Including the approach in the engagement definition compels the engagement manager to both consider the dependencies of the engagement and to incorporate the engagement management necessary to plan and manage the engagement.

4.18 ENGAGEMENT ORGANIZATION (ASSESSMENT TEAM & CLIENT)

It is important to understand who the major players are on the engagement. An organization chart works well. Otherwise, list the major engagement roles and the actual people involved.

4.19 RESPONSIBILITY MATRIX

5 GOOD PRACTICES– PRE ASSESSMENT, ASSESSMENT AND POST ASSESSMENT

This section provides all the good practices / guidelines required to perform the security assessment. Management, key people involved in assessment and all other members of the assessment team must read and follow it. Owner and Assessment Company (irrespective of internal or external) should sign it before starting an assessment.

5.1 PHASE – I: PRE-ASSESSMENT

5.1.1 Request for Proposal (RFP)

The organization shall clearly define followings:

- Name and details of person to whom proposal needs to be submitted
- Maximum time to submit the proposal (E.g. 1st Jan 2005)
- Maximum time to complete the assessment (e.g. March 2005)
- High level design of network architecture to selected companies after signing Non-Disclosure Agreement(NDA)

5.1.2 Evaluation of Third Party Contracts

5.1.2.1 PURPOSE OF THIRD PARTY CONTRACTS EVALUATION – An organization would typically have no control over the security management at a third party and therefore have no control over the security of their own information. The best an organization can do in most cases is to cover themselves legally with the appropriate clauses in contracts with third parties.

5.1.2.2 AIM / OBJECTIVE OF THIRD PARTY CONTRACTS EVALUATION – As part of an evaluation of information systems security, contracts with third parties must be evaluated to see if the organization is adequately covered legally.

This is also a recommendation within ISO 17799.

5.1.2.3 THIRD PARTY CONTRACT EVALUATION GUIDELINES – Contracts with third-parties should have clauses similar to those mentioned in this section. Not all clauses will be suitable in all cases. And additional clauses will be required for the specific services provided.

Existing contracts typically provide good coverage of some of the items listed in ISO 17799, such as service level agreements and intellectual property rights. This section highlights those items that existing contracts do not typically cover.

5.1.3 Sales and Marketing

Some of the guidelines during the sales life cycle are as follows:

- Consider the size, politics, type of industry
- Take into account the skills and knowledge of the organization's personnel
- Consider the organization mission, goals and objectives for this project.
- Consider the risks and complexity of the service required.
- The Sales Person should understand the need for right pricing, based on the two considerations above.
- Sales person should understand the complete assessment cycle.

5.1.4 Obtain Authorization and Make sure Right People has given it

Security assessment involves performing actions very similar, if not identical, to those carried out by an attacker. Likewise, the security test may result in the compromise of information systems due to which classified information may be accessed during the test. Even in the case that an agreement exists between the security assessor and the client, the latter may not accept, for instance, that classified information may become revealed to the security assessor.

5.1.5 Define the scope of work

As part of the contract or agreement between the security assessor and the client, the scope of the work to be done must be clearly specified. Whenever possible, loose or ambiguous definitions should be avoided. The security assessment work will be performed with better accuracy and its results will be more reliable when the extent of the work is bounded.

5.1.6 Define the "Out of Scope" Areas

After going through scope of work definitions; there must be clearly defined limitations and conditions for assessors, which he should not violate.

5.1.7 Sign Agreement

On the basis of above mentioned points sign a formal agreement. This written permission, often called the rules of engagement, should include two agreements: 1. Security Assessment Agreement and 2. Non Disclosure Agreement

5.1.8 Team Composition

Consider efficiency and accountability and compose a team of domain experts, as per the scope of work. Security assessment can be achieved much better with specialized team members' than having one person doing everything. Different team members bring different set of skills together. Some team member may have skills to break into systems but may not know firewall/IDS security assessment. Quite often it is seen, people who are good into breaking into system are not quite good at putting test result in an appropriate format for report and also do not like taking notes of their work.

5.1.9 Commercial

Based on the type of engagement, scope, skill set requirements and complexity of the system, the commercials can be worked out. The type of calculation may vary for time and material/Fixed bid model.

5.1.10 Maintain confidentiality of client data - before start of Project

In preparation for the security assessment job, the assessor may require information from the client in order to carry out the tests, such as network infrastructure diagrams, IP addresses, location of client premises, contact information for people in the organization, existence and location of network access points, vendor of network and IT systems, among other types of information.

This information may be confidential, and it is the security assessor's duty to ensure that any such information handled throughout the project will be treated according to its classification within the client organization.

5.1.11 Access Point Identification

It is of paramount importance that the access points chosen for conducting a security assessment represent all the possible threats, threat agents and possible business risk. The choice of access points along with a good cross section sample of devices is imperative for correct determination of threat to the facility and Information Systems.

– 5.1.11.1 LAYERED NETWORK ARCHITECTURE DESIGN

5.2 PHASE – II: ASSESSMENT

5.2.1 Rules of Engagement

Establish clear rule of engagement based on the assessment scope. Covert the same in the scope of work agreement mutually agreed and signed by client and assessment team.

5.2.2 Time of Assessment and Availability of Staff

5.2.3 A mechanism for dealing with false positive to avoid calling law enforcement unnecessarily

5.2.4 Obtain IP Addresses or ranges that needs to be assessed

5.2.5 Assessment Centre IP Addresses

5.3 PHASE – III: POST ASSESSMENT

After the assessment phase, the analysis and report submission activity starts. Various guidelines and good practices are suggested for various activities of this phase.

5.3.1 Reporting

5.3.1.1 PLANNING AND PREPARATION – Before starting the report writing process you should plan the activities for preparing and submitting the report. A great deal of effort is required to make a good report. It really doesn't matter how good assessment you did if you don't convey it to client in appropriate format. It's generally seen people who perform assessment doesn't like making report of assessment and it's good to assign document writing part someone who has skills and interest in it.

5.3.1.2 ANALYSIS – Analysis of test results shall be conducted on individual basis and with entire team (peer review). All the results should be shared with team members. Discuss should focus on vulnerabilities identified and verification of vulnerabilities based assessment conducted.

5.3.1.3 REPORT CREATION, MERGER AND FORMATTING – ISSAF recommends followings Structure for Report:

- Executive Summary.
- Vulnerability Summary Review.
- Action plan (all recommendations summarized into one table) with priorities assigned.
- Detailed Test Results with Countermeasures.

5.3.1.4 FINAL REVIEW BY THE LEAD – Before sending report to client a final review shall be done by project lead and quality assurance for the project.

5.3.1.5 CLOSING THE DOCUMENT AND SENDING IT TO CLIENT

- Ensure Document control and data classification are implemented in the document.
- An Executive summary and a letter to client lead can be added.

5.3.2 Presentation

5.3.2.1 PRESENTATION WITH (TECHNICAL TEAM AND FUNCTION MANAGER)

- Produce an initial summary of vulnerabilities to analysis team before presentation.

5.3.2.2 PRESENTATION WITH MANAGEMENT – Management presentation should carry the main summary of the assessment with supporting reasons of why, what, when, which, where and how. It should also include the key actions points. Presentation should include quantitative charts and tables of summarized information. This information matches the executive summary section of the report.

5.3.3 After Presentation

- 5.3.3.1.1 ACCEPTANCE CRITERIA IS MET – Ensure that the acceptance criteria are met. Refer Appendix for sample template. This template will contain all the test cases required to perform as per ISSAF.
- 5.3.3.1.2 ENSURE RECOMMENDATIONS ARE BEEN ADDRESSED – Ensure recommendations are been addressed. Follow-up for reasonable assurance that recommendations to plug the vulnerabilities is been addressed.
- 5.3.3.2 HELP CLIENT – Ensure client is not facing any problem to safeguard against vulnerabilities. Make sure you have answered all the questions regarding countermeasure to safeguard client organization. Ask client if he needs any other help before marking the assessment as closed since assessor may need to deploy his resources on some other projects.
- 5.3.3.3 MAINTAIN CONFIDENTIALITY OF CLIENT DATA – All information used before and during the project will normally be used in the reports generated to present the results of the security assessment. In order to maintain the confidentiality of this information, all reports and additional files (such as access log files, network traces and the like) must be kept and transmitted in a form that guarantees the confidentiality of the information, even in the event that storage media is misplaced or stolen.

6 RISK ASSESSMENT

6.1 BACKGROUND

In today's extremely competitive business environment, organizations are being increasingly forced to reduce costs and increase profitability, the Senior Management of organizations worldwide are laying a greater emphasis on the Return on Investments (ROI) and Cost v/s Business Benefit of every dollar spent. Information Technology being an integral part of today's business environment is also required to demonstrate cost benefit justifications and an acceptable level of ROI for all IT spending. Information Systems Security is one IT investment that is constantly under the magnifying glass of the Senior Management, given the fact that millions of dollars are being spent on security assessments and implementations.

6.2 METHODOLOGY

The subject of risk assessment and actually how to carry out a risk assessment exercise can at first be confusing and mind-boggling. However, if some basic rules and the proper methodology are followed, a risk assessment exercise tend to be very fruitful and an interesting one for the business. This area of the framework provides you with practical procedures and tools to actually allow you to effectively run your own risk assessment exercise.

- Establish the Context (Objectives; Stakeholders; Assets).
- Identify (Threats – What can Happen?; Vulnerabilities – How can threats affect us?).
- Analyse and Evaluate (The “analyse and evaluate” activity of the risk assessment methodology consists mainly of communicating, discussing and agreeing upon the ratings with the concerned stakeholders regarding the value that needs to be assigned to: Asset Value; Threats; Vulnerabilities).
- Action (The actions or mitigating factors which are identified in this part of the methodology is greatly depended on the participants' knowledge and expertise. Subject matter experts can also be required to assist in this process; Additionally, the action plan serves as a road map for further monitoring and review of risks whilst performing periodic risk assessment exercise.).

6.3 RISK ASSESSMENT TOOL

As a supplement to ISSAF, a basic spreadsheet-based tool has been developed to assist risk assessors in identifying and rating their asset values, threats and vulnerabilities.

6.4 RISK ASSESSMENT METHODOLOGY EVALUATION

More than often, IS Security experts would be called upon to evaluate the security implementations in a company where risk assessment exercises were already carried out either using internal resources or by hiring external resources. Alternatively, he/she might be called upon to follow up on the action plan following the risk assessment exercise. This section depicts some of the things to look at while evaluating whether the client company has properly undergone a risk assessment exercise.

7 ENTERPRISE INFORMATION SECURITY POLICY

7.1 INTRODUCTION

Enterprise Information security policy demonstrates executive management commitment and direction for implementation and management of information security within the enterprise. Security policy also demonstrates adherence to the concept of due diligence and due care.

7.2 PRE-REQUISITE

1. Documented and formalized enterprise security policy and a formal policy on updates through scheduled reviews and a process for meeting any unscheduled changes.
2. Any audit/review reports of enterprise security policy conducted either internally or externally. If a copy of policy can't be obtained, request for areas covered in policy/table of contents of policy.

7.3 OBJECTIVE

To establish whether the enterprise has formalized, implemented and communicated security policies with enterprise-wide applicability and supported by appropriate standards, procedures and guidelines within the enterprise.

7.4 ASSESSMENT QUESTIONNAIRE

This section contains a set of suggested evaluation check list that are expected to broadly fit the ISSAF based assessment process. Recognizing that each organization has its own unique processes, technologies and information processing architecture, it is possible that the ISSAF evaluation may need further steps to be performed.

7.5 ASSESSMENT QUESTIONNAIRE - NARRATIVE

The following narrative supports the understanding of the contents and logic that is embedded in the assessment questionnaire. While the questionnaire is structured on the basis of possible process flow that may be found in many enterprises, the narrative is presented to aid an understanding of the concepts covered in this domain.

7.5.1 Overview

Information security policies support to implement effective security in an enterprise. Security policies are a statements that are derived from an alignment of information security to the business requirements, as endorsed by executive management of the enterprise. As it is emerging today, security policies are used as vehicles that communicate executive management commitment to securing information assets. In addition, these policies provide an overview of the security stance of an organization and credibility to security activities.

7.5.2 Policy and Trust

Information Security policies, like every other enterprise policy, involves people. Policies are designed and implemented so that the actions and interactions of people among themselves and with the constituents of Information Processing Facilities, Trusted Computing Base, etc. are consistent with the enterprise security stance. The moment we talk of interaction amongst humans, it involves trust related issues.

7.5.3 *Some issues of design*

Policies affect the way people work. It is therefore a good practice to work on a consensus-based policy development and implementation wherever possible. While it is not always possible to get a consensus on all policy issues due to a number of factors, it would be worthwhile to get all those who would be affected by the implementation of the policy to review the policy and share their views as to how the proposed policy could impact their work – in terms of productivity, personal efficiencies, adherence to best practices, impact of changes from what is currently happening, etc. At the stage of eliciting this consensus, if it is demonstrated that the implementation of a policy would result in an unfavorable situation, it may be worthwhile re-visiting the policy.

7.5.4 *Security Policy Development Model for Security Policies*

The Risk Assessment Methodology, the classification levels & the security services needed for securing the information systems are good guiding principles to establish a security policy for the entire organization. The Legal department should also ascertain that the statements within the policy are in compliance with the Local Regulations & other privacy laws. The policy should have disciplinary statements that mention the punishment meted out in case there is non-compliance to the policies. The policies could be high-level statements that could talk about the management's intention to treat information security within the firm on priority and it may also be detailed in terms of outlining various controls & strategies the firm may use to secure the information.

7.5.5 *The Policy must address:*

7.5.5.1 MANAGEMENT STATEMENT ON INFORMATION SECURITY – This statement shall include the management's commitment & support to information security within the organization. This will also encourage other business units to participate in the information security program for the firm.

7.5.5.2 DISCIPLINARY STATEMENT – The policy must include a statement, which should talk about the disciplinary process which shall be taken in case there is a non-compliance with the policies mentioned below. Disciplinary measures can be up to termination of employment.

7.5.5.3 THE SECURITY ORGANIZATION & THE ROLES AND RESPONSIBILITIES – This section should include the various roles in the information security program. This should include at minimum the role of the Information Security Officer, the information owners, the end users, the systems administrator & the end users.

7.5.6 *For the End-Users*

7.5.6.1 ACCEPTABLE USE OF COMPUTER SYSTEMS & RESOURCES – This policy talks about how information systems are important to the organization and it also talks about prudent usage of computer systems by the employees. Most organizations have a policy mentioning that all data stored on the organizations computer systems belongs to the organization & that the employee activity may be monitored.

7.5.6.2 E-MAIL USAGE POLICY – This policy talks about prudent usage of e-mail resources. This means that the employees can use the e-mail system for personal purposes as long as there isn't significant usage of the organization bandwidth.

7.5.6.3 INTERNET USAGE – Internet usage is mostly granted to employees requiring access for business purposes. Employees are also advised against posting any comments on websites with the company e-mail id unless authorized to do so.

7.5.6.4 ENCRYPTION OF SENSITIVE DATA – Employees should be advised to encrypt sensitive information before sending it on the Internet using the firms approved products. They should also confirm the identity of senders and ensure that it is from an authentic source before using information sent to the users.

7.5.6.5 ANTI-VIRUS POLICY – The anti-virus policy should advise users about scanning attachments before getting them from external sources. They should also

report virus incidents to the concerned people that could help in containing the viruses/worms before they start spreading to other systems.

7.5.6.6 **PASSWORD PROTECTION POLICY** – Password protection policy talks about the selection of passwords & password complexity and other parameters like password change frequency; history.

7.5.6.7 **REMOTE ACCESS POLICY** – The remote access policy asks users to ensure that all controls like personal firewalls etc are running well before they connect to the firms systems. This should also create awareness among users about the possible installation of key loggers and other Trojans while connecting to the firms systems from the internet or other untrusted networks.

7.5.6.8 **INCIDENT REPORTING POLICY** – This policy should educate the users on possible security breaches and the way these incidents to be reported to the concerned authorities.

7.5.7 For the Information Owners

7.5.7.1 **RISK ASSESSMENT & ASSET CLASSIFICATION** – The information owners should be entrusted with the Risk assessment & classification of the information systems in their purview. They along with the representatives form the information security department must classify & label the data by analyzing the threats. In case of shared systems across multiple business units the business managers must co-own the data & all of them must be involved in the risk assessment exercise. Information owners must be entrusted with the responsibility of completing the Risk assessment exercise and the information security representatives must act as consultants in facilitating this process.

7.5.7.2 **OUTSOURCED SERVICE PROVIDERS ENGAGEMENT POLICY** – The information owners must notify the information security department about possible engagements with outsourced service providers before establishing a relationship. The information security department should analyze if the service providers meet the minimum criteria required so that the organizations data can be entrusted to the service provider's Service Level Agreements (SLA) Needs to be defined for the Outsourced agency.

7.5.7.3 **BUSINESS CONTINUITY & DISASTER RECOVERY POLICY** – The information owners must be advised to make continuity plans in case of exigencies. The BCP team or the Information Security team would facilitate this process. This also requires the information owners to maintain the required call trees and establish DR processes for the businesses information systems.

7.5.8 For the IT Department

7.5.8.1 **PHYSICAL SECURITY OF INFORMATION SYSTEMS** – This policy must advise the IT Department or other departments (Administration) to deploy all possible security controls to protect the information systems from damage, loss & theft. This may require deploying & operating some controls like a PACS (Personal Access Control System). This should also talk about equipment sitting & procedures to be followed when physical access is required (like maintaining a log of all access to the server systems). This should also address procedure for operating environmental controls

7.5.8.2 **NETWORK & SYSTEMS SECURITY POLICY** – This should discuss the security mechanisms to be implemented on Network & Server systems. The main criteria for configuration of systems should be that access should be granted to resources as required.

7.5.8.3 **WIRELESS SECURITY** – This is an area which is a matter of grave concern. The wireless systems should be properly configured with adequate authorization & authentication methods.

- 7.5.8.4 APPLICATION DEVELOPMENT & DEPLOYMENT – The application development & deployment policy should talk about how security should be a consideration at the time of application development itself. The policy should also discuss means in which the application must first be unit tested, then tested on an integration environment and only after it passes the security tests should it be deployed on the production systems.
- 7.5.8.5 INTERNET & THIRD PARTY CONNECTIVITY – This policy should talk about secure connectivity to the internet & third parties. The organizations acceptable method for external connectivity & the authorization process for the same should be discussed. Some organizations conduct a penetration test on the third party networks before allowing connectivity into their systems.
- 7.5.8.6 VENDOR ENGAGEMENT POLICY – The vendor engagement policy would discuss what minimum security criteria a vendor must adhere to before the organization can establish a relationship. E.g includes a vendor should have a proper background check of all its employees before the vendor representatives work with the organization.
- 7.5.8.7 BACKUP & SYSTEMS AVAILABILITY POLICY – This policy entrusts the proper functioning of the network infrastructure & backup of information systems to the IT Department.

7.5.9 For the Information Security

- 7.5.9.1 MONITORING & REVIEW OF SYSTEM SECURITY EVENTS – The information security team should be advised to check the security events on a regular basis and report breaches or incidents serious in nature to the management. The information security team should regularly monitor for any non-compliance to the security policy as well & work with the business units to have those rectified.
- 7.5.9.2 SYSTEMS VULNERABILITY ASSESSMENT & PENETRATION TESTING – The information security department is often entrusted with the responsibility of conducting vulnerability assessment & penetration tests. This policy talks about how these must be carried out with proper authorization.
- 7.5.9.2.1 THIRD PARTY (VENDOR & OUTSOURCED SERVICE PROVIDERS) ENGAGEMENT REVIEW – The information security team may be required to go onsite & conduct reviews of the Services providers & vendors to ensure that they comply to the minimum security criteria as required by the organizations. This policy details the information security roles in the process.
- 7.5.9.2.2 INCIDENT RESPONSE – The incident response policy details the method of investigating any reported security breaches. How & when law enforcement agencies must be contacted & who should be responsible for communicating with the media should be covered.
- 7.5.9.2.3 BUSINESS CONTINUITY PLANNING – The information security department should also be facilitating the BCP for various business units & should review test results & appraise the management about the same.
- 7.5.9.2.4 SECURITY AWARENESS & TRAINING – This is an often-overlooked subject; the information security department must be responsible for training all users in the organizations. They must also design & constantly update their security awareness programs.

8 ENTERPRISE INFORMATION SECURITY ORGANIZATION & MANAGEMENT

8.1 INTRODUCTION

Information security organization is an important part of the management control structure in an organization. Assessment of the organization structure and management responsibilities are important since these determine if the organization can be aligned to the security stance of executive management. This also stems from the belief that security cannot be achieved only by technology or services and it needs to be ingrained into the overall organizational

functioning. One sure way of examining if executive management has taken cognizance of the need for a comprehensive security stance is to assess the security organization.

8.2 PRE-REQUISITE

Organizational structure of entire organization, IT department, enterprise security organization, internal audit. Document containing formally approved roles and responsibilities, job description for enterprise security functions, any third party assessment/review etc...

8.3 OBJECTIVE

The primary objective of this assessment is to assess the formal organizational controls that are related to organizational structure. Also, to evaluate management support to the security functions, identify segregation of duties, third party security and to address outsourcing security concerns.

8.4 ASSESSMENT QUESTIONNAIRE

This section contains a set of suggested evaluation check list that are expected to broadly fit the ISSAF based assessment process. Recognizing that each organization has its own unique processes, technologies and information processing architecture, it is possible that the ISSAF evaluation may need further steps to be performed.

8.5 ASSESSMENT QUESTIONNAIRE - NARRATIVE

The following narrative supports the understanding of the contents and logic that is embedded in the assessment questionnaire. While the questionnaire is structured on the basis of possible process flow that may be found in many enterprises, the narrative is presented to aid an understanding of the concepts covered in this domain.

8.5.1 Introduction

The security organization plays a vital role in the effective implementation of policies & in maintaining the overall security posture of a company. Most companies generally consider information security as information technology security. The scope of information security is much more broader than just IT security since information in an organizational context extends beyond data processing and computers and therefore involves a lot of interaction with other business departments.

8.5.2 Segregation of Duties;

Segregation of duties is a very important administrative control in information security. This is achieved by ensuring that no complete operation cycles are completed by a single individual or no operation cycles that have significant security content is completed by a single individual.

8.5.3 Two-person Controls

Another form of administrative control that harnesses the organization structure is two-person controls. In this situation, the rationale is similar to that which justifies segregation of duties.

8.5.4 Peer Review

Unlike a supervisory review which comes with its share of psychological and behavioral issues, the concept of peer review of security operations have come to be accepted amongst security professionals as a good organizational control mechanism. In this process, the work of one person is reviewed by his/her peer.

8.5.5 Mandatory Vacations

This form of administrative control has been recommended for quite some time now has yielded good results in organizations that had implemented it. This control stems from the belief that anyone involved in a security infraction would be able to hide it from the belief that anyone involved in a security infraction would be able to hide it successfully so long

as he/she is able to be present at the place of security violation and can continue to cover up the violation.

8.5.6 Information Security Roles and Responsibilities

The effectiveness of any Information Security Management framework is dependent on the personnel who administer the security implementation. This would depend on how effectively the enterprise assigns and manages the roles and responsibilities for the implementation and management of Information Security.

8.5.6.1 CHIEF INFORMATION SECURITY OFFICER – The Chief Information Security Officer (CISO) is the senior most position in a security management organization within an enterprise.

8.5.6.2 PHYSICAL SECURITY MANAGER – The Physical Security Manager's role is responsible for the management the security of the physical facilities related to Information Technology implemented within an organization.

8.5.6.3 INFRASTRUCTURE SECURITY MANAGER – The Infrastructure Security Manager's role is responsible for the management of security of specific infrastructure components of the IS infrastructure of the enterprise.

8.5.6.4 NETWORK SECURITY MANAGER – The Network Security Manager's role is responsible for the management of security of specific network and telecommunication components of the IS infrastructure of the enterprise.

8.5.6.5 APPLICATIONS & DATABASE SECURITY MANAGER – The Application and Database Security Manager's role is responsible for the implementation and management of application security and logical security of both applications and databases of the Information Systems used within the Enterprise.

8.5.6.6 SECURITY COMPLIANCE MANAGER – The Security Compliance Manager's role is responsible for ensuring the compliance to the Information Security Policies, Procedures and associated Standards, Guidelines and MBS by all personnel of the enterprise.

9 ENTERPRISE INFORMATION SECURITY ORGANIZATION & MANAGEMENT

9.1 PERSONNEL SECURITY

People are greatest assets of any enterprise and require specific attention to recruitment, promotion, personnel clearance, training, performance evaluation and job change termination.

The objective is to assess:

- That security responsibilities are addressed at recruitment stage and in contracts and monitored during recruitment.
- That potential recruits are appropriately screened.
- That all employees and third party users of information processing facilities sign a confidentiality agreement

B

Modelo do Questionário

Os questionários foram definidos para três tipos distintos de pessoas, atendendo essencialmente à especificidade das actividades desenvolvidas na instituição. Foram assim definidos os seguintes tipos: Docentes, Não Docentes e Técnicos de Informática.

O questionário dos Docentes foi estabelecido tendo em em atenção a identificação de cada Escola. Os questionários dos Não Docentes e Técnicos de Informática foram estabelecidos atendendo à globalidade do IPS (Serviços Centrais, Centro, Serviço, Escola, etc.)

Cada um dos questionários é constituído por 5 grupos de questões. O grupo A destina-se a caracterizar o(a) inquirido(a), o grupo B pretende obter uma caracterização da utilização do computador pessoal, enquanto que os grupos C, D e E se destinam a obter a percepção do(a) inquirido(a) acerca da utilização e da segurança da informação do Sistema Informático do Serviço/Escola.

Sempre que necessário, com o objectivo de proporcionar um enquadramento adequado ao grupo de questões, entendeu-se como pertinente apresentar as definições de termos menos comuns no início de cada grupo.

Questionário – Docentes

INSTRUÇÕES DE PREENCHIMENTO

Face ao seu processo de tratamento (leitura óptica), este QUESTIONÁRIO deve ser preenchido utilizando caneta ou esferográfica preta ou azul e preenchido como mostra o exemplo.

Preencha

assim ☒
assim não ☒
se rasurado ☒

QUESTIONÁRIO - SEGURANÇA DA INFORMAÇÃO

Caro(a) Colega,

Este questionário é constituído por 5 grupos de questões. O grupo A destina-se a caracterizar o(a) inquirido(a), o grupo B pretende obter uma caracterização da utilização do computador pessoal, enquanto que os grupos C, D e E se destinam a obter a percepção do(a) inquirido(a) acerca da utilização e da Segurança da Informação do Sistema Informático da Escola.

De forma a garantir a privacidade dos(as) inquiridos(as) e o seu anonimato, agradeço que em nenhuma parte do questionário coloque qualquer nome ou número que possibilite a sua identificação.

A - Identificação/Caracterização do(a) inquirido(a)

- A1) Escalão etário ☐ Menos de 30 anos ☐ Entre 30 anos e 45 anos ☐ Mais de 45 anos
- A2) Área de residência ☐ Concelho de Setúbal ☐ Fora do Concelho de Setúbal
- A3) Antiguidade na Escola ☐ Até 5 anos ☐ Mais de 5 anos
- A4) Experiência profissional docente ☐ Menos de 2 anos ☐ Entre 2 anos e 5 anos ☐ Mais de 5 anos
- A5) Habilitações Académicas ☐ Doutoramento ☐ Mestrado ☐ Licenciatura
- A6) Área científica de docência ☐ Informática; Engenharia Informática; Computadores; Sistemas de Informação; etc.
☐ Outra
- A7) Identificação da Escola ☐ ESE ☐ ESTSetúbal ☐ ESCE ☐ ESS ☐ ESTBarreiro
- A8) Categoria profissional ☐ Professor ☐ Equiparado a Professor ☐ Assistente ☐ Equiparado a Assistente
- A9) Regime do contrato ☐ Dedicção exclusiva ☐ Tempo integral ☐ Tempo parcial ☐ Outro

B - Computador pessoal

Nos casos em que dispõe de mais do que um computador pessoal na sua residência, deve responder tendo em consideração aquele que utiliza com maior frequência.

- B1) A quantos computadores possui acesso na sua residência?
☐ Nenhum ☐ 1 ☐ 2 ☐ 3 ou mais Se respondeu NENHUM, passe para o grupo C.
- B2) O computador pessoal a que acede é um portátil?
☐ Não ☐ Sim
- B3) Acede à Internet com o seu computador pessoal?
☐ Não ☐ Sim Se respondeu NÃO, passe para a questão B10).
- B4) Especifique em que locais acede à Internet com o seu computador pessoal? (assinale todos os itens aplicáveis)
☐ Residência ☐ Residência de colegas/amigos(as)
☐ Escola ☐ Cafés/Restaurantes/etc.
☐ Outra Instituição de Ensino Superior ☐ Outros locais
- B5) Com quantas pessoas partilha a utilização do computador pessoal na sua residência?
☐ Nenhuma ☐ 1 ☐ 2 ☐ 3 ou mais
- B6) Com que frequência acede à Internet com o seu computador pessoal?
☐ Todos os dias ☐ Pelo menos uma vez por mês
☐ Quase todos os dias ☐ Uma ou duas vezes por semestre
☐ Pelo menos uma vez por semana
- B7) Durante esses acessos à Internet, qual o tempo médio diário de utilização?
☐ Até 1 hora ☐ Entre 1 e 3 horas ☐ Mais de 3 horas
- B8) Classifique a segurança do seu acesso? (6 para muito seguro e 1 para pouco seguro)

1

2

3

4

5

6

☐

☐

☐

☐

☐

☐
- B9) Identifique a solução que adoptou para acesso à Internet com o seu computador pessoal.
☐ Modem ☐ ADSL ☐ Cabo ☐ Wireless ☐ Outra
- B10) Possui password para acesso ao seu computador pessoal?
☐ Não ☐ Sim Se respondeu NÃO, passe para a questão B18).

53418



B11) Com quantas pessoas partilha a sua password?

- ☐ Nenhuma ☐ 1 ☐ 2 ou 3 ☐ Mais de 3

B12) Já alterou a password de acesso ao seu computador pessoal?

- ☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão B16).

B13) Com que frequência altera a password de acesso ao seu computador pessoal?

- ☐ Uma única vez ☐ Semestralmente/Anualmente
☐ Raramente ☐ Mensalmente/Trimestralmente

B14) Que opções efectua na escolha da sua nova password? (assinale todos os itens aplicáveis)

- ☐ Datas de nascimento/aniversário ☐ Apenas números
☐ Nomes de familiares ☐ Apenas letras
☐ Nomes de locais ☐ Combinação de números e letras
☐ Nomes de animais de estimação ☐ Escolha aleatória de caracteres

B15) Na definição de nova password opta por:

- ☐ Número máximo de caracteres permitido
☐ Número fixo de caracteres, entre máximo e mínimo
☐ Número aleatório de caracteres, entre máximo e mínimo
☐ Número mínimo de caracteres permitido

B16) Classifique o grau de segurança da sua password. (6 para elevado e 1 para baixo)

- 1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

B17) Qual o processo que utiliza para guardar a sua password? (assinale todos os itens aplicáveis)

- ☐ Memorização ☐ Memória do telemóvel ☐ Post-it ☐ Registo na agenda pessoal ☐ Outro

B18) Além da password que mecanismo/ferramenta/software utiliza para protecção do seu computador pessoal? (assinale todos os itens aplicáveis)

- ☐ Nenhum
☐ Firewall (software/hardware para controlo do tráfego da rede informática, etc.)
☐ Antivírus (software destinado à detecção de vírus, entendidos em termos genéricos, e à sua eliminação)
☐ Antispyware (software destinado à detecção de programas intrusivos)
☐ Outros

B19) Com que frequência actualiza esse mecanismo/ferramenta/software? (assinale todos os itens aplicáveis)

- ☐ Sempre que existe uma actualização ☐ Sempre que possível
☐ Mensalmente/Trimestralmente ☐ Nunca actualiza
☐ Semestralmente/Anualmente

B20) Efectua cópias de segurança (backups) da informação contida no seu computador pessoal?

- ☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão B25).

B21) Com que periodicidade efectua cópias de segurança (backups)? (assinale todos os itens aplicáveis)

- ☐ No final de cada sessão de trabalho ☐ Mensalmente
☐ Na conclusão de cada projecto/trabalho/etc. ☐ Trimestralmente
☐ Diariamente ☐ Raramente
☐ Semanalmente

B22) Especifique a opção mais frequente para realização das cópias de segurança (backups)?

- ☐ Apenas os ficheiros alterados ☐ Um conjunto de ficheiros pré-definidos
☐ A totalidade da informação no disco ☐ Apenas os ficheiros considerados importantes

B23) Que tipo de dispositivo utiliza para efectuar as cópias de segurança (backups)? (assinale todos os itens aplicáveis)

- ☐ Disco do computador ☐ Memória flash amovível
☐ Disco externo ☐ Disquete
☐ CD/DVD ☐ Tape

B24) Especifique onde guarda as cópias de segurança (backups) que efectua.

- ☐ Na mesma sala onde se encontra o computador ☐ Fora da sua residência
☐ Em outro espaço da sua residência

B25) Classifique o grau de segurança do seu computador pessoal. (6 para elevado e 1 para baixo)

- 1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

B26) Com que frequência utiliza o seu computador pessoal?

- ☐ Todos os dias ☐ Pelo menos uma vez por mês
☐ Quase todos os dias ☐ Uma ou duas vezes por semestre
☐ Pelo menos uma vez por semana

53418



B27) Caracterize como utiliza o seu computador pessoal. (assinale todos os itens aplicáveis)

☐ Elaboração de relatórios e outros trabalhos	☐ Jogos
☐ Impressão de documentos	☐ Pesquisas na Internet
☐ Trabalhos escolares	☐ Envio/recepção de correio electrónico

B28) Durante a utilização do seu computador pessoal, qual o tempo médio diário de utilização?

- ☐ Até 1 hora ☐ Entre 1 e 3 horas ☐ Mais de 3 horas

B29) Que tipo de software utiliza no seu computador pessoal? (assinale todos os itens aplicáveis)

☐ Sistema Operativo Windows	☐ Folha de Cálculo (por ex. Excel)
☐ Sistema Operativo Macintosh	☐ Base de Dados (por ex. Access)
☐ Sistema Operativo Linux	☐ Apresentações (por ex. PowerPoint)
☐ Outro Sistema Operativo	☐ Outros aplicativos
☐ Processador de Texto (por ex. Word)	

C - Sistema Informático da Escola

Por **Sistema Informático da Escola** entendem-se todos os recursos de computador (computadores, impressoras, scanners, etc.), disponibilizados para realização de trabalhos, pesquisa e comunicação, incluindo procedimentos e regras de acesso e utilização das aplicações disponibilizadas.

C1) Desde a sua entrada na Escola existiu alguma mudança no Sistema Informático (Hardware, Software, Procedimentos, etc.)?

- ☐ Não ☐ Não sabe ☐ Sim Se respondeu **NÃO** ou **NÃO SABE**, passe para a questão C7).

C2) Foi solicitada a sua participação/participou de alguma forma nessas mudanças?

- ☐ Não ☐ Sim Se respondeu **NÃO**, passe para a questão C5).

C3) Caracterize a sua participação nessas mudanças. (assinale todos os itens aplicáveis)

☐ Aquisição de Software/Hardware	☐ Análise de documentos
☐ Instalação/Configuração de Hardware	☐ Preenchimento de inquéritos/questionários
☐ Instalação/Configuração de Software	☐ Resposta a entrevistas
☐ Definição/Implementação de Procedimentos	☐ Elaboração de pareceres

C4) Classifique o seu grau de participação nessas mudanças. (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C5) Classifique o seu grau de satisfação com as mudanças efectuadas. (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C6) Classifique a sua percepção acerca do funcionamento do Sistema Informático depois das mudanças efectuadas. (6 para melhorou muito e 1 para não melhorou)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C7) Classifique o seu grau de conhecimentos na área da Informática/Sistemas de Informação. (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C8) Dispõe de acesso ao Sistema Informático da Escola?

- ☐ Não ☐ Sim Se respondeu **NÃO**, continue aqui o preenchimento do questionário.

C9) O acesso ao Sistema Informático da Escola é feito através de password?

- ☐ Não ☐ Sim Se respondeu **NÃO**, passe para a questão C18).

C10) Já alterou a(s) sua(s) password(s) de acesso ao Sistema Informático da Escola?

- ☐ Não ☐ Sim Se respondeu **NÃO**, passe para a questão C14).

C11) Com que frequência altera a(s) sua(s) password(s) de acesso ao Sistema Informático da Escola?

☐ Uma única vez	☐ Semestralmente/Anualmente
☐ Raramente	☐ Mensalmente/Trimestralmente

C12) Que opções efectua na escolha de nova(s) password(s)? (assinale todos os itens aplicáveis)

☐ Datas de nascimento/aniversário	☐ Apenas números
☐ Nomes de familiares	☐ Apenas letras
☐ Nomes de locais	☐ Combinação de números e letras
☐ Nomes de animais de estimação	☐ Escolha aleatória de caracteres

C13) Na definição de nova password opta por:

- ☐ Número máximo de caracteres permitido
- ☐ Número fixo de caracteres, entre máximo e mínimo
- ☐ Número aleatório de caracteres, entre máximo e mínimo
- ☐ Número mínimo de caracteres permitido

C14) Qual o processo que utiliza para guardar a(s) sua(s) password(s)? (assinale todos os itens aplicáveis)

- ☐ Memorização ☐ Memória do telemóvel ☐ Post-it ☐ Registo na agenda pessoal ☐ Outro

53418



C15) Com quantas pessoas partilha a(s) sua(s) password(s) de acesso ao Sistema Informático da Escola?

☐ Nenhuma ☐ 1 ☐ 2 ou 3 ☐ Mais de 3

C16) Utiliza a mesma password para diversas aplicações/sistemas?

☐ Não ☐ Sim

C17) Classifique o grau de segurança da(s) sua(s) password(s). (6 para elevado e 1 para baixo)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

C18) Além da password, especifique que tipo(s) de mecanismo(s) está(ão) implementado(s) para acesso ao Sistema Informático da Escola. (assinale todos os itens aplicáveis)

☐ Cartão magnético ☐ Controlo biométrico
☐ Cartão com microchip ☐ Identificação pessoal
☐ Chave metálica ☐ Nenhum

C19) Possui algum endereço de correio electrónico associado ao Sistema Informático da Escola?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C23).

C20) Além desse, quantos endereços de correio electrónico possui?

☐ Nenhum ☐ 1 ☐ 2 ☐ 3 ☐ Mais de 3

C21) Utiliza a mesma password para acesso ao correio electrónico e ao Sistema Informático da Escola?

☐ Não ☐ Sim

C22) Existe implementado algum sistema de filtragem de mensagens de correio electrónico?

☐ Não ☐ Não sabe ☐ Sim

C23) Com que frequência acede ao Sistema Informático da Escola?

☐ Todos os dias ☐ Pelo menos uma vez por mês
☐ Quase todos os dias ☐ Uma ou duas vezes por semestre
☐ Pelo menos uma vez por semana

C24) Durante a utilização do Sistema Informático da Escola, qual o tempo médio diário de cada utilização?

☐ Até 1 hora ☐ Entre 1 e 3 horas ☐ Entre 3 e 5 horas ☐ Mais de 5 horas

C25) Que tipo de software utiliza? (assinale todos os itens aplicáveis)

☐ Sistema Operativo Windows 95/98/2000/XP ☐ Base de Dados
☐ Sistema Operativo Windows Server ☐ Programação
☐ Sistema Operativo Linux ☐ Apresentações
☐ Sistema Operativo Macintosh ☐ Desenho técnico
☐ Outro Sistema Operativo ☐ Análise de Sistemas
☐ Processador de Texto ☐ Gestão/Contabilidade/Marketing
☐ Folha de Cálculo ☐ Outros aplicativos

C26) Caracterize a sua utilização do Sistema Informático da Escola. (assinale todos os itens aplicáveis)

☐ Elaboração de relatórios ☐ Registo/Introdução de dados
☐ Elaboração de outros trabalhos ☐ Análise estatística/projecções
☐ Impressão de documentos ☐ Pesquisas na Internet
☐ Leccionação ☐ Envio/recepção de correio electrónico

C27) Utiliza alguma área de trabalho privada no(s) servidor(es) do Sistema Informático da Escola?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C32).

C28) Que tipo de informação guarda nessa área de trabalho?

☐ Ficheiros de trabalho ☐ Ficheiros pessoais ☐ Ambos

C29) Já perdeu informação guardada nessa área de trabalho?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C32).

C30) Que acção tomou para recuperar essa informação?

☐ Expôs a situação aos serviços de informática ☐ Tentou recuperar a informação ☐ Nenhuma

C31) O que aconteceu relativamente a essa situação? (assinale todos os itens aplicáveis)

☐ A informação foi reposta de backups anteriores
☐ A informação foi recuperada mas não sabe como
☐ A informação não foi recuperada
☐ Recebeu comunicação de que era impossível recuperar a informação
☐ Não sabe nada acerca da situação

C32) Possui acesso à impressão de documentos através do Sistema Informático da Escola utilizando impressora(s) partilhada(s)?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C36).

53418



C33) Quando não consegue imprimir documentos através da(s) impressora(s) partilhada(s) qual a atitude que assume?
(assinale todos os itens aplicáveis)

☐ Cancela de imediato o trabalho	☐ Tenta imprimir numa impressora disponível
☐ Tenta imprimir novamente	☐ Tenta imprimir mais tarde
☐ Verifica se a impressora tem algum problema	☐ Informa os serviços de informática
☐ Altera a configuração de acesso à impressora	☐ Nenhuma

C34) Que atitude toma quando encontra documentos que não são seus na(s) impressora(s) partilhada(s)?(assinale todos os itens aplicáveis)

☐ Nunca encontrou	☐ Deita fora ou destrói o documento
☐ Lê o documento (todo ou parte)	☐ Guarda para seu uso pessoal
☐ Entrega aos serviços de informática	☐ Deixa junto à impressora
☐ Tenta entregar/entregou ao(à) seu(sua) proprietário(a)	☐ Nenhuma

C35) Que atitude toma quando não encontra documentos seus que mandou imprimir na(s) impressora(s) partilhada(s)?
(assinale todos os itens aplicáveis)

☐ Nunca aconteceu	☐ Imprime novamente o documento
☐ Verifica se ainda aguarda por impressão	☐ Tenta encontrar o documento
☐ Informa os serviços de informática	☐ Nenhuma

C36) Consideraria a hipótese de aceder ao Sistema Informático da Escola a partir da sua residência ou de outro local onde trabalhe regularmente?

- ☐ Não ☐ Sim ☐ Talvez

D - Segurança da Informação no Sistema Informático da Escola

Por **Segurança da Informação** em sistemas informáticos entende-se: preservação da **confidencialidade** (assegurar que a informação apenas é acedida por quem está autorizado a fazê-lo), da **integridade** (garantir a exactidão e a credibilidade da informação) e da **disponibilidade** (assegurar que as pessoas autorizadas têm acesso à informação e aos activos associados sempre que necessário) da informação [BS ISO/IEC 17799:2005 Information Technology - Code of practice for information security management]

D1) Existem políticas (normas/regulamentos/regras/procedimentos) de segurança do Sistema Informático da Escola?

- ☐ Não ☐ Não sabe ☐ Sim Se respondeu NÃO ou NÃO SABE, passe para a questão D7).

D2) Como tomou conhecimento dessas políticas (normas/regulamentos/regras/procedimentos)?(assinale todos os itens aplicáveis)

☐ Documento entregue na Escola	☐ Consulta da página web da Escola
☐ Informação dos serviços de informática	☐ Colega de trabalho
☐ Informação afixada na Escola	☐ Outro meio

D3) Dos aspectos a seguir mencionados, especifique quais são abrangidos pelas políticas (normas/regulamentos/regras/procedimentos) definidas. (assinale todos os itens aplicáveis)

☐ Definição de acessos ao sistema (por ex. passwords)	☐ Utilização dos recursos de hardware
☐ Utilização do correio electrónico	☐ Acesso aos servidores
☐ Utilização da Internet	☐ Realização de cópias de segurança (backups)
☐ Detecção/Controlo de intrusões	☐ Instalação de software
☐ Controlo dos activos do sistema	☐ Plano de Recuperação de Acidentes

D4) Participou na elaboração/alteração dessas políticas (normas/regulamentos/regras/procedimentos)?

- ☐ Não ☐ Sim Se respondeu NÃO, passe para a questão D7).

D5) Caracterize a sua participação nessas actividades. (assinale todos os itens aplicáveis)

☐ Elaboração das políticas	☐ Preenchimento de inquéritos/questionários
☐ Implementação das políticas	☐ Resposta a entrevistas
☐ Análise de documentos	☐ Elaboração de pareceres

D6) Classifique o seu grau de participação nessas actividades. (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

D7) Caracterize a sua participação nas acções de sensibilização para a problemática da segurança da Informação?

☐ Não teve conhecimento de qualquer acção	☐ Não quis participar
☐ Não teve possibilidade de participar	☐ Participou com interesse
☐ Não foi convidado(a) a participar	☐ Participou sem interesse

D8) Já presenciou alguma(s) violação(ões) da segurança do Sistema Informático da Escola (por exemplo destruição/roubo de equipamentos, entradas em locais interditos, utilização de ficheiros/passwords de outras pessoas, etc.)?

- ☐ Não ☐ Sim Se respondeu NÃO, passe para a questão D10).

D9) Que atitude tomou quando presenciou essa(s) violação(ões)? (assinale todos os itens aplicáveis)

☐ Advertiu o(a) infractor(a)	☐ Propôs medidas para resolução do problema
☐ Informou a Direcção da Escola	☐ Comentou com os(as) seus(suas) colegas
☐ Informou os serviços de informática	☐ Nenhuma

53418



D10) Após o login no acesso ao Sistema Informático da Escola, existe definido algum tempo limite para que a sessão de trabalho esteja activa?

☐ Não ☐ Não sabe ☐ Sim

D11) Durante o tempo em que tem activa a sua sessão de trabalho, utiliza algum mecanismo de protecção de ecrã para quando não está a utilizar o computador?

☐ Não ☐ Sim

D12) Classifique a segurança do Sistema Informático da Escola.
(6 para muito seguro e 1 para pouco seguro)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

D13) Classifique, relativamente à segurança do Sistema Informático da Escola (6 para muito importante e 1 para pouco importante), os seguintes aspectos:

	1	2	3	4	5	6
(a) Utilizadores	☐	☐	☐	☐	☐	☐
(b) Técnicos de informática	☐	☐	☐	☐	☐	☐
(c) Leis/Políticas/Regulamentos/Procedimentos	☐	☐	☐	☐	☐	☐
(d) Computadores Pessoais (Hardware)	☐	☐	☐	☐	☐	☐
(e) Periféricos (Impressoras, Scanners, etc.)	☐	☐	☐	☐	☐	☐
(f) Servidores (Hardware)	☐	☐	☐	☐	☐	☐
(g) Software aplicacional	☐	☐	☐	☐	☐	☐
(h) Sistemas Operativos	☐	☐	☐	☐	☐	☐
(i) Internet	☐	☐	☐	☐	☐	☐
(j) Correio electrónico	☐	☐	☐	☐	☐	☐
(k) Rede informática	☐	☐	☐	☐	☐	☐
(l) Sistema de comunicações (telefones, telefaxes, etc.)	☐	☐	☐	☐	☐	☐

D14) Classifique em que medida considera que a segurança do Sistema Informático da Escola é ou pode ser importante para as suas actividades lectivas e de investigação. (6 para muito importante e 1 para pouco importante)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

D15) Classifique a facilidade de acesso físico ao Sistema Informático da Escola (6 para muito difícil e 1 para muito fácil), nos seguintes pontos de acesso:

	1	2	3	4	5	6
(a) Sala de servidores	☐	☐	☐	☐	☐	☐
(b) Serviços de Informática	☐	☐	☐	☐	☐	☐
(c) Serviços administrativos/académicos/etc.	☐	☐	☐	☐	☐	☐
(d) Gabinetes de colegas	☐	☐	☐	☐	☐	☐
(e) Salas de reunião	☐	☐	☐	☐	☐	☐
(f) Átrios/corredores	☐	☐	☐	☐	☐	☐
(g) Área circundante da Escola	☐	☐	☐	☐	☐	☐
(h) Salas de aula	☐	☐	☐	☐	☐	☐
(i) Laboratórios de Informática	☐	☐	☐	☐	☐	☐
(j) Salas de informática para alunos	☐	☐	☐	☐	☐	☐

D16) Nos locais onde tem acesso ao Sistema Informático da Escola, especifique que actividades estão proibidas.
(assinale todos os itens aplicáveis)

☐ Fumar	☐ Movimentar computadores instalados
☐ Ingerir bebidas	☐ Instalar/Movimentar periféricos
☐ Consumir alimentos	☐ Participar em sessões de chat
☐ Realizar cópias dos seus trabalhos	☐ Efectuar o download de ficheiros
☐ Realizar cópias dos programas instalados	☐ Instalar/desinstalar software

D17) Classifique, de acordo com o impacto na segurança do Sistema Informático da Escola (6 para muito importante e 1 para pouco importante), os seguintes tipos de ameaças:

	1	2	3	4	5	6
(a) Acidentes naturais (incêndios, terremotos, inundações, etc.)	☐	☐	☐	☐	☐	☐
(b) Hackers (acessos não autorizados a partir do exterior das organizações)	☐	☐	☐	☐	☐	☐
(c) Acessos indevidos (não autorizados) a partir do interior das organizações	☐	☐	☐	☐	☐	☐
(d) Virus/Trojan Horses/Worms/etc.	☐	☐	☐	☐	☐	☐
(e) Roubo de informação	☐	☐	☐	☐	☐	☐
(f) Destruição de informação	☐	☐	☐	☐	☐	☐
(g) Utilização incorrecta do sistema	☐	☐	☐	☐	☐	☐
(h) Definição por defeito das passwords iniciais (por ex. Password igual ao UserID)	☐	☐	☐	☐	☐	☐
(i) Intercepção de mensagens de correio electrónico e respectivos anexos	☐	☐	☐	☐	☐	☐
(j) Falhas no fornecimento de energia eléctrica ao sistema	☐	☐	☐	☐	☐	☐
(k) Configuração incorrecta da firewall	☐	☐	☐	☐	☐	☐
(l) Falhas de funcionamento do software do sistema	☐	☐	☐	☐	☐	☐
(m) Falhas de funcionamento do hardware do sistema	☐	☐	☐	☐	☐	☐



E - Usabilidade do Sistema Informático da Escola

Por **usabilidade** em sistemas informáticos entende-se a extensão até onde um sistema pode ser usado por utilizadores específicos para atingir objectivos especificados com eficácia, eficiência e satisfação num contexto de uso especificado [ISO 9241-11 *Requisitos ergonómicos para sistemas de trabalho com terminais de visualização - Orientação em usabilidade*], encontrando-se associada directamente à facilidade de utilização e aprendizagem de um sistema.

E1) Recebeu formação na utilização do Sistema Informático da Escola?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão E4).

E2) Com que frequência recebe formação necessária à utilização do Sistema Informático da Escola?

☐ Uma única vez ☐ Semestralmente
☐ Sempre que existem mudanças no sistema ☐ Anualmente
☐ Trimestralmente

E3) Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

E4) Existe algum(uns) documento(s) acerca da utilização do Sistema Informático da Escola?

☐ Não ☐ Não sabe ☐ Sim

Se respondeu NÃO ou NÃO SABE, passe para a questão E7).

E5) Como tomou conhecimento desse(s) documento(s)? (assinale todos os itens aplicáveis)

☐ Documento entregue na Escola ☐ Consulta da página web da Escola
☐ Informação dos serviços de informática ☐ Informação de colega
☐ Informação afixada na Escola ☐ Outro meio

E6) Classifique a utilidade desse(s) documento(s). (6 para muito útil e 1 para pouco útil)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

E7) Classifique a facilidade de utilização do Sistema Informático da Escola. (6 para fácil de utilizar e 1 para difícil de utilizar)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

E8) Classifique a facilidade de aprendizagem do Sistema Informático da Escola. (6 para fácil de aprender e 1 para difícil de aprender)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

E9) Classifique, relativamente à usabilidade do Sistema Informático da Escola (6 para muito importante e 1 para pouco importante), a relevância dos seguintes aspectos:

	1	2	3	4	5	6
(a) Facilidade de acesso	☐	☐	☐	☐	☐	☐
(b) Disponibilidade	☐	☐	☐	☐	☐	☐
(c) Adequação às necessidades	☐	☐	☐	☐	☐	☐
(d) Apoio técnico à utilização	☐	☐	☐	☐	☐	☐
(e) Interface com o sistema	☐	☐	☐	☐	☐	☐
(f) Regras de utilização	☐	☐	☐	☐	☐	☐
(g) Conhecimento prévio do sistema	☐	☐	☐	☐	☐	☐
(h) Participação no desenvolvimento/implementação do sistema	☐	☐	☐	☐	☐	☐

E10) Classifique em que medida considera que a usabilidade do Sistema Informático da Escola é ou pode ser importante para as suas actividades lectivas e de investigação. (6 para muito importante e 1 para pouco importante)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

Julho de 2007

Obrigado pela sua colaboração!



Questionário – Não Docentes

INSTRUÇÕES DE PREENCHIMENTO

Face ao seu processo de tratamento (leitura óptica), este QUESTIONÁRIO deve ser preenchido utilizando caneta ou esferográfica preta ou azul e preenchido como mostra o exemplo.

Preencha

assim ☒
 assim não ☒
 se rasurado ☒

QUESTIONÁRIO - SEGURANÇA DA INFORMAÇÃO

Caro(a) Colega,

Este questionário é constituído por 5 grupos de questões. O grupo A destina-se a caracterizar o(a) inquirido(a), o grupo B pretende obter uma caracterização da utilização do computador pessoal, enquanto que os grupos C, D e E se destinam a obter a percepção do(a) inquirido(a) acerca da utilização e da Segurança da Informação do Sistema Informático do Serviço.

De forma a garantir a privacidade dos(as) inquiridos(as) e o seu anonimato, agradeço que em nenhuma parte do questionário coloque qualquer nome ou número que possibilite a sua identificação.

A - Identificação/Caracterização do(a) inquirido(a)

- A1) Escalão etário ☐ Menos de 25 anos ☐ Entre 25 anos e 35 anos ☐ Mais de 35 anos
- A2) Área de residência ☐ Concelho de Setúbal ☐ Fora do Concelho de Setúbal
- A3) Antiguidade no IPS/Escola ☐ Até 5 anos ☐ Mais de 5 anos
- A4) Experiência profissional ☐ Menos de 2 anos ☐ Entre 2 anos e 5 anos ☐ Mais de 5 anos
- A5) Habilitações Académicas ☐ Mestrado/Lic./Bach. ☐ Secundário ☐ Básico
- A6) Carreira profissional ☐ Técnico Superior/Técnico ☐ Assistente Administrativo ☐ Técnico-Profissional

B - Computador pessoal

Nos casos em que dispõe de mais do que um computador pessoal na sua residência, deve responder tendo em consideração aquele que utiliza com maior frequência.

- B1) A quantos computadores possui acesso na sua residência?
☐ Nenhum ☐ 1 ☐ 2 ☐ 3 ou mais Se respondeu NENHUM, passe para o grupo C.
- B2) O computador pessoal a que acede é um portátil?
☐ Não ☐ Sim
- B3) Acede à Internet com o seu computador pessoal?
☐ Não ☐ Sim Se respondeu NÃO, passe para a questão B10).
- B4) Especifique em que locais acede à Internet com o seu computador pessoal? (assinale todos os itens aplicáveis)
☐ Residência ☐ Residência de colegas/amigos(as)
☐ Serviço ☐ Cafés/Restaurantes/etc.
☐ Outra Instituição de Ensino Superior ☐ Outros locais
- B5) Com quantas pessoas partilha a utilização do computador pessoal na sua residência?
☐ Nenhuma ☐ 1 ☐ 2 ☐ 3 ou mais
- B6) Com que frequência acede à Internet com o seu computador pessoal?
☐ Todos os dias ☐ Pelo menos uma vez por mês
☐ Quase todos os dias ☐ Uma ou duas vezes por semestre
☐ Pelo menos uma vez por semana
- B7) Durante esses acessos à Internet, qual o tempo médio diário de utilização?
☐ Até 1 hora ☐ Entre 1 e 3 horas ☐ Mais de 3 horas
- B8) Classifique a segurança do seu acesso? (6 para muito seguro e 1 para pouco seguro)

1 2 3 4 5 6

☐ ☐ ☐ ☐ ☐ ☐
- B9) Identifique a solução que adoptou para acesso à Internet com o seu computador pessoal.
☐ Modem ☐ ADSL ☐ Cabo ☐ Wireless ☐ Outra
- B10) Possui password para acesso ao seu computador pessoal?
☐ Não ☐ Sim Se respondeu NÃO, passe para a questão B18).
- B11) Com quantas pessoas partilha a sua password?
☐ Nenhuma ☐ 1 ☐ 2 ou 3 ☐ Mais de 3
- B12) Já alterou a password de acesso ao seu computador pessoal?
☐ Não ☐ Sim Se respondeu NÃO, passe para a questão B16).

23292



B13) Com que frequência altera a password de acesso ao seu computador pessoal?

- ☐ Uma única vez ☐ Semestralmente/Anualmente
☐ Raramente ☐ Mensalmente/Trimestralmente

B14) Que opções efectua na escolha da sua nova password? (assinale todos os itens aplicáveis)

- ☐ Datas de nascimento/aniversário ☐ Apenas números
☐ Nomes de familiares ☐ Apenas letras
☐ Nomes de locais ☐ Combinação de números e letras
☐ Nomes de animais de estimação ☐ Escolha aleatória de caracteres

B15) Na definição de nova password opta por:

- ☐ Número máximo de caracteres permitido
☐ Número fixo de caracteres, entre máximo e mínimo
☐ Número aleatório de caracteres, entre máximo e mínimo
☐ Número mínimo de caracteres permitido

B16) Classifique o grau de segurança da sua password. (6 para elevado e 1 para baixo)

- 1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

B17) Qual o processo que utiliza para guardar a sua password? (assinale todos os itens aplicáveis)

- ☐ Memorização ☐ Memória do telemóvel ☐ Post-it ☐ Registo na agenda pessoal ☐ Outro

B18) Além da password que mecanismo/ferramenta/software utiliza para protecção do seu computador pessoal? (assinale todos os itens aplicáveis)

- ☐ Nenhum
☐ Firewall (software/hardware para controlo do tráfego da rede informática, etc.)
☐ Antivírus (software destinado à detecção de vírus, entendidos em termos genéricos, e à sua eliminação)
☐ Antispyware (software destinado à detecção de programas intrusivos)
☐ Outros

B19) Com que frequência actualiza esse mecanismo/ferramenta/software? (assinale todos os itens aplicáveis)

- ☐ Sempre que existe uma actualização ☐ Sempre que possível
☐ Mensalmente/Trimestralmente ☐ Nunca actualiza
☐ Semestralmente/Anualmente

B20) Efectua cópias de segurança (backups) da informação contida no seu computador pessoal?

- ☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão B25).

B21) Com que periodicidade efectua cópias de segurança (backups)? (assinale todos os itens aplicáveis)

- ☐ No final de cada sessão de trabalho ☐ Mensalmente
☐ Na conclusão de cada projecto/trabalho/etc. ☐ Trimestralmente
☐ Diariamente ☐ Raramente
☐ Semanalmente

B22) Especifique a opção mais frequente para realização das cópias de segurança (backups)?

- ☐ Apenas os ficheiros alterados ☐ Um conjunto de ficheiros pré-definidos
☐ A totalidade da informação no disco ☐ Apenas os ficheiros considerados importantes

B23) Que tipo de dispositivo utiliza para efectuar as cópias de segurança (backups)? (assinale todos os itens aplicáveis)

- ☐ Disco do computador ☐ Memória flash amovível
☐ Disco externo ☐ Disquete
☐ CD/DVD ☐ Tape

B24) Especifique onde guarda as cópias de segurança (backups) que efectua.

- ☐ Na mesma sala onde se encontra o computador ☐ Fora da sua residência
☐ Em outro espaço da sua residência

B25) Classifique o grau de segurança do seu computador pessoal. (6 para elevado e 1 para baixo)

- 1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

B26) Com que frequência utiliza o seu computador pessoal?

- ☐ Todos os dias ☐ Pelo menos uma vez por mês
☐ Quase todos os dias ☐ Uma ou duas vezes por semestre
☐ Pelo menos uma vez por semana

B27) Caracterize como utiliza o seu computador pessoal. (assinale todos os itens aplicáveis)

- ☐ Elaboração de relatórios e outros trabalhos ☐ Jogos
☐ Impressão de documentos ☐ Pesquisas na Internet
☐ Trabalhos escolares ☐ Envio/recepção de correio electrónico



B28) Durante a utilização do seu computador pessoal, qual o tempo médio diário de utilização?

- ☐ Até 1 hora ☐ Entre 1 e 3 horas ☐ Mais de 3 horas

B29) Que tipo de software utiliza no seu computador pessoal? (assinale todos os itens aplicáveis)

☐ Sistema Operativo Windows	☐ Folha de Cálculo (por ex. Excel)
☐ Sistema Operativo Macintosh	☐ Base de Dados (por ex. Access)
☐ Sistema Operativo Linux	☐ Apresentações (por ex. PowerPoint)
☐ Outro Sistema Operativo	☐ Outros aplicativos
☐ Processador de Texto (por ex. Word)	

C - Sistema Informático do Serviço (Serviços Centrais, Centro, Escola, etc.)

Por Sistema Informático do Serviço (Serviços Centrais, Centro, Escola, etc.) entendem-se todos os recursos de computador (computadores, impressoras, scanners, etc.), disponibilizados para realização de trabalhos, pesquisa e comunicação, incluindo procedimentos e regras de acesso e utilização das aplicações disponibilizadas.

C1) Desde a sua entrada no Serviço existiu alguma mudança no Sistema Informático (Hardware, Software, Procedimentos, etc.)?

- ☐ Não ☐ Não sabe ☐ Sim Se respondeu NÃO ou NÃO SABE, passe para a questão C7).

C2) Foi solicitada a sua participação/participou de alguma forma nessas mudanças?

- ☐ Não ☐ Sim Se respondeu NÃO, passe para a questão C5).

C3) Caracterize a sua participação nessas mudanças. (assinale todos os itens aplicáveis)

☐ Aquisição de Software/Hardware	☐ Análise de documentos
☐ Instalação/Configuração de Hardware	☐ Preenchimento de inquéritos/questionários
☐ Instalação/Configuração de Software	☐ Resposta a entrevistas
☐ Definição/Implementação de Procedimentos	☐ Elaboração de pareceres

C4) Classifique o seu grau de participação nessas mudanças. (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C5) Classifique o seu grau de satisfação com as mudanças efectuadas. (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C6) Classifique a sua percepção acerca do funcionamento do Sistema Informático depois das mudanças efectuadas. (6 para melhorou muito e 1 para não melhorou)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C7) Já tinha utilizado computadores antes de ser admitido(a) no IPS/Escola?

- ☐ Não ☐ Sim Se respondeu NÃO, passe para a questão C10).

C8) Realizou algum(uns) curso(s) de formação em Informática/Sistemas de Informação antes de ser admitido(a) no IPS/Escola?

- ☐ Não ☐ Sim

C9) Classifique o seu grau de conhecimentos na área da Informática/Sistemas de Informação. (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C10) Dispõe de acesso ao Sistema Informático do Serviço?

- ☐ Não ☐ Sim Se respondeu NÃO, terminou aqui o preenchimento do questionário.

C11) O acesso ao Sistema Informático do Serviço é feito através de password?

- ☐ Não ☐ Sim Se respondeu NÃO, passe para a questão C20).

C12) Já alterou a(s) sua(s) password(s) de acesso ao Sistema Informático do Serviço?

- ☐ Não ☐ Sim Se respondeu NÃO, passe para a questão C16).

C13) Com que frequência altera a(s) sua(s) password(s) de acesso ao Sistema Informático do Serviço?

☐ Uma única vez	☐ Semestralmente/Anualmente
☐ Raramente	☐ Mensalmente/Trimestralmente

C14) Que opções efectua na escolha de nova(s) password(s)? (assinale todos os itens aplicáveis)

☐ Datas de nascimento/aniversário	☐ Apenas números
☐ Nomes de familiares	☐ Apenas letras
☐ Nomes de locais	☐ Combinação de números e letras
☐ Nomes de animais de estimação	☐ Escolha aleatória de caracteres

C15) Na definição de nova password opta por:

- ☐ Número máximo de caracteres permitido
☐ Número fixo de caracteres, entre máximo e mínimo
☐ Número aleatório de caracteres, entre máximo e mínimo
☐ Número mínimo de caracteres permitido

C16) Qual o processo que utiliza para guardar a(s) sua(s) password(s)? (assinale todos os itens aplicáveis)

- ☐ Memorização ☐ Memória do telemóvel ☐ Post-it ☐ Registo na agenda pessoal ☐ Outro

23292



C17) Com quantas pessoas partilha a(s) sua(s) password(s) de acesso ao Sistema Informático do Serviço?

☐ Nenhuma ☐ 1 ☐ 2 ou 3 ☐ Mais de 3

C18) Utiliza a mesma password para diversas aplicações/sistemas?

☐ Não ☐ Sim

C19) Classifique o grau de segurança da(s) sua(s) password(s). (6 para elevado e 1 para baixo)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

C20) Além da password, especifique que tipo(s) de mecanismo(s) está(ão) implementado(s) para acesso ao Sistema Informático do Serviço. (assinale todos os itens aplicáveis)

☐ Cartão magnético ☐ Controlo biométrico
☐ Cartão com microchip ☐ Identificação pessoal
☐ Chave metálica ☐ Nenhum

C21) Possui algum endereço de correio electrónico associado ao Sistema Informático do Serviço?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C25).

C22) Além desse, quantos endereços de correio electrónico possui?

☐ Nenhum ☐ 1 ☐ 2 ☐ 3 ☐ Mais de 3

C23) Utiliza a mesma password para acesso ao correio electrónico e ao Sistema Informático do Serviço?

☐ Não ☐ Sim

C24) Existe implementado algum sistema de filtragem de mensagens de correio electrónico?

☐ Não ☐ Não sabe ☐ Sim

C25) Com que frequência acede ao Sistema Informático do Serviço?

☐ Todos os dias ☐ Pelo menos uma vez por mês
☐ Quase todos os dias ☐ Uma ou duas vezes por semestre
☐ Pelo menos uma vez por semana

C26) Durante a utilização do Sistema Informático do Serviço, qual o tempo médio diário de cada utilização?

☐ Até 1 hora ☐ Entre 1 e 3 horas ☐ Entre 3 e 5 horas ☐ Mais de 5 horas

C27) Que tipo de software utiliza? (assinale todos os itens aplicáveis)

☐ Sistema Operativo Windows 95/98/2000/XP ☐ Base de Dados
☐ Sistema Operativo Windows Server ☐ Programação
☐ Sistema Operativo Linux ☐ Apresentações
☐ Sistema Operativo Macintosh ☐ Desenho técnico
☐ Outro Sistema Operativo ☐ Análise de Sistemas
☐ Processador de Texto ☐ Gestão/Contabilidade/Marketing
☐ Folha de Cálculo ☐ Outros aplicativos

C28) Caracterize a sua utilização do Sistema Informático do Serviço. (assinale todos os itens aplicáveis)

☐ Elaboração de relatórios ☐ Análise estatística/projecções
☐ Elaboração de outros trabalhos ☐ Pesquisas na Internet
☐ Impressão de documentos ☐ Envio/recepção de correio electrónico
☐ Registo/Introdução de dados

C29) Utiliza alguma área de trabalho privada no(s) servidor(es) do Sistema Informático do Serviço?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C34).

C30) Que tipo de informação guarda nessa área de trabalho?

☐ Ficheiros de trabalho ☐ Ficheiros pessoais ☐ Ambos

C31) Já perdeu informação guardada nessa área de trabalho?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C34).

C32) Que acção tomou para recuperar essa informação?

☐ Expôs a situação ao(à) responsável do Serviço ou aos serviços de informática
☐ Tentou recuperar a informação
☐ Nenhuma

C33) O que aconteceu relativamente a essa situação? (assinale todos os itens aplicáveis)

☐ A informação foi reposta de backups anteriores
☐ A informação foi recuperada mas não sabe como
☐ A informação não foi recuperada
☐ Recebeu comunicação de que era impossível recuperar a informação
☐ Não sabe nada acerca da situação

23292



C34) Possui acesso à impressão de documentos através do Sistema Informático do Serviço utilizando impressora(s) partilhada(s)?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C38)

C35) Quando não consegue imprimir documentos através da(s) impressora(s) partilhada(s) qual a atitude que assume?
(assinale todos os itens aplicáveis)

☐ Cancela de imediato o trabalho	☐ Tenta imprimir mais tarde
☐ Tenta imprimir novamente	☐ Informa o(a) responsável do Serviço
☐ Verifica se a impressora tem algum problema	☐ Informa os serviços de informática
☐ Tenta imprimir numa impressora disponível	☐ Nenhuma
☐ Altera a configuração de acesso à impressora	

C36) Que atitude toma quando encontra documentos que não são seus na(s) impressora(s) partilhada(s)? (assinale todos os itens aplicáveis)

☐ Nunca encontrou	☐ Deita fora ou destrói o documento
☐ Lê o documento (todo ou parte)	☐ Guarda para seu uso pessoal
☐ Entrega ao(a) responsável do Serviço	☐ Deixa junto à impressora
☐ Tenta entregar/entregou ao(a) seu(sua) proprietário(a)	☐ Nenhuma

C37) Que atitude toma quando não encontra documentos seus que mandou imprimir na(s) impressora(s) partilhada(s)?
(assinale todos os itens aplicáveis)

☐ Nunca aconteceu	☐ Imprime novamente o documento
☐ Verifica se ainda aguarda por impressão	☐ Tenta encontrar o documento
☐ Informa o(a) responsável do Serviço	☐ Nenhuma
☐ Informa os serviços de informática	

C38) Consideraria a hipótese de aceder ao Sistema Informático do Serviço a partir da sua residência ou de outro local onde trabalhe regularmente?

☐ Não ☐ Sim ☐ Talvez

D - Segurança da Informação no Sistema Informático do Serviço

Por **Segurança da Informação** em sistemas informáticos entende-se: preservação da **confidencialidade** (assegurar que a informação apenas é acedida por quem está autorizado a fazê-lo), da **integridade** (garantir a exactidão e a credibilidade da informação) e da **disponibilidade** (assegurar que as pessoas autorizadas têm acesso à informação e aos activos associados sempre que necessário) da informação [BS ISO/IEC 17799:2005 Information Technology - Code of practice for information security management]

D1) Existem políticas (normas/regulamentos/regras/procedimentos) de segurança do Sistema Informático do Serviço?

☐ Não ☐ Não sabe ☐ Sim

Se respondeu NÃO ou NÃO SABE, passe para a questão D7).

D2) Como tomou conhecimento dessas políticas (normas/regulamentos/regras/procedimentos)? (assinale todos os itens aplicáveis)

☐ Documento entregue no Serviço	☐ Consulta da página web do Serviço
☐ Informação do(a) responsável do Serviço	☐ Colega de trabalho
☐ Informação afixada no Serviço	☐ Outro meio

D3) Dos aspectos a seguir mencionados, especifique quais são abrangidos pelas políticas (normas/regulamentos/regras/procedimentos) definidas. (assinale todos os itens aplicáveis)

☐ Definição de acessos ao sistema (passwords)	☐ Utilização dos recursos de hardware
☐ Utilização do correio electrónico	☐ Acesso aos servidores
☐ Utilização da Internet	☐ Realização de cópias de segurança (backups)
☐ Detecção/Controlo de intrusões	☐ Instalação de software
☐ Controlo dos activos do sistema	☐ Plano de Recuperação de Acidentes

D4) Participou na elaboração/alteração dessas políticas (normas/regulamentos/regras/procedimentos)?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão D7).

D5) Caracterize a sua participação nessas actividades. (assinale todos os itens aplicáveis)

☐ Elaboração das políticas	☐ Preenchimento de inquéritos/questionários
☐ Implementação das políticas	☐ Resposta a entrevistas
☐ Análise de documentos	☐ Elaboração de pareceres

D6) Classifique o seu grau de participação nessas actividades. (6 para elevado e 1 para baixo)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

D7) Caracterize a sua participação nas acções de sensibilização para a problemática da segurança da informação?

☐ Não teve conhecimento de qualquer acção	☐ Não quis participar
☐ Não teve possibilidade de participar	☐ Participou com interesse
☐ Não foi convidado(a) a participar	☐ Participou sem interesse

D8) Já presenciou alguma(s) violação(ões) da segurança do Sistema Informático do Serviço (por exemplo destruição/roubo de equipamentos, entradas em locais interditos, utilização de ficheiros/passwords de outras pessoas, etc.)?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão D10).

23292



D9) Que atitude tomou quando presenciou essa(s) violação(ões)? (assinale todos os itens aplicáveis)

☐ Advertiu o(a) infractor(a)	☐ Propôs medidas para resolução do problema
☐ Informou o(a) responsável do Serviço	☐ Comentou com os(as) seus(suas) colegas
☐ Informou os serviços de informática	☐ Nenhuma

D10) Após o login no acesso ao Sistema Informático do Serviço, existe definido algum tempo limite para que a sessão de trabalho esteja activa?

- ☐ Não ☐ Não sabe ☐ Sim

D11) Durante o tempo em que tem activa a sua sessão de trabalho, utiliza algum mecanismo de protecção de ecrã para quando não está a utilizar o computador?

- ☐ Não ☐ Sim

D12) Classifique a segurança do Sistema Informático do Serviço.
(6 para muito seguro e 1 para pouco seguro)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

D13) Classifique, relativamente à segurança do Sistema Informático do Serviço (6 para muito importante e 1 para pouco importante), os seguintes aspectos:

	1	2	3	4	5	6
(a) Utilizadores	☐	☐	☐	☐	☐	☐
(b) Técnicos de Informática	☐	☐	☐	☐	☐	☐
(c) Leis/Políticas/Regulamentos/Procedimentos	☐	☐	☐	☐	☐	☐
(d) Computadores Pessoais (Hardware)	☐	☐	☐	☐	☐	☐
(e) Periféricos (Impressoras, Scanners, etc.)	☐	☐	☐	☐	☐	☐
(f) Servidores (Hardware)	☐	☐	☐	☐	☐	☐
(g) Software aplicacional	☐	☐	☐	☐	☐	☐
(h) Sistemas Operativos	☐	☐	☐	☐	☐	☐
(i) Internet	☐	☐	☐	☐	☐	☐
(j) Correio electrónico	☐	☐	☐	☐	☐	☐
(k) Rede informática	☐	☐	☐	☐	☐	☐
(l) Sistema de comunicações (telefones, telefaxes, etc.)	☐	☐	☐	☐	☐	☐

D14) Classifique em que medida considera que a segurança do Sistema Informático do Serviço é ou pode ser importante para as suas actividades laborais. (6 para muito importante e 1 para pouco importante)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

D15) Classifique a facilidade de acesso físico ao Sistema Informático do Serviço (6 para muito difícil e 1 para muito fácil), nos seguintes pontos de acesso:

	1	2	3	4	5	6
(a) Sala de servidores	☐	☐	☐	☐	☐	☐
(b) Serviços de Informática	☐	☐	☐	☐	☐	☐
(c) Serviços administrativos/académicos/etc.	☐	☐	☐	☐	☐	☐
(d) Gabinetes de colegas	☐	☐	☐	☐	☐	☐
(e) Salas de reunião	☐	☐	☐	☐	☐	☐
(f) Átrios/corredores	☐	☐	☐	☐	☐	☐
(g) Área circundante do Serviço	☐	☐	☐	☐	☐	☐
(h) Laboratórios de Informática	☐	☐	☐	☐	☐	☐

D16) Nos locais onde tem acesso ao Sistema Informático do Serviço, especifique que actividades estão proibidas.
(assinale todos os itens aplicáveis)

☐ Fumar	☐ Movimentar computadores instalados
☐ Ingerir bebidas	☐ Instalar/Movimentar periféricos
☐ Consumir alimentos	☐ Participar em sessões de chat
☐ Realizar cópias dos seus trabalhos	☐ Efectuar o download de ficheiros
☐ Realizar cópias dos programas instalados	☐ Instalar/desinstalar software

D17) Classifique, de acordo com o impacto na segurança do Sistema Informático do Serviço (6 para muito importante e 1 para pouco importante), os seguintes tipos de ameaças:

	1	2	3	4	5	6
(a) Acidentes naturais (incêndios, terremotos, inundações, etc.)	☐	☐	☐	☐	☐	☐
(b) Hackers (acessos não autorizados a partir do exterior das organizações)	☐	☐	☐	☐	☐	☐
(c) Acessos indevidos (não autorizados) a partir do interior das organizações	☐	☐	☐	☐	☐	☐
(d) Virus/Trojan Horses/Worms/etc.	☐	☐	☐	☐	☐	☐
(e) Roubo de informação	☐	☐	☐	☐	☐	☐
(f) Destruição de informação	☐	☐	☐	☐	☐	☐
(g) Utilização incorrecta do sistema	☐	☐	☐	☐	☐	☐
(h) Definição por defeito das passwords iniciais (por ex. Password igual ao UserID)	☐	☐	☐	☐	☐	☐
(i) Intercepção de mensagens de correio electrónico e respectivos anexos	☐	☐	☐	☐	☐	☐
(j) Falhas no fornecimento de energia eléctrica ao sistema	☐	☐	☐	☐	☐	☐
(k) Configuração incorrecta da firewall	☐	☐	☐	☐	☐	☐
(l) Falhas de funcionamento do software do sistema	☐	☐	☐	☐	☐	☐
(m) Falhas de funcionamento do hardware do sistema	☐	☐	☐	☐	☐	☐

23292



E - Usabilidade do Sistema Informático do Serviço

Por **usabilidade** em sistemas informáticos entende-se a extensão até onde um sistema pode ser usado por utilizadores específicos para atingir objectivos especificados com eficácia, eficiência e satisfação num contexto de uso especificado [ISO 9241-11 *Requisitos ergonómicos para sistemas de trabalho com terminais de visualização - Orientação em usabilidade*], encontrando-se associada directamente à facilidade de utilização e aprendizagem de um sistema.

E1) Recebeu formação na utilização do Sistema Informático do Serviço?

☐ Não ☐ Sim

Se respondeu **NÃO**, passe para a questão **E4**.

E2) Com que frequência recebe formação necessária à utilização do Sistema Informático do Serviço?

☐ Uma única vez ☐ Semestralmente
☐ Sempre que existem mudanças no sistema ☐ Anualmente
☐ Trimestralmente

E3) Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

E4) Existe algum(uns) documento(s) acerca da utilização do Sistema Informático do Serviço?

☐ Não ☐ Não sabe ☐ Sim

Se respondeu **NÃO** ou **NÃO SABE**, passe para a questão **E7**.

E5) Como tomou conhecimento desse(s) documento(s)? (assinale todos os itens aplicáveis)

☐ Documento entregue no Serviço ☐ Consulta da página web do Serviço
☐ Informação dos serviços de informática ☐ Informação de colega
☐ Informação afixada no Serviço ☐ Outro meio

E6) Classifique a utilidade desse(s) documento(s). (6 para muito útil e 1 para pouco útil)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

E7) Classifique a facilidade de utilização do Sistema Informático do Serviço. (6 para fácil de utilizar e 1 para difícil de utilizar)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

E8) Classifique a facilidade de aprendizagem do Sistema Informático do Serviço. (6 para fácil de aprender e 1 para difícil de aprender)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

E9) Classifique, relativamente à usabilidade do Sistema Informático do Serviço (6 para muito importante e 1 para pouco importante), a relevância dos seguintes aspectos:

	1	2	3	4	5	6
(a) Facilidade de acesso	☐	☐	☐	☐	☐	☐
(b) Disponibilidade	☐	☐	☐	☐	☐	☐
(c) Adequação às necessidades	☐	☐	☐	☐	☐	☐
(d) Apoio técnico à utilização	☐	☐	☐	☐	☐	☐
(e) Interface com o sistema	☐	☐	☐	☐	☐	☐
(f) Regras de utilização	☐	☐	☐	☐	☐	☐
(g) Conhecimento prévio do sistema	☐	☐	☐	☐	☐	☐
(h) Participação no desenvolvimento/implementação do sistema	☐	☐	☐	☐	☐	☐

E10) Classifique em que medida considera que a usabilidade do Sistema Informático do Serviço é ou pode ser importante para as suas actividades laborais. (6 para muito importante e 1 para pouco importante)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

Julho de 2007

Obrigado pela sua colaboração!



Questionário – Técnicos

INSTRUÇÕES DE PREENCHIMENTO

Face ao seu processo de tratamento (leitura óptica), este
QUESTIONÁRIO deve ser preenchido utilizando **caneta ou
esferográfica preta ou azul** e preenchido como mostra o exemplo.

Preencha

assim ☒
assim não ☒
se rasurado ☒

QUESTIONÁRIO - SEGURANÇA DA INFORMAÇÃO

Caro(a) Colega,

Este questionário é constituído por 5 grupos de questões. O grupo A destina-se a caracterizar o(a) inquirido(a), o grupo B pretende obter uma caracterização da utilização do computador pessoal, enquanto que os grupos C, D e E se destinam a obter a percepção do(a) inquirido(a) acerca da utilização e da Segurança da Informação do Sistema Informático do Serviço.

De forma a garantir a privacidade dos(as) inquiridos(as) e o seu anonimato, agradeço que em nenhuma parte do questionário coloque qualquer nome ou número que possibilite a sua identificação.

A - Identificação/Caracterização do(a) inquirido(a)

- A1) Escalão etário ☐ Menos de 25 anos ☐ Entre 25 anos e 35 anos ☐ Mais de 35 anos
- A2) Área de residência ☐ Concelho de Setúbal ☐ Fora do Concelho de Setúbal
- A3) Antiguidade no IPS/Escola ☐ Até 5 anos ☐ Mais de 5 anos
- A4) Experiência profissional ☐ Menos de 2 anos ☐ Entre 2 anos e 5 anos ☐ Mais de 5 anos
- A5) Habilitações Académicas ☐ Mestrado/Licenciatura ☐ Bacharelato ☐ Secundário
- A6) Área de formação ☐ Informática/Engenharia Informática
☐ Engenharia Electrónica/Electrotécnica/Computadores/Telecomunicações
☐ Informática de Gestão/Sistemas de Informação/Tecnologias de Informação e Comunicação
☐ Outra

B - Computador pessoal

Nos casos em que dispõe de mais do que um computador pessoal na sua residência, deve responder tendo em consideração aquele que utiliza com maior frequência.

B1) A quantos computadores possui acesso na sua residência?

☐ Nenhum ☐ 1 ☐ 2 ☐ 3 ou mais

Se respondeu **NENHUM**, passe para o grupo C.

B2) O computador pessoal a que acede é um portátil?

☐ Não ☐ Sim

B3) Acede à Internet com o seu computador pessoal?

☐ Não ☐ Sim

Se respondeu **NÃO**, passe para a questão B10).

B4) Especifique em que locais acede à Internet com o seu computador pessoal? (assinale todos os itens aplicáveis)

☐ Residência ☐ Residência de colegas/amigos(as)
☐ Serviço ☐ Cafés/Restaurantes/etc.
☐ Outra Instituição de Ensino Superior ☐ Outros locais

B5) Com quantas pessoas partilha a utilização do computador pessoal na sua residência?

☐ Nenhuma ☐ 1 ☐ 2 ☐ 3 ou mais

B6) Com que frequência acede à Internet com o seu computador pessoal?

☐ Todos os dias ☐ Pelo menos uma vez por mês
☐ Quase todos os dias ☐ Uma ou duas vezes por semestre
☐ Pelo menos uma vez por semana

B7) Durante esses acessos à Internet, qual o tempo médio diário de utilização?

☐ Até 1 hora ☐ Entre 1 e 3 horas ☐ Mais de 3 horas

B8) Classifique a segurança do seu acesso? (6 para muito seguro e 1 para pouco seguro)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

B9) Identifique a solução que adoptou para acesso à Internet com o seu computador pessoal.

☐ Modem ☐ ADSL ☐ Cabo ☐ Wireless ☐ Outra

B10) Possui password para acesso ao seu computador pessoal?

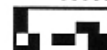
☐ Não ☐ Sim

Se respondeu **NÃO**, passe para a questão B18).

B11) Com quantas pessoas partilha a sua password?

☐ Nenhuma ☐ 1 ☐ 2 ou 3 ☐ Mais de 3

55905



B12) Já alterou a password de acesso ao seu computador pessoal?
☐ Não ☐ Sim Se respondeu NÃO, passe para a questão B16).

B13) Com que frequência altera a password de acesso ao seu computador pessoal?
☐ Uma única vez ☐ Semestralmente/Anualmente
☐ Raramente ☐ Mensalmente/Trimestralmente

B14) Que opções efectua na escolha da sua nova password? (assinale todos os itens aplicáveis)
☐ Datas de nascimento/aniversário ☐ Apenas números
☐ Nomes de familiares ☐ Apenas letras
☐ Nomes de locais ☐ Combinação de números e letras
☐ Nomes de animais de estimação ☐ Escolha aleatória de caracteres

B15) Na definição de nova password opta por:
☐ Número máximo de caracteres permitido
☐ Número fixo de caracteres, entre máximo e mínimo
☐ Número aleatório de caracteres, entre máximo e mínimo
☐ Número mínimo de caracteres permitido

B16) Classifique o grau de segurança da sua password. (6 para elevado e 1 para baixo)

1 2 3 4 5 6

☐ ☐ ☐ ☐ ☐ ☐

B17) Qual o processo que utiliza para guardar a(s) sua(s) password(s)? (assinale todos os itens aplicáveis)
☐ Memorização ☐ Memória do telemóvel ☐ Post-it ☐ Registo na agenda pessoal ☐ Outro

B18) Além da password que mecanismo/ferramenta/software utiliza para protecção do seu computador pessoal? (assinale todos os itens aplicáveis)
☐ Nenhum
☐ Firewall (software/hardware para controlo do tráfego da rede informática, etc.)
☐ Antivírus (software destinado à detecção de vírus, entendidos em termos genéricos, e à sua eliminação)
☐ Antispyware (software destinado à detecção de programas intrusivos)
☐ Outros

B19) Com que frequência actualiza esse mecanismo/ferramenta/software? (assinale todos os itens aplicáveis)
☐ Sempre que existe uma actualização ☐ Sempre que possível
☐ Mensalmente/Trimestralmente ☐ Nunca actualiza
☐ Semestralmente/Anualmente

B20) Efectua cópias de segurança (backups) da informação contida no seu computador pessoal?
☐ Não ☐ Sim Se respondeu NÃO, passe para a questão B25).

B21) Com que periodicidade efectua cópias de segurança (backups)? (assinale todos os itens aplicáveis)
☐ No final de cada sessão de trabalho ☐ Mensalmente
☐ Na conclusão de cada projecto/trabalho/etc. ☐ Trimestralmente
☐ Diariamente ☐ Raramente
☐ Semanalmente

B22) Especifique a opção mais frequente para realização das cópias de segurança (backups)?
☐ Apenas os ficheiros alterados ☐ Um conjunto de ficheiros pré-definidos
☐ A totalidade da informação no disco ☐ Apenas os ficheiros considerados importantes

B23) Que tipo de dispositivo utiliza para efectuar as cópias de segurança (backups)? (assinale todos os itens aplicáveis)
☐ Disco do computador ☐ Memória flash amovível
☐ Disco externo ☐ Disquete
☐ CD/DVD ☐ Tape

B24) Especifique onde guarda as cópias de segurança (backups) que efectua.
☐ Na mesma sala onde se encontra o computador ☐ Fora da sua residência
☐ Em outro espaço da sua residência

B25) Classifique o grau de segurança do seu computador pessoal. (6 para elevado e 1 para baixo)

1 2 3 4 5 6

☐ ☐ ☐ ☐ ☐ ☐

B26) Com que frequência utiliza o seu computador pessoal?
☐ Todos os dias ☐ Pelo menos uma vez por mês
☐ Quase todos os dias ☐ Uma ou duas vezes por semestre
☐ Pelo menos uma vez por semana

B27) Caracterize como utiliza o seu computador pessoal. (assinale todos os itens aplicáveis)
☐ Elaboração de relatórios e outros trabalhos ☐ Jogos
☐ Impressão de documentos ☐ Pesquisas na Internet
☐ Trabalhos escolares ☐ Envio/recepção de correio electrónico

B28) Durante a utilização do seu computador pessoal, qual o tempo médio diário de utilização?
☐ Até 1 hora ☐ Entre 1 e 3 horas ☐ Mais de 3 horas

55905



B29) Que tipo de software utiliza no seu computador pessoal? (assinale todos os itens aplicáveis)

☐ Sistema Operativo Windows	☐ Folha de Cálculo (por ex. Excel)
☐ Sistema Operativo Macintosh	☐ Base de Dados (por ex. Access)
☐ Sistema Operativo Linux	☐ Apresentações (por ex. PowerPoint)
☐ Outro Sistema Operativo	☐ Outros aplicativos
☐ Processador de Texto (por ex. Word)	

C - Sistema Informático do Serviço (Serviços Centrais, Centro, Escola, etc.)

Por Sistema Informático do Serviço (Serviços Centrais, Centro, Escola, etc.) entendem-se todos os recursos de computador (computadores, impressoras, scanners, etc.), disponibilizados para realização de trabalhos, pesquisa e comunicação, incluindo procedimentos e regras de acesso e utilização das aplicações disponibilizadas.

C1) Desde a sua entrada no Serviço existiu alguma mudança no Sistema Informático (Hardware, Software, Procedimentos, etc.)?

- ☐ Não ☐ Não sabe ☐ Sim

Se respondeu NÃO ou NÃO SABE, passe para a questão C7).

C2) Foi solicitada a sua participação/participou de alguma forma nessas mudanças?

- ☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C5).

C3) Caracterize a sua participação nessas mudanças. (assinale todos os itens aplicáveis)

☐ Aquisição de Software/Hardware	☐ Análise de documentos
☐ Instalação/Configuração de Hardware	☐ Preenchimento de inquéritos/questionários
☐ Instalação/Configuração de Software	☐ Resposta a entrevistas
☐ Definição/Implementação de Procedimentos	☐ Elaboração de pareceres

C4) Classifique o seu grau de participação nessas mudanças. (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C5) Classifique o seu grau de satisfação com as mudanças efectuadas. (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C6) Classifique a sua percepção acerca do funcionamento do Sistema Informático depois das mudanças efectuadas. (6 para melhorou muito e 1 para não melhorou)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C7) Qual a frequência média anual das acções de formação em informática que recebeu?

- ☐ Nunca recebeu ☐ 1 ☐ 2 ☐ 3 ☐ 4 ou mais

C8) Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C9) Classifique o seu grau de conhecimentos na área da Informática/Sistemas de Informação. (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C10) O acesso ao Sistema Informático do Serviço é feito através de password?

- ☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C20).

C11) Já alterou a(s) sua(s) password(s) de acesso ao Sistema Informático do Serviço?

- ☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão C15).

C12) Com que frequência altera a(s) sua(s) password(s) de acesso ao Sistema Informático do Serviço?

☐ Uma única vez	☐ Semestralmente/Anualmente
☐ Raramente	☐ Mensalmente/Trimestralmente

C13) Que opções efectua na escolha de nova(s) password(s)? (assinale todos os itens aplicáveis)

☐ Datas de nascimento/aniversário	☐ Apenas números
☐ Nomes de familiares	☐ Apenas letras
☐ Nomes de locais	☐ Combinação de números e letras
☐ Nomes de animais de estimação	☐ Escolha aleatória de caracteres

C14) Na definição de nova password opta por:

- ☐ Número máximo de caracteres permitido
- ☐ Número fixo de caracteres, entre máximo e mínimo
- ☐ Número aleatório de caracteres, entre máximo e mínimo
- ☐ Número mínimo de caracteres permitido

C15) Qual o processo que utiliza para guardar a(s) sua(s) password(s)? (assinale todos os itens aplicáveis)

- ☐ Memorização ☐ Memória do telemóvel ☐ Post-it ☐ Registo na agenda pessoal ☐ Outro

C16) Com quantas pessoas partilha a(s) sua(s) password(s) de acesso ao Sistema Informático do Serviço?

- ☐ Nenhuma ☐ 1 ☐ 2 ou 3 ☐ Mais de 3

C17) Quantas passwords de acesso ao Sistema Informático do Serviço utiliza?

- ☐ 1 ☐ 2 ☐ 3 ☐ 4 ou mais

C18) Utiliza a mesma password para diversas aplicações/sistemas?

- ☐ Não ☐ Sim

55905



C19) Classifique o grau de segurança da(s) sua(s) password(s). (6 para elevado e 1 para baixo)

1	2	3	4	5	6
☐	☐	☐	☐	☐	☐

C20) Além da password, especifique que tipo(s) de mecanismo(s) está(ão) implementado(s) para acesso ao Sistema Informático do Serviço. (assinale todos os itens aplicáveis)

☐ Cartão magnético	☐ Controlo biométrico
☐ Cartão com microchip	☐ Identificação pessoal
☐ Chave metálica	☐ Nenhum

C21) Possui algum endereço de correio electrónico associado ao Sistema Informático do Serviço?

☐ Não ☐ Sim Se respondeu NÃO, passe para a questão C25).

C22) Além desse, quantos endereços de correio electrónico possui?

☐ Nenhum ☐ 1 ☐ 2 ☐ 3 ☐ Mais de 3

C23) Utiliza a mesma password para acesso ao correio electrónico e ao Sistema Informático do Serviço?

☐ Não ☐ Sim

C24) Existe implementado algum sistema de filtragem de mensagens de correio electrónico?

☐ Não ☐ Não sabe ☐ Sim

C25) Com que frequência acede ao Sistema Informático do Serviço?

☐ Todos os dias	☐ Pelo menos uma vez por mês
☐ Quase todos os dias	☐ Uma ou duas vezes por semestre
☐ Pelo menos uma vez por semana	

C26) Durante a utilização do Sistema Informático do Serviço, qual o tempo médio diário de cada utilização?

☐ Até 1 hora ☐ Entre 1 e 3 horas ☐ Entre 3 e 5 horas ☐ Mais de 5 horas

C27) Que tipo de software utiliza? (assinale todos os itens aplicáveis)

☐ Sistema Operativo Windows 95/98/2000/XP	☐ Base de Dados
☐ Sistema Operativo Windows Server	☐ Programação
☐ Sistema Operativo Linux	☐ Apresentações
☐ Sistema Operativo Macintosh	☐ Desenho técnico
☐ Outro Sistema Operativo	☐ Análise de Sistemas
☐ Processador de Texto	☐ Gestão/Contabilidade/Marketing
☐ Folha de Cálculo	☐ Outros aplicativos

C28) Caracterize a sua utilização do Sistema Informático do Serviço. (assinale todos os itens aplicáveis)

☐ Elaboração de relatórios	☐ Análise estatística/projecções
☐ Elaboração de outros trabalhos	☐ Pesquisas na Internet
☐ Impressão de documentos	☐ Envio/recepção de correio electrónico
☐ Registo/Introdução de dados	

C29) Utiliza alguma área de trabalho privada no(s) servidor(es) do Sistema Informático do Serviço?

☐ Não ☐ Sim Se respondeu NÃO, passe para a questão C34).

C30) Que tipo de informação guarda nessa área de trabalho?

☐ Ficheiros de trabalho ☐ Ficheiros pessoais ☐ Ambos

C31) Já perdeu informação guardada nessa área de trabalho?

☐ Não ☐ Sim Se respondeu NÃO, passe para a questão C34).

C32) Que acção tomou para recuperar essa informação?

☐ Expôs a situação ao(à) responsável do Serviço

☐ Tentou recuperar a informação

☐ Nenhuma

C33) O que aconteceu relativamente a essa situação? (assinale todos os itens aplicáveis)

☐ A informação foi reposta de backups anteriores

☐ A informação foi recuperada mas não sabe como

☐ A informação não foi recuperada

☐ Recebeu comunicação de que era impossível recuperar a informação

☐ Não sabe nada acerca da situação

C34) Possui acesso à Impressão de documentos através do Sistema Informático do Serviço utilizando impressora(s) partilhada(s)?

☐ Não ☐ Sim Se respondeu NÃO, passe para a questão C38).

C35) Quando não consegue imprimir documentos através da(s) impressora(s) partilhada(s) qual a atitude que assume? (assinale todos os itens aplicáveis)

☐ Cancela de imediato o trabalho	☐ Altera a configuração de acesso à impressora
☐ Tenta imprimir novamente	☐ Tenta imprimir mais tarde
☐ Verifica se a impressora tem algum problema	☐ Informa o(a) responsável do Serviço
☐ Tenta imprimir numa impressora disponível	☐ Nenhuma

55805



C36) Que atitude toma quando encontra documentos que não são seus na(s) impressora(s) partilhada(s)? (assinale todos os itens aplicáveis)

☐ Nunca encontrou	☐ Deita fora ou destrói o documento
☐ Lê o documento (todo ou parte)	☐ Guarda para seu uso pessoal
☐ Entrega ao(a) responsável do Serviço	☐ Deixa junto à impressora
☐ Tenta entregar/entregou ao(a) seu(sua) proprietário(a)	☐ Nenhuma

C37) Que atitude toma quando não encontra documentos seus que mandou imprimir na(s) impressora(s) partilhada(s)? (assinale todos os itens aplicáveis)

☐ Nunca aconteceu	☐ Imprime novamente o documento
☐ Verifica se ainda aguarda por impressão	☐ Tenta encontrar o documento
☐ Informa o(a) responsável do Serviço	☐ Nenhuma

C38) Consideraria a hipótese de aceder ao Sistema Informático do Serviço a partir da sua residência ou de outro local onde trabalhe regularmente?

☐ Não ☐ Sim ☐ Talvez

D - Segurança da Informação no Sistema Informático do Serviço

Por **Segurança da Informação** em sistemas informáticos entende-se: preservação da **confidencialidade** (assegurar que a informação apenas é acedida por quem está autorizado a fazê-lo), da **integridade** (garantir a exactidão e a credibilidade da informação) e da **disponibilidade** (assegurar que as pessoas autorizadas têm acesso à informação e aos activos associados sempre que necessário) da informação [BS ISO/IEC 17799:2005 Information Technology - Code of practice for information security management]

D1) Existem políticas (normas/regulamentos/regras/procedimentos) de segurança do Sistema Informático do Serviço?

☐ Não ☐ Não sabe ☐ Sim Se respondeu NÃO ou NÃO SABE, passe para a questão D7).

D2) Como tomou conhecimento dessas políticas (normas/regulamentos/regras/procedimentos)? (assinale todos os itens aplicáveis)

☐ Documento entregue no Serviço	☐ Consulta da página web do Serviço
☐ Informação do(a) responsável do Serviço	☐ Colega de trabalho
☐ Informação afixada no Serviço	☐ Outro meio

D3) Dos aspectos a seguir mencionados, especifique quais são abrangidos pelas políticas (normas/regulamentos/regras/procedimentos) definidas. (assinale todos os itens aplicáveis)

☐ Definição de acessos ao sistema (por ex. passwords)	☐ Utilização dos recursos de hardware
☐ Utilização do correio electrónico	☐ Acesso aos servidores
☐ Utilização da Internet	☐ Realização de cópias de segurança (backups)
☐ Detecção/Controlo de intrusões	☐ Instalação de software
☐ Controlo dos activos do sistema	☐ Plano de Recuperação de Acidentes

D4) Participou na elaboração/alteração dessas políticas (normas/regulamentos/regras/procedimentos)?

☐ Não ☐ Sim Se respondeu NÃO, passe para a questão D7).

D5) Caracterize a sua participação nessas actividades. (assinale todos os itens aplicáveis)

☐ Elaboração das políticas	☐ Implementação das políticas
☐ Análise de documentos	☐ Análise/Auditoria de segurança
☐ Preenchimento de inquéritos/questionários	☐ Elaboração de pareceres
☐ Resposta a entrevistas	

D6) Classifique o seu grau de participação nessas actividades. (6 para elevado e 1 para baixo)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

D7) Caracterize a sua participação nas acções de sensibilização para a problemática da segurança da informação?

☐ Não teve conhecimento de qualquer acção	☐ Não quis participar
☐ Não teve possibilidade de participar	☐ Participou com interesse
☐ Não foi convidado(a) a participar	☐ Participou sem interesse

D8) Já presenciou alguma(s) violação(ões) da segurança do Sistema Informático do Serviço (por exemplo destruição/roubo de equipamentos, entradas em locais interditos, utilização de ficheiros/passwords de outras pessoas, etc.)?

☐ Não ☐ Sim Se respondeu NÃO, passe para a questão D10).

D9) Que atitude tomou quando presenciou essa(s) violação(ões)? (assinale todos os itens aplicáveis)

☐ Advertiu o(a) infractor(a)	☐ Comentou com os(as) seus(suas) colegas
☐ Informou o(a) responsável do Serviço	☐ Nenhuma
☐ Propôs medidas para resolução do problema	

D10) Após o login no acesso ao Sistema Informático, existe definido algum tempo limite para que a sessão de trabalho esteja activa?

☐ Não ☐ Não sabe ☐ Sim

D11) Durante o tempo em que tem activa a sua sessão de trabalho, utiliza algum mecanismo de protecção de ecrã para quando não está a utilizar o computador?

☐ Não ☐ Sim

D12) Além da password que mecanismo/ferramenta/software é utilizado para protecção do Sistema Informático do Serviço? (assinale todos os itens aplicáveis)

☐ Nenhum	☐ Encriptação das comunicações
☐ Firewall	☐ Sistema de Detecção de Intrusões
☐ Antivirus	☐ Outros
☐ Antispyware	

55905



D13) Com que frequência se actualiza esse mecanismo/ferramenta/software? (assinale todos os itens aplicáveis)

☐ Sempre que existe uma actualização ☐ Semestralmente/Anualmente
☐ Mensalmente/Trimestralmente ☐ Nunca se actualiza

D14) Está implementada alguma política de cópias de segurança da informação contida nos servidores?

☐ Não ☐ Sim **Se respondeu NÃO, passe para a questão D20).**

D15) Essa política de cópias de segurança da informação estabelece regras em função da criticidade da informação?

☐ Não ☐ Sim **Se respondeu NÃO, passe para a questão D17).**

D16) Caracterize essas regras para as cópias de segurança?

☐ A totalidade da informação
☐ A totalidade da informação, com periodicidades distintas em função da criticidade
☐ Apenas a informação crítica

D17) Com que periodicidade são efectuadas as cópias de segurança da informação crítica? (assinale todos os itens aplicáveis)

☐ Não sabe ☐ Mensalmente
☐ Sempre que necessário ☐ Trimestralmente
☐ Diariamente ☐ Raramente
☐ Semanalmente

D18) Que tipo de dispositivo é utilizado para efectuar as cópias de segurança? (assinale todos os itens aplicáveis)

☐ Disco do servidor ☐ Disco óptico
☐ Disco externo ☐ Disquete
☐ CD/DVD ☐ Tape

D19) Onde são guardadas as cópias de segurança efectuadas.

☐ Não sabe ☐ Em outro espaço do Serviço
☐ Na sala dos servidores ☐ Fora do Serviço

D20) Existem registos do hardware e software existente no Serviço?

☐ Não ☐ Sim **Se respondeu NÃO, passe para a questão D22).**

D21) Com que periodicidade são actualizados esses registos?

☐ Não sabe ☐ Mensalmente
☐ Sempre que necessário ☐ Trimestralmente
☐ Diariamente ☐ Raramente
☐ Semanalmente

D22) Classifique a segurança do Sistema Informático do Serviço.
(6 para muito seguro e 1 para pouco seguro)

	1	2	3	4	5	6
	☐	☐	☐	☐	☐	☐

D23) Classifique, relativamente à segurança do Sistema Informático do Serviço (6 para muito importante e 1 para pouco importante), os seguintes aspectos:

	1	2	3	4	5	6
(a) Pessoas	☐	☐	☐	☐	☐	☐
(b) Leis/Políticas/Regulamentos/Procedimentos	☐	☐	☐	☐	☐	☐
(c) Computadores Pessoais (Hardware)	☐	☐	☐	☐	☐	☐
(d) Periféricos (Impressoras, Scanners, etc.)	☐	☐	☐	☐	☐	☐
(e) Servidores (Hardware)	☐	☐	☐	☐	☐	☐
(f) Software aplicacional	☐	☐	☐	☐	☐	☐
(g) Sistemas Operativos	☐	☐	☐	☐	☐	☐
(h) Internet	☐	☐	☐	☐	☐	☐
(i) Correio electrónico	☐	☐	☐	☐	☐	☐
(j) Rede informática	☐	☐	☐	☐	☐	☐
(k) Sistema de comunicações (telefones, telefaxes, etc.)	☐	☐	☐	☐	☐	☐

D24) Classifique em que medida considera que a segurança do Sistema Informático do Serviço é ou pode ser importante para as suas actividades laborais. (6 para muito importante e 1 para pouco importante)

	1	2	3	4	5	6
	☐	☐	☐	☐	☐	☐

D25) Classifique a facilidade de acesso físico ao Sistema Informático do Serviço (6 para muito difícil e 1 para muito fácil), nos seguintes pontos de acesso:

	1	2	3	4	5	6
(a) Sala de servidores	☐	☐	☐	☐	☐	☐
(b) Serviços de Informática	☐	☐	☐	☐	☐	☐
(c) Serviços administrativos/académicos/etc.	☐	☐	☐	☐	☐	☐
(d) Gabinetes de colegas	☐	☐	☐	☐	☐	☐
(e) Salas de reunião	☐	☐	☐	☐	☐	☐
(f) Átrios/corredores	☐	☐	☐	☐	☐	☐
(g) Área circundante do Serviço	☐	☐	☐	☐	☐	☐
(h) Laboratórios de Informática	☐	☐	☐	☐	☐	☐



D26) Nos locais onde tem acesso ao Sistema Informático do Serviço, especifique que actividades estão proibidas.
(assinale todos os itens aplicáveis)

☐ Fumar	☐ Movimentar computadores instalados
☐ Ingerir bebidas	☐ Instalar/Movimentar periféricos
☐ Consumir alimentos	☐ Participar em sessões de chat
☐ Realizar cópias dos seus trabalhos	☐ Efectuar o download de ficheiros
☐ Realizar cópias dos programas instalados	☐ Instalar/desinstalar software

D27) Classifique, de acordo com o Impacto na segurança do Sistema Informático do Serviço (6 para muito importante e 1 para pouco importante), os seguintes tipos de ameaças:

	1	2	3	4	5	6
(a) Acidentes naturais (incêndios, terremotos, inundações, etc.)	☐	☐	☐	☐	☐	☐
(b) Hackers (acessos não autorizados a partir do exterior das organizações)	☐	☐	☐	☐	☐	☐
(c) Acessos indevidos (não autorizados) a partir do interior das organizações	☐	☐	☐	☐	☐	☐
(d) Virus/Trojan Horses/Worms/etc.	☐	☐	☐	☐	☐	☐
(e) Roubo de informação	☐	☐	☐	☐	☐	☐
(f) Destruição de informação	☐	☐	☐	☐	☐	☐
(g) Utilização incorrecta do sistema	☐	☐	☐	☐	☐	☐
(h) Definição por defeito das passwords iniciais (por ex. Password igual ao UserID)	☐	☐	☐	☐	☐	☐
(i) Intercepção de mensagens de correio electrónico e respectivos anexos	☐	☐	☐	☐	☐	☐
(j) Falhas no fornecimento de energia eléctrica ao sistema	☐	☐	☐	☐	☐	☐
(k) Configuração incorrecta da firewall	☐	☐	☐	☐	☐	☐
(l) Falhas de funcionamento do software do sistema	☐	☐	☐	☐	☐	☐
(m) Falhas de funcionamento do hardware do sistema	☐	☐	☐	☐	☐	☐

E - Usabilidade do Sistema Informático do Serviço

Por **usabilidade** em sistemas informáticos entende-se a extensão até onde um sistema pode ser usado por utilizadores específicos para atingir objectivos especificados com eficácia, eficiência e satisfação num contexto de uso especificado [ISO 9241-11 *Requisitos ergonómicos para sistemas de trabalho com terminais de visualização - Orientação em usabilidade*], encontrando-se associada directamente à facilidade de utilização e aprendizagem de um sistema.

E1) Recebeu formação na utilização do Sistema Informático do Serviço?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão E3).

E2) Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

E3) São proporcionadas acções de formação sobre a utilização do Sistema Informático do Serviço aos utilizadores finais?

☐ Não ☐ Sim

Se respondeu NÃO, passe para a questão E5).

E4) Com que frequência são realizadas essas acções?

☐ Uma única vez ☐ Semestralmente
☐ Sempre que existem mudanças no sistema ☐ Anualmente
☐ Trimestralmente ☐ Ocasionalmente

E5) São elaborados alguns documentos acerca da utilização do Sistema Informático do Serviço para apoio aos utilizadores finais?

☐ Não ☐ Sim

E6) Classifique a facilidade de utilização do Sistema Informático do Serviço. (6 para fácil de utilizar e 1 para difícil de utilizar)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

E7) Classifique a facilidade de aprendizagem do Sistema Informático do Serviço. (6 para fácil de aprender e 1 para difícil de aprender)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

E8) Classifique, relativamente à usabilidade do Sistema Informático do Serviço (6 para muito importante e 1 para pouco importante), a relevância dos seguintes aspectos:

	1	2	3	4	5	6
(a) Facilidade de acesso	☐	☐	☐	☐	☐	☐
(b) Disponibilidade	☐	☐	☐	☐	☐	☐
(c) Adequação às necessidades	☐	☐	☐	☐	☐	☐
(d) Apoio técnico à utilização	☐	☐	☐	☐	☐	☐
(e) Interface com o sistema	☐	☐	☐	☐	☐	☐
(f) Regras de utilização	☐	☐	☐	☐	☐	☐
(g) Conhecimento prévio do sistema	☐	☐	☐	☐	☐	☐
(h) Participação no desenvolvimento/implementação do sistema	☐	☐	☐	☐	☐	☐

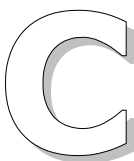
E9) Classifique em que medida considera que a usabilidade do Sistema Informático do Serviço é ou pode ser importante para as suas actividades laborais. (6 para muito importante e 1 para pouco importante)

1 2 3 4 5 6
☐ ☐ ☐ ☐ ☐ ☐

Julho de 2007

Obrigado pela sua colaboração!





Modelo das instruções de entrega dos questionários

Atendendo essencialmente à especificidade dos Serviços/Escolas onde vão ser distribuídos os questionários, entende-se como pertinente definir um modelo (apresentado a seguir) de documento de acompanhamento do questionário, com o contexto em que se enquadram as questões colocadas e instruções de entrega do mesmo após preenchimento.

Caro(a) Colega,

No actual contexto social e organizacional, onde a informação assume um papel de crescente relevância e é assumida como um dos mais importantes activos para a actividade da generalidade das organizações, em conjunto com as pessoas, torna-se essencial perceber como a informação é utilizada para a criação de valor nas organizações, particularmente quando é colocada em causa a sua confidencialidade, integridade e disponibilidade.

Tendo como objectivo suportar os trabalhos de investigação do meu doutoramento, pretendo analisar a percepção das Pessoas acerca da utilização dos Sistemas de Informação e das Tecnologias de Informação e Comunicação, assim como da sua percepção acerca da Segurança da Informação.

Por entender que a utilização dos Sistemas de Informação e das Tecnologias de Informação e Comunicação, assim como a forma como é assegurada a segurança da informação que suportam, deve corresponder às expectativas e às necessidades das pessoas, considero que a sua perspectiva é importante para o trabalho a desenvolver, solicito-lhe por isso que preencha o questionário em anexo (não devolva este documento, apenas o questionário) e que o deposite {identificação do local em que deve ser depositado e/ou entregue o questionário depois de preenchido}.

Na medida do possível, agradeço que proceda ao seu preenchimento e devolução no espaço de uma semana a partir da data da sua recepção.

Atendendo a que se pretende garantir a privacidade dos(as) inquiridos(as) e o seu anonimato, agradeço que em nenhuma parte do questionário coloque qualquer nome ou número que possibilite a sua identificação.

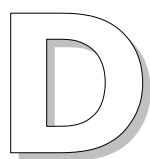
Obrigado pela sua colaboração,

José Manuel Gaivéo

Professor Adjunto

Departamento de Sistemas de Informação

Escola Superior de Ciências Empresariais



Resultados do Questionário – Grupo de Teste

Os resultados aqui apresentados correspondem às respostas dos alunos que constituíram o grupo de teste para a elaboração do modelo final do questionário, cujos resultados são apresentados no capítulo 8.

Grupo A – Identificação/Caracterização do(a) inquirido(a)

A1 - Escalão etário		
	nº	%
Menos de 20 anos	4	5,13
Entre 20 anos e 30 anos	72	92,31
Mais de 30 anos	2	2,56
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

A2 - Área de residência		
	nº	%
Concelho de Setúbal	38	48,72
Fora do Concelho de Setúbal	39	50,00
<i>Não Responderam</i>	1	1,28
Total de Respostas	78	

A3 - Trabalhador-Estudante		
	nº	%
Não	69	88,46
Sim	9	11,54
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

A4 - Ano do curso em que está matriculado(a)		
	nº	%
1º Ano (1ª Vez)	18	23,08
1º Ano	0	0,00
2º Ano	23	29,49
3º Ano	15	19,23
4º Ano	21	26,92
<i>Não Responderam</i>	1	1,28
Total de Respostas	78	

Grupo B – Computador pessoal

B1 - A quantos computadores possui acesso na sua residência?		
	nº	%
Nenhum	0	0,00
1	29	37,18
2	35	44,87
3 ou mais	14	17,95
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

B2 - O computador pessoal a que acede é um portátil?		
	nº	%
Não	37	47,44
Sim	41	52,56
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

B3 - Acede à Internet com o seu computador pessoal?		
	nº	%
Não	2	2,56
Sim	76	97,44
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

B4 - Especifique em que locais acede à Internet com o seu computador pessoal? (assinale todos os itens aplicáveis)		
	nº	%
Residência	73	96,05
Residência de colegas/amigos(as)	27	35,53
Escola/Serviço	52	68,42
Cafés/Restaurantes/etc.	5	6,58
Outros locais	7	9,21
<i>Não Responderam</i>	0	0,00
Total de Respostas	76	

B5 - Com quantas pessoas partilha a utilização do computador pessoal na sua residência?		
	nº	%
Nenhuma	21	27,63
1	19	25,00
2	23	30,26
3 ou mais	12	15,79
<i>Não Responderam</i>	1	1,32
Total de Respostas	76	

B6 - Com que frequência acede à Internet com o seu computador pessoal?		
	nº	%
Todos os dias	68	89,47
Quase todos os dias	7	9,21
Pelo menos uma vez por semana	1	1,32
Pelo menos uma vez por mês	0	0,00
Uma ou duas vezes por semestre	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	76	

B7 - Durante esses acessos à Internet, qual o tempo médio diário de utilização?		
	nº	%
Até 1 hora	6	7,89
Entre 1 e 3 horas	34	44,74
Mais de 3 horas	36	47,37
<i>Não Responderam</i>	0	0,00
Total de Respostas	76	

B8 - Classifique a segurança do seu acesso? (6 para muito seguro e 1 para pouco seguro)		
	nº	%
1	0	0,00
2	1	1,32
3	8	10,53
4	22	28,95
5	32	42,11
6	12	15,79
<i>Não Responderam</i>	1	1,32
Total de Respostas	76	

B9 - Identifique a solução que adoptou para acesso à Internet com o seu computador pessoal.		
	nº	%
Modem	11	14,47
ADSL	14	18,42
Cabo	41	53,95
<i>Wireless</i>	9	11,84
Outra	1	1,32
<i>Não Responderam</i>	0	0,00
Total de Respostas	76	

B10 - Possui <i>password</i> para acesso ao seu computador pessoal?		
	nº	%
Não	42	53,85
Sim	33	42,31
<i>Não Responderam</i>	3	3,85
Total de Respostas	78	

B11 - Com quantas pessoas partilha a sua <i>password</i> ?		
	nº	%
Nenhuma	23	63,89
1	4	11,11
2 ou 3	7	19,44
Mais de 3	2	5,56
<i>Não Responderam</i>	0	0,00
Total de Respostas	36	

B12 - Já alterou a <i>password</i> de acesso ao seu computador pessoal?		
	nº	%
Não	16	44,44
Sim	18	50,00
<i>Não Responderam</i>	2	5,56
Total de Respostas	36	

B13 - Com que frequência altera a <i>password</i> de acesso ao seu computador pessoal?		
	nº	%
Uma única vez	2	10,00
Raramente	8	40,00
Semestralmente/Anualmente	7	35,00
Mensalmente/Trimestralmente	2	10,00
<i>Não Responderam</i>	1	5,00
Total de Respostas	20	

B14 - Que opções efectua na escolha da sua nova <i>password</i> ? (assinale todos os itens aplicáveis)		
	nº	%
Datas de nascimento/aniversário	3	15,00
Nomes de familiares	3	15,00
Nomes de locais	0	0,00
Nomes de animais de estimação	2	10,00
Apenas números	4	20,00
Apenas letras	6	30,00
Combinação de números e letras	11	55,00
Escolha aleatória de caracteres	1	5,00
<i>Não Responderam</i>	1	5,00
Total de Respostas	20	

B15 - Na definição de nova <i>password</i> opta por:		
	nº	%
Nº máx. de caracteres permitido	4	20,00
Nº fixo de caracteres, entre máximo e mínimo	5	25,00
Nº aleatório de caracteres, entre máximo e mínimo	8	40,00
Nº mín. de caracteres permitido	2	10,00
<i>Não Responderam</i>	1	5,00
Total de Respostas	20	

B16 - Classifique o grau de segurança da sua <i>password</i> . (6 para elevado e 1 para baixo)			
	nº	%	
1	0	0,00	
2	0	0,00	
3	5	13,89	
4	9	25,00	
5	13	36,11	
6	8	22,22	
	<i>Não Responderam</i>	1	2,78
Total de Respostas		36	

B17 - Qual o processo que utiliza para guardar a sua <i>password</i> ? (<i>assinale todos os itens aplicáveis</i>)		
	nº	%
Memorização	32	88,89
Memória do telemóvel	2	5,56
<i>Post-it</i>	0	0,00
Registo na agenda pessoal	0	0,00
Outro	4	11,11
<i>Não Responderam</i>	1	2,78
Total de Respostas	36	

B18 - Além da <i>password</i> que mecanismo/ferramenta/ <i>software</i> utiliza para protecção do seu computador pessoal? (<i>assinale todos os itens aplicáveis</i>)		
	nº	%
Nenhum	2	2,56
<i>Firewall</i> (<i>software/hardware</i> para controlo do tráfego da rede informática, etc.)	61	78,21
Antivírus (<i>software</i> destinado à detecção de vírus, entendidos em termos genéricos, e à sua eliminação)	72	92,31
<i>Antispyware</i> (<i>software</i> destinado à detecção de programas intrusivos)	48	61,54
Outros	8	10,26
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

B19 - Com que frequência actualiza esse mecanismo/ferramenta/software? (assinale todos os itens aplicáveis)		
	nº	%
Sempre que existe uma actualização	66	84,62
Mensalmente/Trimestralmente	5	6,41
Semestralmente/Anualmente	2	2,56
Nunca actualiza	5	6,41
Não Responderam	1	1,28
Total de Respostas	78	

B20 - Efectua cópias de segurança (<i>backups</i>) da informação contida no seu computador pessoal?		
	nº	%
Não	30	38,46
Sim	46	58,97
<i>Não Responderam</i>	2	2,56
Total de Respostas	78	

B21 - Com que periodicidade efectua cópias de segurança (<i>backups</i>)? (<i>assinale todos os itens aplicáveis</i>)		
	nº	%
No final de cada sessão de trabalho	4	8,33
Na conclusão de cada projecto/trabalho/etc.	6	12,50
Diariamente	3	6,25
Semanalmente	5	10,42
Mensalmente	8	16,67
Trimestralmente	12	25,00
Raramente	10	20,83
<i>Não Responderam</i>	2	4,17
Total de Respostas	48	

B22 - Especifique a opção mais frequente para realização das cópias de segurança (<i>backups</i>)?		
	nº	%
Apenas os ficheiros alterados	8	16,67
A totalidade da informação no disco	6	12,50
Um conjunto de ficheiros pré-definidos	4	8,33
Apenas os ficheiros considerados importantes	30	62,50
<i>Não Responderam</i>	0	0,00
Total de Respostas	48	

B23 - Que tipo de dispositivo utiliza para efectuar as cópias de segurança (<i>backups</i>)? (<i>assinale todos os itens aplicáveis</i>)		
	nº	%
Disco do computador	19	39,58
Disco externo	11	22,92
CD/DVD	40	83,33
Memória <i>flash</i> amovível	23	47,92
Disquete	1	2,08
Tape	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	48	

B24 - Especifique onde guarda as cópias de segurança (<i>backups</i>) que efectua.		
	nº	%
Na mesma sala onde se encontra o computador	31	64,58
Em outro espaço da sua residência	17	35,42
Fora da sua residência	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	48	

B25 - Classifique o grau de segurança do seu computador pessoal. (6 para elevado e 1 para baixo)		
	nº	%
1	0	0,00
2	1	1,28
3	14	17,95
4	24	30,77
5	29	37,18
6	10	12,82
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

B26 - Com que frequência utiliza o seu computador pessoal?		
	nº	%
Todos os dias	70	89,74
Quase todos os dias	7	8,97
Pelo menos uma vez por semana	1	1,28
Pelo menos uma vez por mês	0	0,00
Uma ou duas vezes por semestre	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

B27 - Caracterize a sua utilização do seu computador pessoal. (assinale todos os itens aplicáveis)		
	nº	%
Elaboração de relatórios e outros trabalhos	71	91,03
Impressão de documentos	60	76,92
Trabalhos escolares	76	97,44
Jogos	57	73,08
Pesquisas na Internet	76	97,44
Envio/recepção de correio electrónico	70	89,74
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

B28 - Durante a utilização do seu computador pessoal, qual o tempo médio diário de utilização?		
	nº	%
Até 1 hora	2	2,56
Entre 1 e 3 horas	35	44,87
Mais de 3 horas	41	52,56
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

B29 - Que tipo de <i>software</i> utiliza no seu computador pessoal? (<i>assinale todos os itens aplicáveis</i>)		
	nº	%
Sistema Operativo Windows	76	97,44
Outro Sistema Operativo	7	8,97
Processador de Texto (por ex. Word)	69	88,46
Folha de Cálculo (por ex. Excel)	63	80,77
Base de Dados (por ex. Access)	41	52,56
Outros aplicativos	51	65,38
	<i>Não Responderam</i>	1
	Total de Respostas	78

Grupo C – Sistema Informático da Escola

C1 - Desde a sua entrada na Escola existiu alguma mudança no Sistema Informático (<i>Hardware, Software, Procedimentos, etc.</i>)?		
	nº	%
Não	33	42,31
Sim	45	57,69
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C2 - Foi solicitada a sua participação/participou de alguma forma nessas mudanças?		
	nº	%
Não	43	95,56
Sim	2	4,44
<i>Não Responderam</i>	0	0,00
Total de Respostas	45	

C3 - Caracterize a sua participação nessas mudanças. (<i>assinale todos os itens aplicáveis</i>)		
	nº	%
Análise de documentos	1	33,33
Preenchimento de inquéritos/questionários	1	33,33
Resposta a entrevistas	0	0,00
Elaboração de pareceres	0	0,00
<i>Não Responderam</i>	1	33,33
Total de Respostas	3	

C4 - Classifique o seu grau de participação nessas mudanças. (6 para elevado e 1 para baixo)		
	nº	%
1	0	0,00
2	1	33,33
3	0	0,00
4	0	0,00
5	0	0,00
6	1	33,33
<i>Não Responderam</i>	1	33,33
Total de Respostas	3	

C5 - Classifique o seu grau de satisfação com as mudanças efectuadas. (6 para elevado e 1 para baixo)		
	nº	%
1	0	0,00
2	3	6,67
3	3	6,67
4	22	48,89
5	12	26,67
6	2	4,44
<i>Não Responderam</i>	3	6,67
Total de Respostas	45	

C6 - Classifique a sua percepção acerca do funcionamento do Sistema Informático depois das mudanças efectuadas. (6 para melhorou muito e 1 para não melhorou)		
	nº	%
1	1	2,22
2	2	4,44
3	4	8,89
4	17	37,78
5	17	37,78
6	2	4,44
<i>Não Responderam</i>	2	4,44
Total de Respostas	45	

C7 - Já tinha utilizado computadores antes de ser colocado(a) no Ensino Superior?		
	nº	%
Não	0	0,00
Sim	78	100,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C8 - Realizou algum curso de formação em Informática/Sistemas de Informação antes de se matricular no Ensino Superior?		
	nº	%
Não	45	57,69
Sim	32	41,03
Não Responderam	1	1,28
Total de Respostas	78	

C9 - Classifique o seu grau de conhecimentos na área da Informática/Sistemas de Informação. (6 para elevado e 1 para baixo)		
	nº	%
1	0	0,00
2	2	2,56
3	4	5,13
4	37	47,44
5	23	29,49
6	12	15,38
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C10 - Dispõe de acesso ao Sistema Informático da Escola?		
	nº	%
Não	0	0,00
Sim	78	100,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C11 - O acesso ao Sistema Informático da Escola é feito através de <i>password</i> ?		
	nº	%
Não	0	0,00
Sim	77	98,72
<i>Não Responderam</i>	1	1,28
Total de Respostas	78	

C12 - Já alterou a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático da Escola?		
	nº	%
Não	21	26,92
Sim	56	71,79
<i>Não Responderam</i>	1	1,28
Total de Respostas	78	

C13 - Com que frequência altera a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático da Escola?		
	nº	%
Uma única vez	27	47,37
Raramente	22	38,60
Semestralmente/Anualmente	7	12,28
Mensalmente/Trimestralmente	1	1,75
<i>Não Responderam</i>	0	0,00
Total de Respostas	57	

C14 - Que opções efectua na escolha de nova(s) <i>password(s)</i> ? (assinale todos os itens aplicáveis)		
	nº	%
Datas de nascimento/aniversário	8	14,04
Nomes de familiares	4	7,02
Nomes de locais	9	15,79
Nomes de animais de estimação	4	7,02
Apenas números	6	10,53
Apenas letras	14	24,56
Combinação de números e letras	35	61,40
Escolha aleatória de caracteres	11	19,30
<i>Não Responderam</i>	0	0,00
Total de Respostas	57	

C15 - Na definição de nova(s) <i>password(s)</i> opta por:		
	nº	%
Número máximo de caracteres permitido	7	12,28
Número fixo de caracteres, entre máximo e mínimo	5	8,77
Número aleatório de caracteres, entre máximo e mínimo	36	63,16
Número mínimo de caracteres permitido	8	14,04
<i>Não Responderam</i>	1	1,75
Total de Respostas	57	

C16 - Qual o processo que utiliza para guardar a(s) sua(s) <i>password(s)</i> ? (assinale todos os itens aplicáveis)		
	nº	%
Memorização	71	91,03
Memória do telemóvel	6	7,69
<i>Post-it</i>	1	1,28
Registo na agenda pessoal	1	1,28
Outro	4	5,13
<i>Não Responderam</i>	2	2,56
Total de Respostas	78	

C17 - Com quantas pessoas partilha a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático da Escola?		
	nº	%
Nenhuma	61	78,21
1	6	7,69
2 ou 3	5	6,41
Mais de 3	6	7,69
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C18 - Utiliza a mesma <i>password</i> para diversas aplicações/sistemas?		
	nº	%
Não	23	29,49
Sim	55	70,51
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C19 - Classifique o grau de segurança da(s) sua(s) <i>password(s)</i> . (6 para elevado e 1 para baixo)		
	nº	%
1	3	3,85
2	1	1,28
3	9	11,54
4	25	32,05
5	23	29,49
6	16	20,51
<i>Não Responderam</i>	1	1,28
Total de Respostas	78	

C20 - Além da <i>password</i> , especifique que tipo(s) de mecanismo(s) está(ão) implementado(s) para acesso ao Sistema Informático da Escola. (<i>assinale todos os itens aplicáveis</i>)		
	nº	%
Cartão magnético	1	1,28
Cartão com <i>microchip</i>	0	0,00
Chave metálica	0	0,00
Controlo biométrico	0	0,00
Identificação pessoal	31	39,74
Nenhum	45	57,69
<i>Não Responderam</i>	2	2,56
Total de Respostas	78	

C21 - Possui algum endereço de correio electrónico associado ao Sistema Informático da Escola?		
	nº	%
Não	43	55,13
Sim	33	42,31
<i>Não Responderam</i>	2	2,56
Total de Respostas	78	

C22 - Além desse, quantos endereços de correio electrónico possui?		
	nº	%
Nenhum	3	8,57
1	2	5,71
2	15	42,86
3	6	17,14
Mais de 3	9	25,71
<i>Não Responderam</i>	0	0,00
Total de Respostas	35	

C23 - Utiliza a mesma <i>password</i> para acesso ao correio electrónico e ao Sistema Informático da Escola?		
	nº	%
Não	24	68,57
Sim	11	31,43
<i>Não Responderam</i>	0	0,00

C24 - Existe implementado algum sistema de filtragem de mensagens de correio electrónico?		
	nº	%
Não	4	11,43
Não sabe	17	48,57
Sim	14	40,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	35	

C25 - Com que frequência acede ao Sistema Informático da Escola?		
	nº	%
Todos os dias	11	14,10
Quase todos os dias	28	35,90
Pelo menos uma vez por semana	26	33,33
Pelo menos uma vez por mês	11	14,10
Uma ou duas vezes por semestre	2	2,56
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C26 - Durante a utilização do Sistema Informático da Escola, qual o tempo médio diário de cada utilização?		
	nº	%
Até 1 hora	42	53,85
Entre 1 e 3 horas	30	38,46
Entre 3 e 5 horas	4	5,13
Mais de 5 horas	2	2,56
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C27 - Que tipo de <i>software</i> utiliza? (<i>assinale todos os itens aplicáveis</i>)		
	nº	%
Sistema Operativo Windows 95/98/2000/XP	77	98,72
Sistema Operativo Windows Server	7	8,97
Sistema Operativo Linux	5	6,41
Outro Sistema Operativo	2	2,56
Processador de Texto	58	74,36
Folha de Cálculo	49	62,82
Base de Dados	41	52,56
Programação	50	64,10
Auditoria/Controlo de qualidade	0	0,00
Desenho técnico	15	19,23
Análise de Sistemas	21	26,92
Outros	16	20,51
<i>Não Responderam</i>	1	1,28
Total de Respostas	78	

C28 - Caracterize a sua utilização do Sistema Informático da Escola. (<i>assinale todos os itens aplicáveis</i>)		
	nº	%
Elaboração de relatórios e outros trabalhos	52	66,67
Impressão de documentos	61	78,21
Trabalhos escolares	67	85,90
Jogos	14	17,95
Pesquisas na Internet	66	84,62
Envio/recepção de correio electrónico	47	60,26
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C29 - Utiliza alguma área de trabalho privada no(s) servidor(es) do Sistema Informático da Escola?		
	nº	%
Não	24	30,77
Sim	54	69,23
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C30 - Que tipo de informação guarda nessa área de trabalho?		
	nº	%
Ficheiros de trabalho	43	79,63
Ficheiros pessoais	0	0,00
Ambos	10	18,52
<i>Não Responderam</i>	1	1,85
Total de Respostas	54	

C31 - Já perdeu informação guardada nessa área de trabalho?		
	nº	%
Não	49	90,74
Sim	4	7,41
<i>Não Responderam</i>	1	1,85
Total de Respostas	54	

C32 - Que acção tomou para recuperar essa informação?		
	nº	%
Expôs a situação aos serviços de informática	2	40,00
Tentou recuperar a informação	0	0,00
Nenhuma	2	40,00
<i>Não Responderam</i>	1	20,00
Total de Respostas	5	

C33 - O que aconteceu relativamente a essa situação? (assinale todos os itens aplicáveis)		
	nº	%
A informação foi reposta de <i>backups</i> anteriores	0	0,00
A informação foi recuperada mas não sabe como	0	0,00
A informação não foi recuperada	2	40,00
Recebeu comunicação de que era impossível recuperar a informação	2	40,00
Não sabe nada acerca da situação	1	20,00
<i>Não Responderam</i>	1	20,00
Total de Respostas	5	

C34 - Possui acesso à impressão de documentos através do Sistema Informático da Escola utilizando impressora(s) partilhada(s)?		
	nº	%
Não	3	3,85
Sim	75	96,15
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

C35 - Quando não consegue imprimir documentos através da(s) impressora(s) partilhada(s) qual a atitude que assume? (assinale todos os itens aplicáveis)		
	nº	%
Cancela de imediato o trabalho	34	45,33
Tenta imprimir novamente	41	54,67
Tenta imprimir numa impressora disponível	48	64,00
Altera a configuração de acesso à impressora	11	14,67
Informa os serviços de informática	28	37,33
Nenhuma	3	4,00
<i>Não Responderam</i>	1	1,33
Total de Respostas	75	

C36 - Que atitude toma quando encontra documentos que não são seus na(s) impressora(s) partilhada(s)? (assinale todos os itens aplicáveis)		
	nº	%
Nunca encontrou	25	33,33
Lê o documento (todo ou parte)	7	9,33
Entrega aos serviços de informática	5	6,67
Tenta entregar/entregou ao seu proprietário	26	34,67
Deita fora ou distroi o documento	17	22,67
Guarda para seu uso pessoal	2	2,67
Nenhuma	11	14,67
<i>Não Responderam</i>	1	1,33
Total de Respostas	75	

C37 - Que atitude toma quando não encontra documentos seus que mandou imprimir na(s) impressora(s) partilhada(s)? (assinale todos os itens aplicáveis)		
	nº	%
Nunca aconteceu	42	56,00
Informou os serviços de informática	5	6,67
Imprimiu novamente o documento	25	33,33
Tentou encontrar o documento	12	16,00
Nenhuma	2	2,67
<i>Não Responderam</i>	1	1,33
Total de Respostas	75	

C38 - Consideraria a hipótese de aceder ao Sistema Informático da Escola a partir da sua residência ou de outro local onde trabalhe regularmente?			
	nº	%	
Não	8	10,26	
Sim	57	73,08	
Talvez	13	16,67	
	<i>Não Responderam</i>	0	0,00
	Total de Respostas	78	

Grupo D – Segurança da Informação no Sistema Informático da Escola

D1 - Existem políticas (normas/regulamentos/regras/procedimentos) de segurança do Sistema Informático da Escola?		
	nº	%
Não	1	1,28
Não sabe	33	42,31
Sim	44	56,41
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

D2 - Como tomou conhecimento dessas políticas (normas/regulamentos/regras/procedimentos)? (assinale todos os itens aplicáveis)		
	nº	%
Entrega no acto de matrícula	12	27,27
Entrega pelos serviços de informática	8	18,18
Informação verbal dos serviços de informática	12	27,27
Informação afixada na Escola	12	27,27
Consulta da página <i>web</i> da Escola	4	9,09
Informação de colega	14	31,82
Outro meio	11	25,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	44	

D3 - Dos aspectos a seguir mencionados, especifique quais são abrangidos pelas políticas (normas/regulamentos/regras/procedimentos) definidas. (assinale todos os itens aplicáveis)		
	nº	%
Definição de acessos ao sistema (<i>password</i>)	41	93,18
Utilização do correio electrónico	24	54,55
Utilização da Internet	21	47,73
Utilização dos recursos de <i>hardware</i>	17	38,64
Acesso aos servidores	11	25,00
Realização de cópias de segurança (<i>backups</i>)	5	11,36
Instalação de <i>software</i>	16	36,36
Plano de Recuperação de Acidentes	6	13,64
<i>Não Responderam</i>	0	0,00
Total de Respostas	44	

D4 - Participou na elaboração/alteração dessas políticas (normas/regulamentos/regras/procedimentos)?		
	nº	%
Não	44	100,00
Sim	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	44	

D5 - Caracterize a sua participação nessas actividades. (assinale todos os itens aplicáveis)		
	nº	%
Análise de documentos	0	0,00
Preenchimento de inquéritos/questionários	0	0,00
Resposta a entrevistas	0	0,00
Elaboração de pareceres	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	0	

D6 - Classifique o seu grau de participação nessas actividades. (6 para elevado e 1 para baixo)		
	nº	%
1	0	0,00
2	0	0,00
3	0	0,00
4	0	0,00
5	0	0,00
6	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	0	

D7 - Caracterize a sua participação nas acções de sensibilização para a problemática da segurança da informação?		
	nº	%
Não teve conhecimento de qualquer acção	66	84,62
Não foi convidado(a) a participar	8	10,26
Não quis participar	1	1,28
Participou com interesse	3	3,85
Participou sem interesse	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

D8 - Já presenciou alguma(s) violação(ões) da segurança do Sistema Informático da Escola (por exemplo destruição/ roubo de equipamentos, entradas em locais interditos, utilização de ficheiros/passwords de outras pessoas, etc.)?		
	nº	%
Não	74	94,87
Sim	4	5,13
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

D9 - Que atitude tomou quando presenciou essa(s) violação(ões)? (assinale todos os itens aplicáveis)		
	nº	%
Informou os serviços de informática	1	25,00
Comentou com os seus colegas	3	75,00
Tentou resolver a situação	0	0,00
Nenhuma	1	25,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	4	

D10 - Após o login no acesso ao Sistema Informático da Escola, existe definido algum tempo limite para que a sessão de trabalho esteja activa?		
	nº	%
Não	42	53,85
Não sabe	31	39,74
Sim	5	6,41
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

D11 - Classifique a segurança do Sistema Informático da Escola. (6 para muito seguro e 1 para pouco seguro)		
	nº	%
1	0	0,00
2	3	3,85
3	8	10,26
4	34	43,59
5	29	37,18
6	4	5,13
<i>Não Responderam</i>	0	0,00
Total de Respostas	78	

D12 - Classifique, relativamente à segurança do Sistema Informático da Escola (6 para muito importante e 1 para pouco importante), os seguintes aspectos:							
	1	2	3	4	5	6	NR
(a) Pessoas	0,00	0,00	14,10	33,33	23,08	29,49	0,00
(b) Leis/Políticas/Regulamentos/Procedimentos	1,28	2,56	11,54	34,62	34,62	15,38	0,00
(c) Computadores Pessoais (<i>Hardware</i>)	0,00	0,00	14,10	41,03	34,62	10,26	0,00
(d) Periféricos (Impressoras, <i>Scanners</i> , etc.)	3,85	7,69	16,67	35,90	21,79	14,10	0,00
(e) Servidores (<i>Hardware/ Software</i>)	0,00	1,28	10,26	32,05	34,62	21,79	0,00
(f) Programas (<i>Software</i>)	0,00	1,28	15,38	33,33	30,77	19,23	0,00
(g) Sistema de comunicações/Rede informática	0,00	1,28	5,13	25,64	37,18	30,77	0,00

D13 - Classifique em que medida considera que a segurança do Sistema Informático da Escola é ou pode ser importante para as suas actividades lectivas. (6 para muito importante e 1 para pouco importante)		
	nº	%
1	0	0,00
2	2	2,56
3	3	3,85
4	15	19,23
5	24	30,77
6	32	41,03
Não Responderam	2	2,56
Total de Respostas	78	

D14 - Classifique a facilidade de acesso físico ao Sistema Informático da Escola (6 para muito difícil e 1 para muito fácil), nos seguintes pontos de acesso:							
	1	2	3	4	5	6	NR
(a) Sala de servidores	5,13	6,41	20,51	14,10	15,38	38,46	0,00
(b) Serviços de Informática	10,26	15,38	23,08	17,95	23,08	10,26	0,00
(c) Serviços administrativos/académicos/etc.	6,41	6,41	26,92	23,08	21,79	15,38	0,00
(d) Laboratórios de Informática	11,54	12,82	21,79	21,79	24,36	7,69	0,00
(e) Salas de informática para alunos	38,46	14,10	12,82	10,26	10,26	14,10	0,00

D15 - Nos locais onde tem acesso ao Sistema Informático da Escola, especifique que actividades estão proibidas. <i>(assinale todos os itens aplicáveis)</i>			
	nº	%	
Fumar	74	94,87	
Ingerir bebidas	65	83,33	
Consumir alimentos	65	83,33	
Realizar cópias dos seus trabalhos	4	5,13	
Realizar cópias dos programas instalados	24	30,77	
Movimentar computadores instalados	57	73,08	
Instalar/Movimentar periféricos	40	51,28	
Participar em sessões de <i>chat</i>	5	6,41	
Efectuar o <i>download</i> de ficheiros	8	10,26	
Instalar/desinstalar <i>software</i>	51	65,38	
	<i>Não Responderam</i>	0	0,00
	Total de Respostas	78	

D16 - Classifique, de acordo com o impacto na segurança do Sistema Informático da Escola (6 para muito importante e 1 para pouco importante), os seguintes tipos de ameaças.							
	1	2	3	4	5	6	NR
(a) Acidentes naturais (incêndios, terremotos, inundações, etc.)	1,28	3,85	19,23	15,38	24,36	29,49	6,41
(b) <i>Hackers</i> (acessos não autorizados a partir do exterior das organizações)	1,28	0,00	10,26	17,95	24,36	38,46	6,00
(c) Acessos indevidos (não autorizados) a partir do interior das organizações	1,32	1,32	10,53	18,42	28,95	30,26	9,21
(d) Roubo de informação	1,28	0,00	10,26	17,95	20,51	43,59	6,41
(e) Destruição de informação	1,28	0,00	6,41	14,10	20,51	51,28	6,41
(f) Utilização incorrecta do sistema	1,28	0,00	11,54	30,77	26,92	24,36	5,13
(g) Definição por defeito das <i>passwords</i> iniciais (por ex. <i>Password</i> igual ao <i>UserID</i>)	1,28	5,13	17,95	24,36	20,51	25,64	5,13
(h) Intercepção de mensagens de correio electrónico e respectivos anexos	2,56	2,56	12,82	21,79	21,79	33,33	5,13
(i) Falhas no fornecimento de energia eléctrica ao sistema	0,00	5,13	11,54	28,21	21,79	28,21	5,13
(j) Falhas de funcionamento do <i>software</i> do sistema	0,00	3,85	19,23	17,95	28,21	25,64	5,13
(k) Falhas de funcionamento do <i>hardware</i> do sistema	1,28	2,56	12,82	23,08	25,64	29,49	5,13

Grupo E – Usabilidade do Sistema Informático da Escola

E1 - Recebeu formação na utilização do Sistema Informático da Escola?		
	nº	%
Não	72	92,31
Sim	4	5,13
<i>Não Responderam</i>	2	2,56
Total de Respostas	78	

E2 - Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)		
	nº	%
1	0	0,00
2	1	16,67
3	1	16,67
4	0	0,00
5	2	33,33
6	0	0,00
<i>Não Responderam</i>	3	50,00
Total de Respostas	6	

E3 - Existe algum(uns) documento(s) acerca da utilização do Sistema Informático da Escola?		
	nº	%
Não	9	11,54
Não sabe	46	58,97
Sim	22	28,21
<i>Não Responderam</i>	1	1,28
Total de Respostas	78	

E4 - Como tomou conhecimento desse(s) documento(s)? (assinale todos os itens aplicáveis)		
	nº	%
Entrega no acto de matrícula	10	43,48
Informação afixada na Escola	10	43,48
Consulta da página <i>web</i> da Escola	4	17,39
Informação de colega	4	17,39
Outro meio	0	0,00
<i>Não Responderam</i>	1	4,35
Total de Respostas	23	

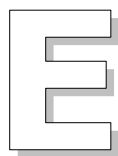
E5 - Classifique a utilidade desse(s) documento(s). (6 para muito útil e 1 para pouco útil)		
	nº	%
1	0	0,00
2	0	0,00
3	6	26,09
4	7	30,43
5	7	30,43
6	2	8,70
<i>Não Responderam</i>	1	4,35
Total de Respostas	23	

E6 - Classifique a facilidade de utilização do Sistema Informático da Escola. (6 para fácil de utilizar e 1 para difícil de utilizar)		
	nº	%
1	1	1,28
2	1	1,28
3	1	1,28
4	9	11,54
5	33	42,31
6	32	41,03
<i>Não Responderam</i>	1	1,28
Total de Respostas	78	

E7 - Classifique a facilidade de aprendizagem do Sistema Informático da Escola. (6 para fácil de aprender e 1 para difícil de aprender)		
	nº	%
1	1	1,28
2	0	0,00
3	1	1,28
4	8	10,26
5	33	42,31
6	34	43,59
<i>Não Responderam</i>	1	1,28
Total de Respostas	78	

E8 - Classifique, relativamente à usabilidade do Sistema Informático da Escola (6 para muito importante e 1 para pouco importante), a relevância dos seguintes aspectos:							
	1	2	3	4	5	6	NR
(a) Facilidade de acesso	0,00	0,00	2,56	15,38	29,49	51,28	1,28
(b) Disponibilidade	0,00	1,28	1,28	12,82	29,49	53,85	1,28
(c) Adequação às necessidades	0,00	1,28	2,56	20,51	41,03	33,33	1,28
(d) Apoio técnico à utilização	1,28	5,13	14,10	17,95	34,62	25,64	1,28
(e) Interface com o sistema	0,00	2,56	10,26	26,92	35,90	23,08	1,28
(f) Regras de utilização	1,28	5,13	16,67	25,64	34,62	15,38	1,28
(g) Manual de utilização	5,13	15,38	20,51	25,64	21,79	10,26	1,28

E9 - Classifique em que medida considera que a usabilidade do Sistema Informático da Escola é ou pode ser importante para as suas actividades lectivas. (6 para muito importante e 1 para pouco importante)		
	nº	%
1	0	0,00
2	1	1,28
3	3	3,85
4	13	16,67
5	17	21,79
6	43	55,13
<i>Não Responderam</i>	1	1,28
Total de Respostas	78	



Resultados dos Questionários tipos A, B e C

Os resultados aqui apresentados correspondem às respostas dos inquiridos aos questionário tipo A, B e C. A análise destes resultados e o estabelecimento de conclusões derivadas da sua apreciação são apresentados nos capítulos 8 e 9 da tese.

Grupo A – Identificação/Caracterização do(a) inquirido(a)

A1) Escalão etário				
	Docentes		Não Docentes	
	nº	%	nº	%
Menos de 30 anos	14	10,22	1	1,27
Entre 30 anos e 45 anos	78	56,93	42	53,16
Mais de 45 anos	45	32,85	36	45,57
<i>Não Responderam</i>	0	0,00	0	0,00
Total de Respostas	137		79	

A1) Escalão etário		
	Técnicos	
	nº	%
Menos de 25 anos	0	0,00
Entre 25 anos e 35 anos	13	92,86
Mais de 35 anos	1	7,14
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

A2) Área de residência						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Concelho de Setúbal	53	38,69	64	81,01	6	42,86
Fora do Concelho de Setúbal	84	61,31	15	18,99	8	57,14
<i>Não Responderam</i>	0	0,00	0	0,00	0	0,00
Total de Respostas	137		79		14	

A3) Antiguidade no IPS/Escola						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Até 5 anos	36	26,28	25	31,65	5	35,71
Mais de 5 anos	100	72,99	51	64,56	9	64,29
<i>Não Responderam</i>	1	0,73	3	3,80	0	0,00
Total de Respostas	137		79		14	

A4) Experiência profissional						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Menos de 2 anos	9	6,57	1	1,27	0	0,00
Entre 2 anos e 5 anos	20	14,60	10	12,66	3	21,43
Mais de 5 anos	108	78,83	68	86,08	11	78,57
<i>Não Responderam</i>	0	0,00	0	0,00	0	0,00
Total de Respostas	137		79		14	

A5) Habilitações Académicas		
	Docentes	
	nº	%
Doutoramento	22	16,06
Mestrado	87	63,50
Licenciatura	28	20,44
<i>Não Responderam</i>	0	0,00
Total de Respostas	137	

A5) Habilitações Académicas		
	Não Docentes	
	nº	%
Mestrado/Licenciatura/Bacharelato	32	40,51
Secundário	45	56,96
Básico	2	2,53
<i>Não Responderam</i>	0	0,00
Total de Respostas	79	

A5) Habilitações Académicas		
	Técnicos	
	nº	%
Mestrado/Licenciatura	12	85,71
Bacharelato	2	14,29
Secundário	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

A6) Área científica de docência		
	Docentes	
	nº	%
Informática; Engenharia Informática; Computadores; Sistemas de Informação; etc.	27	19,71
Outra	109	79,56
<i>Não Responderam</i>	1	0,73
Total de Respostas	137	

A6) Área de formação		
	Técnicos	
	nº	%
Informática/Engenharia Informática	10	71,43
Engenharia Electrónica/Electrotécnica/Computadores/Telecomunicações	2	14,29
Informática de Gestão/Sistemas de Informação/Tecnologias de Informação e Comunicação	1	7,14
Outra	1	7,14
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

A7) Identificação da Escola		
	Docentes	
	nº	%
ESE	24	17,52
ESTSetúbal	33	24,09
ESCE	57	41,61
ESS	15	10,95
ESTBarreiro	8	5,84
<i>Não Responderam</i>	0	0,00
Total de Respostas	137	

A8) Categoria profissional		
	Docentes	
	nº	%
Professor	50	36,50
Equiparado a Professor	32	23,36
Assistente	7	5,11
Equiparado a Assistente	47	34,31
<i>Não Responderam</i>	1	0,73
Total de Respostas	137	

A6) Carreira profissional		
	Não Docentes	
	nº	%
Técnico Superior/Técnico	25	31,65
Assistente Administrativo	31	39,24
Técnico-Profissional	21	26,58
<i>Não Responderam</i>	2	2,53
Total de Respostas	79	

A9) Regime do contrato		
	Docentes	
	nº	%
Dedicação exclusiva	105	76,64
Tempo integral	7	5,11
Tempo parcial	19	13,87
Outro	3	2,19
<i>Não Responderam</i>	3	2,19
Total de Respostas	137	

Grupo B – Computador pessoal

B1) A quantos computadores possui acesso na sua residência?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Nenhum	0	0,00	14	17,72	0	0,00
1	45	32,85	44	55,70	8	57,14
2	55	40,15	17	21,52	3	21,43
3 ou mais	37	27,01	3	3,80	3	21,43
<i>Não Responderam</i>	0	0,00	1	1,27	0	0,00
Total de Respostas	137		79		14	

B2) O computador pessoal a que acede é um portátil?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	36	26,28	35	53,85	9	64,29
Sim	101	73,72	29	44,62	5	35,71
<i>Não Responderam</i>	0	0,00	1	1,54	0	0,00
Total de Respostas	137		65		14	

B3) Acede à Internet com o seu computador pessoal?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	11	8,03	15	23,08	1	7,14
Sim	126	91,97	49	75,38	13	92,86
<i>Não Responderam</i>	0	0,00	1	1,54	0	0,00
Total de Respostas	137		65		14	

B4) Especifique em que locais acede à Internet com o seu computador pessoal? (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Residência	125	99,21	48	96,00	13	100,00
Residência de colegas/amigos(as)	8	6,35	6	12,00	0	0,00
Escola/Serviço	85	67,46	22	44,00	6	46,15
Cafés/Restaurantes/etc.	5	3,97	0	0,00	0	0,00
Outra Instituição de Ensino Superior	31	24,60	1	2,00	0	0,00
Outros locais	29	23,02	5	10,00	0	0,00
<i>Não Responderam</i>	0	0,00	1	2,00	0	0,00
Total de Respostas	126		50		13	

B5) Com quantas pessoas partilha a utilização do computador pessoal na sua residência?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Nenhuma	58	46,03	10	20,00	5	38,46
1	33	26,19	18	36,00	6	46,15
2	15	11,90	12	24,00	1	7,69
3 ou mais	20	15,87	9	18,00	1	7,69
<i>Não Responderam</i>	0	0,00	1	2,00	0	0,00
Total de Respostas	126		50		13	

B6) Com que frequência acede à Internet com o seu computador pessoal?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Todos os dias	95	75,40	17	34,00	5	38,46
Quase todos os dias	23	18,25	19	38,00	4	30,77
Pelo menos uma vez por semana	5	3,97	9	18,00	2	15,38
Pelo menos uma vez por mês	3	2,38	4	8,00	2	15,38
Uma ou duas vezes por semestre	0	0,00	0	0,00	0	0,00
<i>Não Responderam</i>	0	0,00	1	2,00	0	0,00
Total de Respostas	126		50		13	

B7) Durante esses acessos à Internet, qual o tempo médio diário de utilização?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Até 1 hora	39	30,95	24	48,00	5	38,46
Entre 1 e 3 horas	53	42,06	22	44,00	7	53,85
Mais de 3 horas	32	25,40	3	6,00	1	7,69
<i>Não Responderam</i>	2	1,59	1	2,00	0	0,00
Total de Respostas	126		50		13	

B8) Classifique a segurança do seu acesso? (6 para muito seguro e 1 para pouco seguro)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,59	0	0,00	1	7,69
2	6	4,76	2	4,00	0	0,00
3	23	18,25	14	28,00	1	7,69
4	33	26,19	17	34,00	5	38,46
5	43	34,13	14	28,00	4	30,77
6	13	10,32	1	2,00	2	15,38
<i>Não Responderam</i>	6	4,76	2	4,00	0	0,00
Total de Respostas	126		50		13	

B9) Identifique a solução que adoptou para acesso à Internet com o seu computador pessoal.						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Modem	15	11,90	8	16,00	1	8,33
ADSL	34	26,98	5	10,00	2	16,67
Cabo	39	30,95	30	60,00	7	58,33
Wireless	27	21,43	5	10,00	2	16,67
Outra	2	1,59	1	2,00	0	0,00
<i>Não Responderam</i>	9	7,14	1	2,00	0	0,00
Total de Respostas	126		50		12	

B10) Possui <i>password</i> para acesso ao seu computador pessoal?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	79	57,66	40	61,54	6	42,86
Sim	58	42,34	24	36,92	8	57,14
<i>Não Responderam</i>	0	0,00	1	1,54	0	0,00
Total de Respostas	137		65		14	

B11) Com quantas pessoas partilha a sua <i>password</i> ?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Nenhuma	34	58,62	10	40,00	5	62,50
1	17	29,31	10	40,00	2	25,00
2 ou 3	4	6,90	4	16,00	1	12,50
Mais de 3	2	3,45	0	0,00	0	0,00
<i>Não Responderam</i>	1	1,72	1	4,00	0	0,00
Total de Respostas	58		25		8	

B12) Já alterou a <i>password</i> de acesso ao seu computador pessoal?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	23	39,66	13	52,00	1	12,50
Sim	35	60,34	11	44,00	7	87,50
<i>Não Responderam</i>	0	0,00	1	4,00	0	0,00
Total de Respostas	58		25		8	

B13) Com que frequência altera a <i>password</i> de acesso ao seu computador pessoal?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Uma única vez	2	5,71	0	0,00	1	14,29
Raramente	19	54,29	6	50,00	4	57,14
Semestralmente/Anualmente	10	28,57	1	8,33	2	28,57
Mensalmente/Trimestralmente	4	11,43	5	41,67	0	0,00
<i>Não Responderam</i>	0	0,00	0	0,00	0	0,00
Total de Respostas	35		12		7	

B14) Que opções efectua na escolha da sua nova <i>password</i> ? (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Datas de nascimento/aniversário	3	8,57	2	16,67	1	14,29
Apenas números	1	2,86	1	8,33	0	0,00
Nomes de familiares	7	20,00	2	16,67	0	0,00
Apenas letras	6	17,14	3	25,00	0	0,00
Nomes de locais	4	11,43	1	8,33	0	0,00
Combinação de números e letras	23	65,71	7	58,33	7	100,00
Nomes de animais de estimação	1	2,86	0	0,00	0	0,00
Escolha aleatória de caracteres	3	8,57	0	0,00	1	14,29
<i>Não Responderam</i>	0	0,00	1	8,33	0	0,00
Total de Respostas	35		12		7	

B15) Na definição de nova <i>password</i> opta por:						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Nº máximo de caracteres permitido	4	11,43	2	16,67	0	0,00
Nº fixo de caracteres, entre máx. e mín.	4	11,43	2	16,67	0	0,00
Nº aleatório de caracteres, entre máx. e mín.	22	62,86	6	50,00	7	100,00
Nº mínimo de caracteres permitido	4	11,43	1	8,33	0	0,00
<i>Não Responderam</i>	1	2,86	1	8,33	0	0,00
Total de Respostas	35		12		7	

B16) Classifique o grau de segurança da sua <i>password</i> . (6 para elevado e 1 para baixo)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	3	5,17	0	0,00	0	0,00
2	3	5,17	1	4,00	0	0,00
3	9	15,52	8	32,00	1	12,50
4	15	25,86	10	40,00	2	25,00
5	18	31,03	6	24,00	3	37,50
6	9	15,52	0	0,00	2	25,00
<i>Não Responderam</i>	1	1,72	0	0,00	0	0,00
Total de Respostas	58		25		8	

B17) Qual o processo que utiliza para guardar a sua <i>password</i> ? (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Memorização	56	96,55	24	96,00	8	100,00
Memória do telemóvel	1	1,72	1	4,00	1	12,50
<i>Post-it</i>	1	1,72	1	4,00	0	0,00
Registo na agenda pessoal	1	1,72	0	0,00	0	0,00
Outro	6	10,34	1	4,00	1	12,50
<i>Não Responderam</i>	0	0,00	0	0,00	0	0,00
Total de Respostas	58		25		8	

B18) Além da <i>password</i> que mecanismo/ferramenta/software utiliza para protecção do seu computador pessoal? (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Nenhum	10	7,30	14	21,54	0	0,00
<i>Firewall</i> (software/hardware para controlo do tráfego da rede informática, etc.)	79	57,66	22	33,85	13	92,86
Antivírus (software destinado à detecção de vírus, entendidos em termos genéricos, e à sua eliminação)	118	86,13	46	70,77	14	100,00
<i>Antispyware</i> (software destinado à detecção de programas intrusivos)	59	43,07	14	21,54	10	71,43
Outros	1	0,73	2	3,08	1	7,14
<i>Não Responderam</i>	2	1,46	2	3,08	0	0,00
Total de Respostas	137		65		14	

B19) Com que frequência actualiza esse mecanismo/ferramenta/software? (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Sempre que existe uma actualização	75	54,74	31	47,69	10	71,43
Sempre que possível	36	26,28	16	24,62	5	35,71
Mensalmente/Trimestralmente	4	2,92	1	1,54	0	0,00
Nunca	9	6,57	7	10,77	0	0,00
Semestralmente/Anualmente	8	5,84	3	4,62	0	0,00
<i>Não Responderam</i>	8	5,84	8	12,31	0	0,00
Total de Respostas	137		65		14	

B20) Efectua cópias de segurança (<i>backups</i>) da informação contida no seu computador pessoal?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	40	29,20	36	55,38	2	14,29
Sim	95	69,34	27	41,54	11	78,57
<i>Não Responderam</i>	2	1,46	2	3,08	1	7,14
Total de Respostas	137		65		14	

B21) Com que periodicidade efectua cópias de segurança (<i>backups</i>)? (<i>assinale todos os itens aplicáveis</i>)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
No final de cada sessão de trabalho	14	14,43	3	10,34	2	16,67
Mensalmente	14	14,43	5	17,24	4	33,33
Na conclusão de cada projecto/ trabalho/etc.	28	28,87	6	20,69	2	16,67
Trimestralmente	22	22,68	6	20,69	2	16,67
Diariamente	5	5,15	0	0,00	0	0,00
Raramente	23	23,71	11	37,93	5	41,67
Semanalmente	5	5,15	2	6,90	0	0,00
<i>Não Responderam</i>	1	1,03	1	3,45	0	0,00
Total de Respostas	97		29		12	

B22) Especifique a opção mais frequente para realização das cópias de segurança (<i>backups</i>)?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Apenas os ficheiros alterados	19	19,59	1	3,45	0	0,00
A totalidade da informação no disco	21	21,65	12	41,38	2	16,67
Um conjunto de ficheiros pré-definidos	22	22,68	3	10,34	2	16,67
Apenas os ficheiros considerados importantes	29	29,90	12	41,38	0	0,00
<i>Não Responderam</i>	6	6,19	1	3,45	8	66,67
Total de Respostas	97		29		12	

B23) Que tipo de dispositivo utiliza para efectuar as cópias de segurança (<i>backups</i>)? (<i>assinale todos os itens aplicáveis</i>)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Disco do computador	9	9,28	1	3,45	0	0,00
Memória <i>flash</i> amovível	44	45,36	7	24,14	4	33,33
Disco externo	34	35,05	7	24,14	8	66,67
Disquete	1	1,03	1	3,45	0	0,00
CD/DVD	68	70,10	20	68,97	10	83,33
Tape	0	0,00	0	0,00	0	0,00
<i>Não Responderam</i>	0	0,00	1	3,45	0	0,00
Total de Respostas	97		29		12	

B24) Especifique onde guarda as cópias de segurança (<i>backups</i>) que efectua.						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Na mesma sala onde se encontra o computador	57	58,76	22	75,86	9	75,00
Em outro espaço da sua residência	27	27,84	5	17,24	3	25,00
Fora da sua residência	9	9,28	1	3,45	0	0,00
<i>Não Responderam</i>	4	4,12	1	3,45	0	0,00
Total de Respostas	97		29		12	

B25) Classifique o grau de segurança do seu computador pessoal. (6 para elevado e 1 para baixo)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	3	2,19	6	9,23	0	0,00
2	10	7,30	3	4,62	0	0,00
3	25	18,25	16	24,62	2	14,29
4	47	34,31	26	40,00	5	35,71
5	37	27,01	9	13,85	3	21,43
6	7	5,11	2	3,08	4	28,57
<i>Não Responderam</i>	8	5,84	3	4,62	0	0,00
Total de Respostas	137		65		14	

B26) Com que frequência utiliza o seu computador pessoal?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Todos os dias	97	70,80	21	32,31	4	28,57
Quase todos os dias	31	22,63	23	35,38	6	42,86
Pelo menos uma vez por semana	7	5,11	16	24,62	2	14,29
Pelo menos uma vez por mês	1	0,73	4	6,15	2	14,29
Uma ou duas vezes por semestre	1	0,73	0	0,00	0	0,00
<i>Não Responderam</i>	0	0,00	1	1,54	0	0,00
Total de Respostas	137		65		14	

B27) Caracterize a sua utilização do seu computador pessoal. (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Elaboração de relatórios e outros trabalhos	131	95,62	46	70,77	13	92,86
Jogos	29	21,17	14	21,54	6	42,86
Impressão de documentos	103	75,18	29	44,62	10	71,43
Pesquisas na Internet	119	86,86	49	75,38	13	92,86
Trabalhos escolares	102	74,45	15	23,08	5	35,71
Envio/recepção de correio electrónico	123	89,78	45	69,23	12	85,71
<i>Não Responderam</i>	1	0,73	2	3,08	0	0,00
Total de Respostas	137		65		14	

B28) Durante a utilização do seu computador pessoal, qual o tempo médio diário de utilização?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Até 1 hora	10	7,30	23	35,38	3	21,43
Entre 1 e 3 horas	60	43,80	34	52,31	10	71,43
Mais de 3 horas	65	47,45	6	9,23	1	7,14
<i>Não Responderam</i>	2	1,46	2	3,08	0	0,00
Total de Respostas	137		65		14	

B29) Que tipo de software utiliza no seu computador pessoal? (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Sistema Operativo Windows	129	94,16	55	84,62	14	100,00
Folha de Cálculo (por ex. Excel)	120	87,59	51	78,46	13	92,86
Sistema Operativo Macintosh	8	5,84	0	0,00	0	0,00
Base de Dados (por ex. Access)	51	37,23	24	36,92	10	71,43
Sistema Operativo Linux	9	6,57	0	0,00	1	7,14
Apresentações (por ex. PowerPoint)	118	86,13	36	55,38	10	71,43
Outro Sistema Operativo	1	0,73	2	3,08	0	0,00
Outros aplicativos	86	62,77	22	33,85	12	85,71
Processador de Texto (por ex. Word)	123	89,78	55	84,62	14	100,00
<i>Não Responderam</i>	1	0,73	4	6,15	0	0,00
Total de Respostas	137		65		14	

Grupo C – Sistema Informático do Serviço/Escola

C1) Desde a sua entrada no Serviço/Escola existiu alguma mudança no Sistema Informático (<i>Hardware, Software, Procedimentos, etc.</i>)?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	6	4,38	9	11,39	0	0,00
Não sabe	13	9,49	14	17,72	0	0,00
Sim	116	84,67	54	68,35	14	100,00
<i>Não Responderam</i>	2	1,46	2	2,53	0	0,00
Total de Respostas	137		79		14	

C2) Foi solicitada a sua participação/participou de alguma forma nessas mudanças?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	78	66,10	26	46,43	1	7,14
Sim	39	33,05	27	48,21	13	92,86
<i>Não Responderam</i>	1	0,85	3	5,36	0	0,00
Total de Respostas	118		56		14	

C3) Caracterize a sua participação nessas mudanças. (<i>assinale todos os itens aplicáveis</i>)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Aquisição de <i>Software/Hardware</i>	25	62,50	9	30,00	13	100,00
Análise de documentos	17	42,50	7	23,33	4	30,77
Instalação/Configuração de <i>Hardware</i>	10	25,00	4	13,33	13	100,00
Preenchimento de inquéritos/questionários	6	15,00	8	26,67	2	15,38
Instalação/Configuração de <i>Software</i>	21	52,50	5	16,67	13	100,00
Resposta a entrevistas	2	5,00	3	10,00	0	0,00
Definição/Implementação de Procedimentos	18	45,00	15	50,00	9	69,23
Elaboração de pareceres	10	25,00	5	16,67	3	23,08
<i>Não Responderam</i>	2	5,00	4	13,33	0	0,00
Total de Respostas	40		30		13	

C4) Classifique o seu grau de participação nessas mudanças. (6 para elevado e 1 para baixo)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	5	12,50	1	3,33	0	0,00
2	8	20,00	6	20,00	0	0,00
3	10	25,00	8	26,67	2	15,38
4	9	22,50	8	26,67	3	23,08
5	5	12,50	4	13,33	3	23,08
6	3	7,50	1	3,33	5	38,46
<i>Não Responderam</i>	0	0,00	2	6,67	0	0,00
Total de Respostas	40		30		13	

C5) Classifique o seu grau de satisfação com as mudanças efectuadas. (6 para elevado e 1 para baixo)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,69	1	1,79	0	0,00
2	2	1,69	2	3,57	1	7,14
3	16	13,56	14	25,00	2	14,29
4	37	31,36	21	37,50	4	28,57
5	49	41,53	15	26,79	6	42,86
6	10	8,47	1	1,79	1	7,14
<i>Não Responderam</i>	2	1,69	2	3,57	0	0,00
Total de Respostas	118		56		14	

C6) Classifique a sua percepção acerca do funcionamento do Sistema Informático depois das mudanças efectuadas. (6 para melhorou muito e 1 para não melhorou)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	3	2,54	3	5,36	0	0,00
2	4	3,39	2	3,57	2	14,29
3	14	11,86	10	17,86	0	0,00
4	40	33,90	26	46,43	6	42,86
5	47	39,83	8	14,29	6	42,86
6	8	6,78	5	8,93	0	0,00
<i>Não Responderam</i>	2	1,69	2	3,57	0	0,00
Total de Respostas	118		56		14	

C7) Já tinha utilizado computadores antes de ser admitido(a) no IPS/ Escola?		
	Não Docentes	
	nº	%
Não	13	16,46
Sim	66	83,54
<i>Não Responderam</i>	0	0,00
Total de Respostas	79	

C8) Realizou algum(uns) curso(s) de formação em Informática/Sistemas de Informação antes de ser admitido(a) no IPS/ Escola?		
	Não Docentes	
	nº	%
Não	25	37,88
Sim	40	60,61
<i>Não Responderam</i>	1	1,52
Total de Respostas	66	

C7) Qual a frequência média anual das acções de formação em informática que recebeu?		
	Técnicos	
	nº	%
Nunca recebeu	0	0,00
1	5	35,71
2	7	50,00
3	2	14,29
4 ou mais	0	0,00
<i>Não Responderam</i>		0 0,00
Total de Respostas		14

C8) Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)		
	Técnicos	
	nº	%
1	0	0,00
2	1	7,14
3	1	7,14
4	1	7,14
5	7	50,00
6	4	28,57
<i>Não Responderam</i>		0 0,00
Total de Respostas		14

C7) Classifique o seu grau de conhecimentos na área da Informática/Sistemas de Informação. (6 para elevado e 1 para baixo)						
[Não Docentes C9)/Técnicos C9)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	6	4,38	1	1,52	0	0,00
2	8	5,84	1	1,52	0	0,00
3	47	34,31	16	24,24	0	0,00
4	34	24,82	39	59,09	4	28,57
5	28	20,44	8	12,12	7	50,00
6	11	8,03	0	0,00	3	21,43
<i>Não Responderam</i>	3	2,19	1	1,52	0	0,00
Total de Respostas	137		66		14	

C8) Dispõe de acesso ao Sistema Informático do Serviço/Escola?				
[Não Docentes C10)]	Docentes		Não Docentes	
	nº	%	nº	%
Não	3	2,19	3	3,80
Sim	133	97,08	76	96,20
<i>Não Responderam</i>	1	0,73	0	0,00
Total de Respostas	137		79	

C9) O acesso ao Sistema Informático do Serviço/Escola é feito através de <i>password</i> ?						
[Não Docentes C11)/Técnicos C10)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	1	0,75	2	2,63	0	0,00
Sim	132	98,51	73	96,05	14	100,00
<i>Não Responderam</i>	1	0,75	1	1,32	0	0,00
Total de Respostas	134		76		14	

C10) Já alterou a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático do Serviço/Escola?						
[Não Docentes C12)/Técnicos C11)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	31	23,31	24	32,43	1	7,14
Sim	101	75,94	50	67,57	13	92,86
<i>Não Responderam</i>	1	0,75	0	0,00	0	0,00
Total de Respostas	133		74		14	

C11) Com que frequência altera a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático do Serviço/Escola?						
[Não Docentes C13)/Técnicos C12)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Uma única vez	18	17,65	11	22,00	0	0,00
Raramente	42	41,18	19	38,00	2	15,38
Semestralmente/Anualmente	26	25,49	8	16,00	11	84,62
Mensalmente/Trimestralmente	13	12,75	11	22,00	0	0,00
<i>Não Responderam</i>	3	2,94	1	2,00	0	0,00
Total de Respostas	102		50		13	

C12) Que opções efectua na escolha de nova(s) <i>password(s)</i> ? (assinale todos os itens aplicáveis)						
[Não Docentes C14)/Técnicos C13)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Datas de nascimento/aniversário	7	6,86	7	14,00	0	0,00
Apenas números	2	1,96	4	8,00	0	0,00
Nomes de familiares	29	28,43	15	30,00	0	0,00
Apenas letras	14	13,73	6	12,00	1	7,69
Nomes de locais	9	8,82	9	18,00	0	0,00
Combinação de números e letras	65	63,73	18	36,00	12	92,31
Nomes de animais de estimação	4	3,92	3	6,00	0	0,00
Escolha aleatória de caracteres	7	6,86	2	4,00	2	15,38
<i>Não Responderam</i>	2	1,96	3	6,00	0	0,00
Total de Respostas	102		50		13	

C13) Na definição de nova(s) <i>password(s)</i> opta por:						
[Não Docentes C15)/Técnicos C14)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
N.º máximo de caracteres permitido	17	16,67	5	10,00	0	0,00
N.º fixo de caracteres, entre máx. e mín.	18	17,65	6	12,00	1	7,69
N.º aleatório de caracteres, entre máx. e mín.	50	49,02	28	56,00	11	84,62
N.º mínimo de caracteres permitido	13	12,75	8	16,00	1	7,69
<i>Não Responderam</i>	4	3,92	3	6,00	0	0,00
Total de Respostas	102		50		13	

C14) Qual o processo que utiliza para guardar a(s) sua(s) <i>password(s)</i> ? (assinale todos os itens aplicáveis)						
[Não Docentes C16)/Técnicos C15)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Memorização	117	87,97	63	85,14	14	100,00
Memória do telemóvel	4	3,01	3	4,05	0	0,00
<i>Post-it</i>	4	3,01	3	4,05	0	0,00
Registo na agenda pessoal	17	12,78	8	10,81	0	0,00
Outro	19	14,29	0	0,00	0	0,00
<i>Não Responderam</i>	2	1,50	2	2,70	0	0,00
Total de Respostas	133		74		14	

C15) Com quantas pessoas partilha a(s) sua(s) <i>password(s)</i> de acesso ao Sistema Informático do Serviço/Escola?						
[Não Docentes C17)/Técnicos C16)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Nenhuma	112	84,21	41	55,41	10	71,43
1	10	7,52	21	28,38	2	14,29
2 ou 3	6	4,51	12	16,22	2	14,29
Mais de 3	2	1,50	0	0,00	0	0,00
<i>Não Responderam</i>	3	2,26	0	0,00	0	0,00
Total de Respostas	133		74		14	

C17) Quantas <i>passwords</i> de acesso ao Sistema Informático do Serviço utiliza?		
	Técnicos	
	nº	%
1	2	14,29
2	2	14,29
3	4	28,57
4 ou mais	6	42,86
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

C16) Utiliza a mesma <i>password</i> para diversas aplicações/sistemas?						
[Não Docentes C18)/Técnicos C18)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	50	37,59	42	56,76	3	21,43
Sim	81	60,90	31	41,89	11	78,57
<i>Não Responderam</i>	2	1,50	1	1,35	0	0,00
Total de Respostas	133		74		14	

C17) Classifique o grau de segurança da(s) sua(s) <i>password(s)</i> . (6 para elevado e 1 para baixo)						
[Não Docentes C19)/Técnicos C19)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,50	0	0,00	0	0,00
2	9	6,77	3	4,05	1	7,14
3	21	15,79	18	24,32	1	7,14
4	51	38,35	29	39,19	3	21,43
5	32	24,06	17	22,97	8	57,14
6	11	8,27	4	5,41	1	7,14
<i>Não Responderam</i>	7	5,26	3	4,05	0	0,00
Total de Respostas	133		74		14	

C18) Além da <i>password</i> , especifique que tipo(s) de mecanismo(s) está(ão) implementado(s) para acesso ao Sistema Informático do Serviço/Escola. (assinale todos os itens aplicáveis)						
[Não Docentes C20)/Técnicos C20)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Cartão magnético	4	2,99	2	2,63	0	0,00
Controlo biométrico	0	0,00	0	0,00	0	0,00
Cartão com <i>microchip</i>	0	0,00	0	0,00	0	0,00
Identificação pessoal	30	22,39	13	17,11	0	0,00
Chave metálica	4	2,99	0	0,00	0	0,00
Nenhum	85	63,43	57	75,00	14	100,00
<i>Não Responderam</i>	17	12,69	5	6,58	0	0,00
Total de Respostas	134		76		14	

C19) Possui algum endereço de correio electrónico associado ao Sistema Informático do Serviço/Escola?						
[Não Docentes C21)/Técnicos C21)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	3	2,24	10	13,16	0	0,00
Sim	129	96,27	65	85,53	14	100,00
<i>Não Responderam</i>	2	1,49	1	1,32	0	0,00
Total de Respostas	134		76		14	

C20) Além desse, quantos endereços de correio electrónico possui?						
[Não Docentes C22)/Técnicos C22)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Nenhum	15	11,45	17	25,76	0	0,00
1	37	28,24	21	31,82	4	28,57
2	47	35,88	20	30,30	5	35,71
3	14	10,69	6	9,09	3	21,43
Mais de 3	15	11,45	1	1,52	2	14,29
<i>Não Responderam</i>	3	2,29	1	1,52	0	0,00
Total de Respostas	131		66		14	

C21) Utiliza a mesma <i>password</i> para acesso ao correio electrónico e ao Sistema Informático do Serviço/Escola?						
[Não Docentes C23)/Técnicos C23)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	105	80,15	51	77,27	12	85,71
Sim	21	16,03	14	21,21	2	14,29
<i>Não Responderam</i>	5	3,82	1	1,52	0	0,00
Total de Respostas	131		66		14	

C22) Existe implementado algum sistema de filtragem de mensagens de correio electrónico?						
[Não Docentes C24)/Técnicos C24)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	1	0,76	2	3,03	0	0,00
Não sabe	16	12,21	23	34,85	0	0,00
Sim	110	83,97	38	57,58	14	100,00
<i>Não Responderam</i>	4	3,05	3	4,55	0	0,00
Total de Respostas	131		66		14	

C23) Com que frequência acede ao Sistema Informático do Serviço/Escola?						
[Não Docentes C25)/Técnicos C25)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Todos os dias	71	52,99	60	78,95	14	100,00
Quase todos os dias	52	38,81	11	14,47	0	0,00
Pelo menos uma vez por semana	6	4,48	3	3,95	0	0,00
Pelo menos uma vez por mês	3	2,24	1	1,32	0	0,00
Uma ou duas vezes por semestre	0	0,00	0	0,00	0	0,00
<i>Não Responderam</i>	2	1,49	1	1,32	0	0,00
Total de Respostas	134		76		14	

C24) Durante a utilização do Sistema Informático do Serviço/Escola, qual o tempo médio diário de cada utilização?						
[Não Docentes C26)/Técnicos C27)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Até 1 hora	27	20,15	11	14,47	1	7,14
Entre 1 e 3 horas	41	30,60	10	13,16	0	0,00
Entre 3 e 5 horas	36	26,87	18	23,68	2	14,29
Mais de 5 horas	28	20,90	36	47,37	11	78,57
<i>Não Responderam</i>	2	1,49	1	1,32	0	0,00
Total de Respostas	134		76		14	

C25) Que tipo de software utiliza? (assinale todos os itens aplicáveis)						
[Não Docentes C27)/Técnicos C28)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Sistema Operativo Windows 95/98/2000/XP	128	95,52	62	81,58	14	100,00
Base de Dados	44	32,84	29	38,16	11	78,57
Programação	26	19,40	1	1,32	7	50,00
Sistema Operativo Windows Server	11	8,21	1	1,32	11	78,57
Apresentações	94	70,15	13	17,11	8	57,14
Sistema Operativo Linux	6	4,48	0	0,00	2	14,29
Desenho técnico	17	12,69	2	2,63	0	0,00
Sistema Operativo Macintosh	0	0,00	0	0,00	0	0,00
Análise de sistemas	5	3,73	0	0,00	2	14,29
Outro Sistema Operativo	1	0,75	2	2,63	0	0,00
Processador de Texto	109	81,34	52	68,42	13	92,86
Gestão/Contabilidade/Marketing	11	8,21	15	19,74	0	0,00
Folha de Cálculo	107	79,85	48	63,16	13	92,86
Outros aplicativos	62	46,27	30	39,47	10	71,43
<i>Não Responderam</i>	2	1,49	4	5,26	0	0,00
Total de Respostas	134		76		14	

C26) Caracterize a sua utilização do Sistema Informático do Serviço/Escola. (assinale todos os itens aplicáveis)						
[Não Docentes C28)/Técnicos C29)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Elaboração de relatórios	111	82,84	42	55,26	12	85,71
Registo/Introdução de dados	76	56,72	68	89,47	12	85,71
Elaboração de outros trabalhos	104	77,61	57	75,00	13	92,86
Análise estatística/projecções	41	30,60	16	21,05	1	7,14
Impressão de documentos	114	85,07	65	85,53	13	92,86
Pesquisas na Internet	116	86,57	65	85,53	14	100,00
Leccionação {apenas Docentes}	116	86,57	-	-	-	-
Envio/recepção de correio electrónico	120	89,55	66	86,84	14	100,00
<i>Não Responderam</i>	4	2,99	2	2,63	0	0,00
Total de Respostas	134		76		14	

C27) Utiliza alguma área de trabalho privada no(s) servidor(es) do Sistema Informático do Serviço/Escola?						
[Não Docentes C29)/Técnicos C29)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	57	42,54	42	55,26	2	14,29
Sim	74	55,22	30	39,47	12	85,71
<i>Não Responderam</i>	3	2,24	4	5,26	0	0,00
Total de Respostas	134		76		14	

C28) Que tipo de informação guarda nessa área de trabalho?						
[Não Docentes C30)/Técnicos C30)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Ficheiros de trabalho	47	61,04	14	41,18	7	58,33
Ficheiros pessoais	1	1,30	1	2,94	0	0,00
Ambos	26	33,77	16	47,06	5	41,67
<i>Não Responderam</i>	3	3,90	3	8,82	0	0,00
Total de Respostas	77		34		12	

C29) Já perdeu informação guardada nessa área de trabalho?						
[Não Docentes C31)/Técnicos C31)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	65	84,42	25	73,53	10	83,33
Sim	9	11,69	6	17,65	2	16,67
<i>Não Responderam</i>	3	3,90	3	8,82	0	0,00
Total de Respostas	77		34		12	

C30) Que acção tomou para recuperar essa informação?						
[Não Docentes C32)/Técnicos C32)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Expôs a situação aos serviços de informática	6	50,00	-	-	-	-
Expôs a situação ao(à) responsável do Serviço ou aos serviços de informática	-	-	3	33,33	-	-
Expôs a situação ao(à) responsável do Serviço	-	-	-	-	0	0,00
Tentou recuperar a informação	1	8,33	3	33,33	2	100,00
Nenhuma	0	0,00	0	0,00	0	0,00
<i>Não Responderam</i>	5	41,67	3	33,33	0	0,00
Total de Respostas	12		9		2	

C31) O que aconteceu relativamente a essa situação? (assinale todos os itens aplicáveis)						
[Não Docentes C33)/Técnicos C33)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
A informação foi reposta de <i>backups</i> anteriores	4	33,33	2	22,22	2	100,00
A informação foi recuperada mas não sabe como	2	16,67	2	22,22	0	0,00
A informação não foi recuperada	3	25,00	2	22,22	0	0,00
Recebeu comunicação de que era impossível recuperar a informação	0	0,00	0	0,00	0	0,00
Não sabe nada acerca da situação	0	0,00	0	0,00	0	0,00
<i>Não Responderam</i>	4	33,33	3	33,33	0	0,00
Total de Respostas	12		9		2	

C32) Possui acesso à impressão de documentos através do Sistema Informático do Serviço/Escola utilizando impressora(s) partilhada(s)?						
[Não Docentes C34)/Técnicos C34)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	9	6,72	11	14,47	0	0,00
Sim	120	89,55	65	85,53	14	100,00
<i>Não Responderam</i>	5	3,73	0	0,00	0	0,00
Total de Respostas	134		76		14	

C33) Quando não consegue imprimir documentos através da(s) impressora(s) partilhada(s) qual a atitude que assume? (assinale todos os itens aplicáveis)						
[Não Docentes C35)/Técnicos C35)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Cancela de imediato o trabalho	48	38,40	13	20,00	2	14,29
Tenta imprimir numa impressora disponível	70	56,00	21	32,31	5	35,71
Tenta imprimir novamente	59	47,20	33	50,77	5	35,71
Tenta imprimir mais tarde	46	36,80	19	29,23	1	7,14
Verifica se a impressora tem algum problema	82	65,60	39	60,00	14	100,00
Informa os serviços de informática	67	53,60	36	55,38	-	-
Informa o(a) responsável do Serviço	-	-	13	20,00	2	14,29
Altera a configuração de acesso à impressora	5	4,00	3	4,62	2	14,29
Nenhuma	0	0,00	0	0,00	0	0,00
<i>Não Responderam</i>	3	2,40	0	0,00	0	0,00
Total de Respostas	125		65		14	

C34) Que atitude toma quando encontra documentos que não são seus na(s) impressora(s) partilhada(s)? (assinale todos os itens aplicáveis)						
[Não Docentes C36)/Técnicos C36)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Nunca encontrou	3	2,40	5	7,69	1	7,14
Deita fora ou destrói o documento	0	0,00	2	3,08	0	0,00
Lê o documento (todo ou parte)	7	5,60	5	7,69	0	0,00
Guarda para seu uso pessoal	0	0,00	0	0,00	0	0,00
Entrega aos serviços de informática	5	4,00	-	-	-	-
Entrega ao(à) responsável do Serviço	-	-	8	12,31	1	7,14
Deixa junto à impressora	104	83,20	30	46,15	12	85,71
Tenta entregar/entregou ao seu proprietário	54	43,20	39	60,00	3	21,43
Nenhuma	3	2,40	1	1,54	0	0,00
<i>Não Responderam</i>	2	1,60	0	0,00	0	0,00
Total de Respostas	125		65		14	

C35) Que atitude toma quando não encontra documentos seus que mandou imprimir na(s) impressora(s) partilhada(s)? (assinale todos os itens aplicáveis)						
[Não Docentes C37)/Técnicos C37)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Nunca aconteceu	28	22,40	19	29,23	10	71,43
Imprime novamente o documento	70	56,00	27	41,54	1	7,14
Verifica se ainda aguarda por impressão	76	60,80	27	41,54	4	28,57
Tenta encontrar o documento	53	42,40	22	33,85	1	7,14
Informa os serviços de informática	14	11,20	12	18,46	-	-
Informa o(a) responsável do Serviço	-	-	0	0,00	0	0,00
Nenhuma	1	0,80	0	0,00	0	0,00
<i>Não Responderam</i>	2	1,60	0	0,00	0	0,00
Total de Respostas	125		65		14	

C36) Consideraria a hipótese de aceder ao Sistema Informático do Serviço/Escola a partir da sua residência ou de outro local onde trabalhe regularmente?						
[Não Docentes C38)/Técnicos C38)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	5	3,73	22	28,95	1	7,14
Sim	116	86,57	32	42,11	12	85,71
Talvez	7	5,22	19	25,00	1	7,14
<i>Não Responderam</i>	6	4,48	3	3,95	0	0,00
Total de Respostas	134		76		14	

Grupo D – Segurança da Informação no Sistema Informático do Serviço/Escola

D1) Existem políticas (normas/regulamentos/regras/procedimentos) de segurança do Sistema Informático do Serviço/Escola?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	6	4,48	2	2,63	1	7,14
Não sabe	76	56,72	39	51,32	0	0,00
Sim	50	37,31	32	42,11	13	92,86
<i>Não Responderam</i>	2	1,49	3	3,95	0	0,00
Total de Respostas	134		76		14	

D2) Como tomou conhecimento dessas políticas (normas/regulamentos/regras/procedimentos)? (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Documento entregue no Serviço/Escola	13	25,00	4	11,43	2	15,38
Consulta da página <i>web</i> do Serviço/Escola	6	11,54	1	2,86	0	0,00
Informação dos serviços de informática	35	67,31	-	-	-	-
Informação do(a) responsável do Serviço	-	-	14	40,00	8	61,54
Colega de trabalho	14	26,92	16	45,71	7	53,85
Informação afixada no Serviço/Escola	2	3,85	1	2,86	0	0,00
Outro meio	3	5,77	5	14,29	2	15,38
<i>Não Responderam</i>	2	3,85	3	8,57	0	0,00
Total de Respostas	52		35		13	

D3) Dos aspectos a seguir mencionados, especifique quais são abrangidos pelas políticas (normas/regulamentos/regras/procedimentos) definidas. (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Definição de acessos ao sistema (por ex. <i>passwords</i>)	45	86,54	24	68,57	11	84,62
Utilização dos recursos de <i>hardware</i>	13	25,00	9	25,71	8	61,54
Acesso aos servidores	24	46,15	13	37,14	9	69,23
Utilização do correio electrónico	36	69,23	18	51,43	8	61,54
Realização de cópias de segurança (<i>backups</i>)	12	23,08	12	34,29	9	69,23
Utilização da Internet	14	26,92	11	31,43	5	38,46
Instalação de <i>software</i>	27	51,92	7	20,00	6	46,15
Detecção/Controlo de intrusões	14	26,92	5	14,29	1	7,69
Plano de Recuperação de Acidentes	3	5,77	2	5,71	1	7,69
Controlo dos activos do sistema	4	7,69	1	2,86	2	15,38
<i>Não Responderam</i>	3	5,77	6	17,14	0	0,00
Total de Respostas	52		35		13	

D4) Participou na elaboração/alteração dessas políticas (normas/regulamentos/regras/procedimentos)?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	46	88,46	30	85,71	8	61,54
Sim	4	7,69	3	8,57	5	38,46
<i>Não Responderam</i>	2	3,85	2	5,71	0	0,00
Total de Respostas	52		35		13	

D5) Caracterize a sua participação nessas actividades. (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Elaboração das políticas	2	33,33	1	20,00	4	80,00
Preenchimento de inquéritos/questionários	0	0,00	1	20,00	0	0,00
Implementação das políticas	2	33,33	0	0,00	5	100,00
Resposta a entrevistas	0	0,00	1	20,00	0	0,00
Análise de documentos	1	16,67	1	20,00	2	40,00
Análise/Auditoria de segurança	-	-	-	-	0	0,00
Elaboração de pareceres	1	16,67	0	0,00	0	0,00
<i>Não Responderam</i>	3	50,00	2	40,00	0	0,00
Total de Respostas	6		5		5	

D6) Classifique o seu grau de participação nessas actividades. (6 para elevado e 1 para baixo)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	1	16,67	0	0,00	0	0,00
2	0	0,00	1	20,00	0	0,00
3	2	33,33	1	20,00	0	0,00
4	1	16,67	1	20,00	3	60,00
5	0	0,00	0	0,00	1	20,00
6	0	0,00	0	0,00	1	20,00
<i>Não Responderam</i>	2	33,33	2	40,00	0	0,00
Total de Respostas	6		5		5	

D7) Caracterize a sua participação nas acções de sensibilização para a problemática da segurança da informação?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não teve conhecimento de qualquer accção	99	73,88	64	84,21	3	21,43
Não teve possibilidade de participar	13	9,70	2	2,63	2	14,29
Não foi convidado(a) a participar	8	5,97	5	6,58	2	14,29
Não quis participar	0	0,00	0	0,00	0	0,00
Participou com interesse	8	5,97	2	2,63	5	35,71
Participou sem interesse	0	0,00	0	0,00	0	0,00
<i>Não Responderam</i>	6	4,48	3	3,95	2	14,29
Total de Respostas	134		76		14	

D8) Já presenciou alguma(s) violação(ões) da segurança do Sistema Informático do Serviço/Escola (por exemplo destruição/roubo de equipamentos, entradas em locais interditos, utilização de ficheiros/passwords de outras pessoas, etc.)?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	124	92,54	72	94,74	8	57,14
Sim	8	5,97	4	5,26	6	42,86
<i>Não Responderam</i>	2	1,49	0	0,00	0	0,00
Total de Respostas	134		76		14	

D9) Que atitude tomou quando presenciou essa(s) violação(ões)? (assinale todos os itens aplicáveis)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Advertiu o(a) infractor(a)	7	70,00	1	25,00	3	50,00
Propôs medidas para resolução do problema	4	40,00	0	0,00	3	50,00
Informou a Direcção da Escola	2	20,00	-	-	-	-
Informou o(a) responsável do Serviço	-	-	0	0,00	4	66,67
Comentou com os(as) seus(suas) colegas	2	20,00	1	25,00	0	0,00
Informou os serviços de informática	3	30,00	1	25,00	-	-
Nenhuma	0	0,00	3	75,00	0	0,00
<i>Não Responderam</i>	2	20,00	0	0,00	0	0,00
Total de Respostas	10		4		6	

D10) Após o login no acesso ao Sistema Informático do Serviço/Escola, existe definido algum tempo limite para que a sessão de trabalho esteja activa?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	42	31,34	29	38,16	7	50,00
Não sabe	64	47,76	29	38,16	1	7,14
Sim	26	19,40	12	15,79	5	35,71
<i>Não Responderam</i>	2	1,49	6	7,89	1	7,14
Total de Respostas	134		76		14	

D11) Durante o tempo em que tem activa a sua sessão de trabalho, utiliza algum mecanismo de protecção de ecrã para quando não está a utilizar o computador?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	72	53,73	34	44,74	1	7,14
Sim	58	43,28	42	55,26	13	92,86
<i>Não Responderam</i>	4	2,99	0	0,00	0	0,00
Total de Respostas	134		76		14	

D12) Além da <i>password</i> que mecanismo/ferramenta/software é utilizado para protecção do Sistema Informático do Serviço. (assinale todos os itens aplicáveis)		
	Técnicos	
	nº	%
Nenhum	0	0,00
Encriptação das comunicações	2	14,29
<i>Firewall</i>	12	85,71
Sistema de Detecção de Intrusão	2	14,29
Antivirus	14	100,00
Outros	1	7,14
<i>Antispyware</i>	13	92,86
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

D13) Com que frequência se actualiza esse mecanismo/ferramenta/software. (assinale todos os itens aplicáveis)		
	Técnicos	
	nº	%
Sempre que existe uma actualização	14	100,00
Semestralmente/Anualmente	0	0,00
Mensalmente/Trimestralmente	0	0,00
Nunca actualiza	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

D14) Está implementada alguma política de segurança da informação contida nos servidores?		
	Técnicos	
	nº	%
Não	0	0,00
Sim	14	100,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

D15) Essa política de cópias de segurança da informação estabelece regras em função da criticidade da informação?		
	Técnicos	
	nº	%
Não	2	14,29
Sim	12	85,71
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

D16) Caracterize essas regras para as cópias de segurança?		
	Técnicos	
	nº	%
A totalidade da informação	2	16,67
A totalidade da informação, com periodicidades distintas em função da criticidade	8	66,67
Apenas a informação crítica	2	16,67
<i>Não Responderam</i>	0	0,00
Total de Respostas	12	

D17) Com que periodicidade são efectuadas as cópias de segurança da informação crítica. (assinale todos os itens aplicáveis)		
	Técnicos	
	nº	%
Não sabe	0	0,00
Mensalmente	3	21,43
Sempre que necessário	4	28,57
Trimestralmente	1	7,14
Diariamente	14	100,00
Raramente	0	0,00
Semanalmente	3	21,43
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

D18) Que tipo de dispositivo é utilizado para efectuar as cópias de segurança. (assinale todos os itens aplicáveis)		
	Técnicos	
	nº	%
Disco do servidor	6	42,86
Disco óptico	0	0,00
Disco externo	5	35,71
Disquete	0	0,00
CD/DVD	0	0,00
Tape	12	85,71
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

D19) Onde são guardadas as cópias de segurança efectuadas.		
	Técnicos	
	nº	%
Não sabe	1	7,14
Na sala de servidores	7	50,00
Em outro espaço do Serviço	4	28,57
Fora do Serviço	0	0,00
<i>Não Responderam</i>	2	14,29
Total de Respostas	14	

D20) Existem registos do <i>hardware</i> e <i>software</i> existente no Serviço?		
	Técnicos	
	nº	%
Não	1	7,14
Sim	12	85,71
<i>Não Responderam</i>	1	7,14
Total de Respostas	14	

D21) Com que periodicidade são actualizados esses registos.		
	Técnicos	
	nº	%
Não sabe	4	30,77
Sempre que necessário	8	61,54
Diariamente	0	0,00
Semanalmente	1	7,69
Mensalmente	0	0,00
Trimestralmente	0	0,00
Raramente	0	0,00
<i>Não Responderam</i>	0	0,00
Total de Respostas	13	

D12) Classifique a segurança do Sistema Informático do Serviço/Escola. (6 para muito seguro e 1 para pouco seguro)						
[Técnicos D22)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	1	0,75	0	0,00	0	0,00
2	4	2,99	5	6,58	0	0,00
3	20	14,93	20	26,32	2	14,29
4	65	48,51	23	30,26	5	35,71
5	30	22,39	23	30,26	6	42,86
6	3	2,24	2	2,63	1	7,14
<i>Não Responderam</i>	11	8,21	3	3,95	0	0,00
Total de Respostas	134		76		14	

D13) Classifique, relativamente à segurança do Sistema Informático da Escola (6 para muito importante e 1 para pouco importante), os seguintes aspectos:				
[Técnicos D23)]				
(a) Utilizadores				
	Docentes		Não Docentes	
	nº	%	nº	%
1	2	1,49	0	0,00
2	2	1,49	3	3,95
3	14	10,45	13	17,11
4	18	13,43	18	23,68
5	45	33,58	20	26,32
6	36	26,87	12	15,79
<i>Não Responderam</i>	17	12,69	10	13,16
Total de Respostas	134		76	

(b) Técnicos de informática						
	Docentes		Não Docentes			
	nº	%	nº	%		
1	3	2,24	1	1,32		
2	1	0,75	0	0,00		
3	9	6,72	6	7,89		
4	16	11,94	12	15,79		
5	37	27,61	24	31,58		
6	47	35,07	23	30,26		
<i>Não Responderam</i>	21	15,67	10	13,16		
Total de Respostas	134		76			
(a) Pessoas						
			Técnicos			
			nº	%		
1			0	0,00		
2			0	0,00		
3			2	14,29		
4			3	21,43		
5			3	21,43		
6			5	35,71		
<i>Não Responderam</i>			1	7,14		
Total de Respostas			14			
(c) Leis/Políticas/Regulamentos/Procedimentos						
[Técnicos (b)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	4	2,99	3	3,95	0	0,00
2	2	1,49	7	9,21	1	7,14
3	17	12,69	7	9,21	2	14,29
4	28	20,90	13	17,11	1	7,14
5	41	30,60	21	27,63	4	28,57
6	17	12,69	13	17,11	5	35,71
<i>Não Responderam</i>	25	18,66	12	15,79	1	7,14
Total de Respostas	134		76		14	
(d) Computadores Pessoais (<i>Hardware</i>)						
[Técnicos (c)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	6	4,48	1	1,32	0	0,00
2	3	2,24	1	1,32	1	7,14
3	16	11,94	16	21,05	2	14,29
4	35	26,12	18	23,68	1	7,14
5	33	24,63	17	22,37	4	28,57
6	16	11,94	11	14,47	5	35,71
<i>Não Responderam</i>	25	18,66	12	15,79	1	7,14
Total de Respostas	134		76		14	

(e) Periféricos (Impressoras, Scanners, etc.)						
[Técnicos (d)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	12	8,96	1	1,32	0	0,00
2	11	8,21	7	9,21	1	7,14
3	18	13,43	15	19,74	3	21,43
4	26	19,40	22	28,95	5	35,71
5	31	23,13	16	21,05	3	21,43
6	11	8,21	6	7,89	1	7,14
<i>Não Responderam</i>	25	18,66	9	11,84	1	7,14
Total de Respostas	134		76		14	
(f) Servidores (Hardware)						
[Técnicos (e)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	0	0,00	0	0,00
2	1	0,75	3	3,95	3	21,43
3	7	5,22	9	11,84	5	35,71
4	26	19,40	15	19,74	4	28,57
5	31	23,13	17	22,37	1	7,14
6	37	27,61	21	27,63	0	0,00
<i>Não Responderam</i>	30	22,39	11	14,47	1	7,14
Total de Respostas	134		76		14	
(g) Software aplicacional						
[Técnicos (f)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	0	0,00	0	0,00
2	4	2,99	3	3,95	1	7,14
3	13	9,70	13	17,11	1	7,14
4	26	19,40	18	23,68	3	21,43
5	37	27,61	20	26,32	4	28,57
6	24	17,91	9	11,84	4	28,57
<i>Não Responderam</i>	28	20,90	13	17,11	1	7,14
Total de Respostas	134		76		14	
(h) Sistemas Operativos						
[Técnicos (g)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	0	0,00	0	0,00
2	3	2,24	3	3,95	0	0,00
3	10	7,46	10	13,16	3	21,43
4	26	19,40	19	25,00	6	42,86
5	34	25,37	21	27,63	3	21,43
6	29	21,64	10	13,16	1	7,14
<i>Não Responderam</i>	30	22,39	13	17,11	1	7,14
Total de Respostas	134		76		14	

(i) Internet						
[Técnicos (h)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	0	0,00	0	0,00
2	2	1,49	1	1,32	1	7,14
3	10	7,46	7	9,21	1	7,14
4	17	12,69	16	21,05	3	21,43
5	40	29,85	26	34,21	7	50,00
6	39	29,10	16	21,05	1	7,14
<i>Não Responderam</i>	24	17,91	10	13,16	1	7,14
Total de Respostas	134		76		14	
(j) Correio electrónico						
[Técnicos (i)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	0	0,00	0	0,00
2	1	0,75	3	3,95	0	0,00
3	9	6,72	6	7,89	2	14,29
4	20	14,93	14	18,42	2	14,29
5	41	30,60	21	27,63	4	28,57
6	39	29,10	24	31,58	5	35,71
<i>Não Responderam</i>	22	16,42	8	10,53	1	7,14
Total de Respostas	134		76		14	
(k) Rede informática						
[Técnicos (j)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	3	2,24	0	0,00	0	0,00
2	0	0,00	4	5,26	0	0,00
3	10	7,46	7	9,21	1	7,14
4	19	14,18	10	13,16	4	28,57
5	36	26,87	16	21,05	4	28,57
6	40	29,85	29	38,16	4	28,57
<i>Não Responderam</i>	26	19,40	10	13,16	1	7,14
Total de Respostas	134		76		14	
(l) Sistema de comunicações (telefones, telefaxes, etc.)						
[Técnicos (k)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	11	8,21	3	3,95	0	0,00
2	8	5,97	7	9,21	0	0,00
3	12	8,96	11	14,47	1	7,14
4	28	20,90	23	30,26	2	14,29
5	31	23,13	16	21,05	6	42,86
6	13	9,70	7	9,21	4	28,57
<i>Não Responderam</i>	31	23,13	9	11,84	1	7,14
Total de Respostas	134		76		14	

D14) Classifique em que medida considera que a segurança do Sistema Informático do Serviço/Escola é ou pode ser importante para as suas actividades laborais/lectivas e de investigação. (6 para muito importante e 1 para pouco importante)						
[Técnicos 24)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	1	0,75	0	0,00	0	0,00
2	1	0,75	1	1,32	0	0,00
3	10	7,46	1	1,32	3	21,43
4	19	14,18	12	15,79	8	57,14
5	45	33,58	29	38,16	2	14,29
6	53	39,55	31	40,79	0	0,00
<i>Não Responderam</i>	5	3,73	2	2,63	1	7,14
Total de Respostas	134		76		14	

D15) Classifique a facilidade de acesso físico ao Sistema Informático da Escola (6 para muito difícil e 1 para muito fácil), nos seguintes pontos de acesso:						
[Técnicos 25)]						
(a) Sala de servidores						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	11	8,21	4	5,26	0	0,00
2	6	4,48	4	5,26	0	0,00
3	12	8,96	11	14,47	1	7,14
4	19	14,18	8	10,53	0	0,00
5	22	16,42	13	17,11	5	35,71
6	31	23,13	24	31,58	8	57,14
<i>Não Responderam</i>	33	24,63	12	15,79	0	0,00
Total de Respostas	134		76		14	
(b) Serviços de Informática						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	10	7,46	7	9,21	0	0,00
2	19	14,18	5	6,58	0	0,00
3	16	11,94	18	23,68	2	14,29
4	24	17,91	18	23,68	3	21,43
5	25	18,66	11	14,47	7	50,00
6	13	9,70	7	9,21	2	14,29
<i>Não Responderam</i>	27	20,15	10	13,16	0	0,00
Total de Respostas	134		76		14	
(c) Serviços administrativos/académicos/etc.						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	9	6,72	7	9,21	0	0,00
2	18	13,43	8	10,53	1	7,14
3	17	12,69	19	25,00	4	28,57
4	29	21,64	16	21,05	7	50,00
5	20	14,93	9	11,84	1	7,14
6	11	8,21	6	7,89	1	7,14
<i>Não Responderam</i>	30	22,39	11	14,47	0	0,00
Total de Respostas	134		76		14	

(d) Gabinetes de colegas						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	14	10,45	10	13,16	0	0,00
2	19	14,18	10	13,16	0	0,00
3	24	17,91	15	19,74	4	28,57
4	20	14,93	17	22,37	4	28,57
5	21	15,67	6	7,89	5	35,71
6	9	6,72	4	5,26	1	7,14
<i>Não Responderam</i>	27	20,15	14	18,42	0	0,00
Total de Respostas	134		76		14	
(e) Salas de reunião						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	17	12,69	7	9,21	0	0,00
2	16	11,94	16	21,05	0	0,00
3	21	15,67	18	23,68	6	42,86
4	24	17,91	8	10,53	6	42,86
5	12	8,96	6	7,89	0	0,00
6	9	6,72	8	10,53	2	14,29
<i>Não Responderam</i>	35	26,12	13	17,11	0	0,00
Total de Respostas	134		76		14	
(f) Átrios/corredores						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	31	23,13	14	18,42	0	0,00
2	17	12,69	12	15,79	1	7,14
3	14	10,45	17	22,37	6	42,86
4	18	13,43	6	7,89	5	35,71
5	12	8,96	4	5,26	1	7,14
6	9	6,72	7	9,21	1	7,14
<i>Não Responderam</i>	33	24,63	16	21,05	0	0,00
Total de Respostas	134		76		14	
(g) Área circundante do Serviço/Escola						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	27	20,15	6	7,89	4	28,57
2	13	9,70	8	10,53	3	21,43
3	18	13,43	18	23,68	2	14,29
4	16	11,94	11	14,47	2	14,29
5	15	11,19	4	5,26	1	7,14
6	10	7,46	10	13,16	1	7,14
<i>Não Responderam</i>	35	26,12	19	25,00	1	7,14
Total de Respostas	134		76		14	

(h) Salas de aula								
				Docentes				
				nº	%			
1				18	13,43			
2				19	14,18			
3				26	19,40			
4				20	14,93			
5				17	12,69			
6				12	8,96			
<i>Não Responderam</i>				22	16,42			
Total de Respostas				134				
(i) Laboratórios de Informática								
[Não Docentes (h)/Técnicos (h)]			Docentes		Não Docentes		Técnicos	
			nº	%	nº	%	nº	%
1			15	11,19	3	3,95	4	28,57
2			18	13,43	8	10,53	3	21,43
3			22	16,42	16	21,05	1	7,14
4			22	16,42	14	18,42	3	21,43
5			21	15,67	7	9,21	1	7,14
6			6	4,48	9	11,84	1	7,14
<i>Não Responderam</i>			30	22,39	19	25,00	1	7,14
Total de Respostas			134		76		14	
(j) Salas de informática para alunos								
							Docentes	
							nº	%
1							21	15,67
2							21	15,67
3							24	17,91
4							11	8,21
5							14	10,45
6							9	6,72
<i>Não Responderam</i>							34	25,37
Total de Respostas							134	

D16) Nos locais onde tem acesso ao Sistema Informático do Serviço/Escola, especifique que actividades estão proibidas. <i>(assinale todos os itens aplicáveis)</i>						
[Técnicos 26)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Fumar	89	66,42	57	75,00	13	92,86
Movimentar computadores instalados	70	52,24	38	50,00	7	50,00
Instalar/Movimentar periféricos	56	41,79	32	42,11	7	50,00
Ingerir bebidas	58	43,28	36	47,37	7	50,00
Participar em sessões de chat	16	11,94	27	35,53	3	21,43
Consumir alimentos	59	44,03	36	47,37	9	64,29
Efectuar o download de ficheiros	15	11,19	13	17,11	0	0,00
Realizar cópias dos seus trabalhos	13	9,70	7	9,21	1	7,14
Instalar/desinstalar <i>software</i>	65	48,51	37	48,68	6	42,86
Realizar cópias dos programas instalados	51	38,06	36	47,37	10	71,43
<i>Não Responderam</i>	29	21,64	9	11,84	1	7,14
Total de Respostas	134		76		14	

D17) Classifique, de acordo com o impacto na segurança do Sistema Informático do Serviço/Escola (6 para muito importante e 1 para pouco importante), os seguintes tipos de ameaças.						
[Técnicos 27)]						
(a) Acidentes naturais (incêndios, terremotos, inundações, etc.)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	5	3,73	4	5,26	0	0,00
2	6	4,48	3	3,95	0	0,00
3	17	12,69	10	13,16	1	7,14
4	24	17,91	11	14,47	2	14,29
5	21	15,67	10	13,16	4	28,57
6	31	23,13	25	32,89	6	42,86
<i>Não Responderam</i>	30	22,39	13	17,11	1	7,14
Total de Respostas	134		76		14	
(b) Hackers (acessos não autorizados a partir do exterior das organizações)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	1	1,32	0	0,00
2	2	1,49	0	0,00	0	0,00
3	6	4,48	4	5,26	1	7,14
4	15	11,19	7	9,21	3	21,43
5	26	19,40	15	19,74	5	35,71
6	54	40,30	38	50,00	4	28,57
<i>Não Responderam</i>	29	21,64	11	14,47	1	7,14
Total de Respostas	134		76		14	
(c) Acessos indevidos (não autorizados) a partir do interior das organizações						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	0	0,00	0	0,00
2	2	1,49	1	1,32	0	0,00
3	6	4,48	4	5,26	1	7,14
4	17	12,69	10	13,16	3	21,43
5	32	23,88	23	30,26	3	21,43
6	46	34,33	25	32,89	5	35,71
<i>Não Responderam</i>	29	21,64	13	17,11	2	14,29
Total de Respostas	134		76		14	
(d) Virus/Trojan Horses/Worms/etc.						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	0	0,00	0	0,00	0	0,00
2	3	2,24	1	1,32	0	0,00
3	4	2,99	5	6,58	1	7,14
4	14	10,45	3	3,95	4	28,57
5	31	23,13	17	22,37	6	42,86
6	52	38,81	38	50,00	2	14,29
<i>Não Responderam</i>	30	22,39	12	15,79	1	7,14
Total de Respostas	134		76		14	

(e) Roubo de informação						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	0	0,00	0	0,00
2	2	1,49	1	1,32	0	0,00
3	7	5,22	5	6,58	3	21,43
4	21	15,67	9	11,84	2	14,29
5	27	20,15	17	22,37	5	35,71
6	46	34,33	32	42,11	3	21,43
<i>Não Responderam</i>	29	21,64	12	15,79	1	7,14
Total de Respostas	134		76		14	
(f) Destruição de informação						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	0	0,00	0	0,00
2	0	0,00	1	1,32	0	0,00
3	8	5,97	4	5,26	2	14,29
4	15	11,19	8	10,53	4	28,57
5	29	21,64	19	25,00	3	21,43
6	50	37,31	32	42,11	4	28,57
<i>Não Responderam</i>	30	22,39	12	15,79	1	7,14
Total de Respostas	134		76		14	
(g) Utilização incorrecta do sistema						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	1	0,75	0	0,00	0	0,00
2	2	1,49	2	2,63	0	0,00
3	22	16,42	6	7,89	6	42,86
4	25	18,66	25	32,89	4	28,57
5	30	22,39	21	27,63	2	14,29
6	22	16,42	11	14,47	1	7,14
<i>Não Responderam</i>	32	23,88	11	14,47	1	7,14
Total de Respostas	134		76		14	
(h) Definição por defeito das <i>passwords</i> iniciais (por ex. <i>Password</i> igual ao <i>UserID</i>)						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	4	2,99	2	2,63	0	0,00
2	6	4,48	3	3,95	1	7,14
3	18	13,43	9	11,84	3	21,43
4	23	17,16	22	28,95	3	21,43
5	31	23,13	15	19,74	3	21,43
6	21	15,67	13	17,11	3	21,43
<i>Não Responderam</i>	31	23,13	12	15,79	1	7,14
Total de Respostas	134		76		14	

(i) Intercepção de mensagens de correio electrónico e respectivos anexos						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	0	0,00	0	0,00
2	1	0,75	2	2,63	0	0,00
3	12	8,96	8	10,53	4	28,57
4	13	9,70	17	22,37	4	28,57
5	40	29,85	23	30,26	4	28,57
6	35	26,12	14	18,42	1	7,14
<i>Não Responderam</i>	31	23,13	12	15,79	1	7,14
Total de Respostas	134		76		14	
(j) Falhas no fornecimento de energia eléctrica ao sistema						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	1,49	0	0,00	1	7,14
2	4	2,99	4	5,26	0	0,00
3	17	12,69	7	9,21	3	21,43
4	21	15,67	20	26,32	4	28,57
5	30	22,39	20	26,32	2	14,29
6	30	22,39	12	15,79	3	21,43
<i>Não Responderam</i>	30	22,39	13	17,11	1	7,14
Total de Respostas	134		76		14	
(k) Configuração incorrecta da <i>firewall</i>						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	1	0,75	0	0,00	0	0,00
2	5	3,73	6	7,89	0	0,00
3	8	5,97	5	6,58	3	21,43
4	20	14,93	18	23,68	3	21,43
5	37	27,61	16	21,05	3	21,43
6	31	23,13	17	22,37	4	28,57
<i>Não Responderam</i>	32	23,88	14	18,42	1	7,14
Total de Respostas	134		76		14	
(l) Falhas de funcionamento do <i>software</i> do sistema						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	0	0,00	0	0,00	0	0,00
2	3	2,24	1	1,32	1	7,14
3	12	8,96	8	10,53	2	14,29
4	16	11,94	24	31,58	3	21,43
5	40	29,85	16	21,05	5	35,71
6	33	24,63	15	19,74	2	14,29
<i>Não Responderam</i>	30	22,39	12	15,79	1	7,14
Total de Respostas	134		76		14	

(m) Falhas de funcionamento do <i>hardware</i> do sistema						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	1	0,75	0	0,00	0	0,00
2	3	2,24	1	1,32	1	7,14
3	13	9,70	7	9,21	2	14,29
4	18	13,43	23	30,26	2	14,29
5	37	27,61	18	23,68	6	42,86
6	32	23,88	15	19,74	2	14,29
<i>Não Responderam</i>	30	22,39	12	15,79	1	7,14
Total de Respostas	134		76		14	

Grupo E – Usabilidade do Sistema Informático do Serviço/Escola

E1) Recebeu formação na utilização do Sistema Informático do Serviço/Escola?						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
Não	99	73,88	27	35,53	5	35,71
Sim	31	23,13	47	61,84	9	64,29
<i>Não Responderam</i>	4	2,99	2	2,63	0	0,00
Total de Respostas	134		76		14	

E2) Com que frequência recebe formação necessária à utilização do Sistema Informático do Serviço/Escola?				
	Docentes		Não Docentes	
	nº	%	nº	%
Uma única vez	12	34,29	10	20,41
Sempre que existem mudanças no sistema	19	54,29	34	69,39
Trimestralmente	0	0,00	0	0,00
Semestralmente	0	0,00	0	0,00
Anualmente	2	5,71	2	4,08
<i>Não Responderam</i>	2	5,71	3	6,12
Total de Respostas	35		49	

E3) Classifique a relevância dessa formação. (6 para muito relevante e 1 para pouco relevante)						
[Técnicos 2]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	2	5,71	0	0,00	0	0,00
2	1	2,86	0	0,00	0	0,00
3	3	8,57	6	12,24	1	11,11
4	12	34,29	2	4,08	2	22,22
5	11	31,43	15	30,61	3	33,33
6	4	11,43	22	44,90	3	33,33
<i>Não Responderam</i>	2	5,71	4	8,16	0	0,00
Total de Respostas	35		49		9	

E3) São proporcionadas acções de formação sobre a utilização do Sistema Informático do Serviço aos utilizadores finais?		
	Técnicos	
	nº	%
Não	8	57,14
Sim	6	42,86
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

E4) Com que frequência são realizadas essas acções?		
	Técnicos	
	nº	%
Uma única vez	0	0,00
Sempre que existem mudanças no sistema	4	66,67
Trimestralmente	0	0,00
Semestralmente	0	0,00
Anualmente	0	0,00
Ocasionalmente	2	33,33
<i>Não Responderam</i>	0	0,00
Total de Respostas	6	

E4) Existe algum(uns) documento(s) acerca da utilização do Sistema Informático do Serviço/Escola?				
	Docentes		Não Docentes	
	nº	%	nº	%
Não	9	6,72	18	23,68
Não sabe	79	58,96	38	50,00
Sim	43	32,09	19	25,00
<i>Não Responderam</i>	3	2,24	1	1,32
Total de Respostas	134		76	

E5) Como tomou conhecimento desse(s) documento(s)? (assinale todos os itens aplicáveis)				
	Docentes		Não Docentes	
	nº	%	nº	%
Documento entregue no Serviço/Escola	25	54,35	10	50,00
Consulta da página <i>web</i> do Serviço/Escola	5	10,87	0	0,00
Informação dos serviços de informática	25	54,35	5	25,00
Informação de colega	8	17,39	9	45,00
Informação afixada no Serviço/Escola	3	6,52	0	0,00
Outro meio	2	4,35	0	0,00
<i>Não Responderam</i>	2	4,35	1	5,00
Total de Respostas	46		20	

E6) Classifique a utilidade desse(s) documento(s). (6 para muito útil e 1 para pouco útil)				
	Docentes		Não Docentes	
	nº	%	nº	%
1	1	2,17	0	0,00
2	2	4,35	1	5,00
3	3	6,52	1	5,00
4	10	21,74	3	15,00
5	18	39,13	10	50,00
6	9	19,57	4	20,00
<i>Não Responderam</i>	3	6,52	1	5,00
Total de Respostas	46		20	

E5) São elaborados alguns documentos acerca da utilização do Sistema Informático do Serviço para apoio aos utilizadores finais?		
	Técnicos	
	nº	%
Não	3	21,43
Sim	11	78,57
<i>Não Responderam</i>	0	0,00
Total de Respostas	14	

E7) Classifique a facilidade de utilização do Sistema Informático do Serviço/Escola. (6 para fácil de utilizar e 1 para difícil de utilizar)						
[Técnicos 6)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	5	3,73	0	0,00	0	0,00
2	2	1,49	0	0,00	0	0,00
3	12	8,96	9	11,84	1	7,14
4	24	17,91	21	27,63	2	14,29
5	49	36,57	33	43,42	6	42,86
6	26	19,40	13	17,11	5	35,71
<i>Não Responderam</i>	16	11,94	0	0,00	0	0,00
Total de Respostas	134		76		14	

E8) Classifique a facilidade de aprendizagem do Sistema Informático do Serviço/Escola. (6 para fácil de aprender e 1 para difícil de aprender)						
[Técnicos 7)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	6	4,48	0	0,00	0	0,00
2	4	2,99	0	0,00	0	0,00
3	8	5,97	9	11,84	1	7,14
4	30	22,39	26	34,21	2	14,29
5	44	32,84	31	40,79	9	64,29
6	22	16,42	10	13,16	2	14,29
<i>Não Responderam</i>	20	14,93	0	0,00	0	0,00
Total de Respostas	134		76		14	

E9) Classifique, relativamente à usabilidade do Sistema Informático do Serviço/Escola (6 para muito importante e 1 para pouco importante), a relevância dos seguintes aspectos:						
[Técnicos 8]						
(a) Facilidade de acesso						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	0	0,00	0	0,00	0	0,00
2	0	0,00	1	1,32	0	0,00
3	8	5,97	2	2,63	1	7,14
4	14	10,45	13	17,11	2	14,29
5	47	35,07	34	44,74	7	50,00
6	55	41,04	23	30,26	4	28,57
<i>Não Responderam</i>	10	7,46	3	3,95	0	0,00
Total de Respostas	134		76		14	
(b) Disponibilidade						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	0	0,00	0	0,00	0	0,00
2	0	0,00	0	0,00	0	0,00
3	4	2,99	4	5,26	1	7,14
4	18	13,43	15	19,74	3	21,43
5	39	29,10	33	43,42	4	28,57
6	63	47,01	21	27,63	6	42,86
<i>Não Responderam</i>	10	7,46	3	3,95	0	0,00
Total de Respostas	134		76		14	
(c) Adequação às necessidades						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	0	0,00	0	0,00	0	0,00
2	2	1,49	2	2,63	0	0,00
3	8	5,97	3	3,95	1	7,14
4	23	17,16	15	19,74	3	21,43
5	38	28,36	28	36,84	6	42,86
6	51	38,06	22	28,95	4	28,57
<i>Não Responderam</i>	12	8,96	6	7,89	0	0,00
Total de Respostas	134		76		14	
(d) Apoio técnico à utilização						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	1	0,75	0	0,00	0	0,00
2	7	5,22	1	1,32	0	0,00
3	17	12,69	2	2,63	2	14,29
4	23	17,16	22	28,95	7	50,00
5	40	29,85	22	28,95	3	21,43
6	37	27,61	22	28,95	2	14,29
<i>Não Responderam</i>	9	6,72	7	9,21	0	0,00
Total de Respostas	134		76		14	

(e) Interface com o sistema						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	1	0,75	1	1,32	0	0,00
2	5	3,73	2	2,63	0	0,00
3	14	10,45	6	7,89	1	7,14
4	28	20,90	19	25,00	6	42,86
5	46	34,33	26	34,21	6	42,86
6	23	17,16	12	15,79	1	7,14
<i>Não Responderam</i>	17	12,69	10	13,16	0	0,00
Total de Respostas	134		76		14	
(f) Regras de utilização						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	0	0,00	0	0,00	0	0,00
2	0	0,00	1	1,32	0	0,00
3	22	16,42	6	7,89	2	14,29
4	37	27,61	19	25,00	5	35,71
5	42	31,34	28	36,84	4	28,57
6	21	15,67	16	21,05	3	21,43
<i>Não Responderam</i>	12	8,96	6	7,89	0	0,00
Total de Respostas	134		76		14	
(g) Conhecimento prévio do sistema						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	5	3,73	1	1,32	0	0,00
2	8	5,97	4	5,26	3	21,43
3	20	14,93	11	14,47	5	35,71
4	37	27,61	22	28,95	4	28,57
5	37	27,61	15	19,74	2	14,29
6	15	11,19	16	21,05	0	0,00
<i>Não Responderam</i>	12	8,96	7	9,21	0	0,00
Total de Respostas	134		76		14	
(h) Participação no desenvolvimento/implementação do sistema						
	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	11	8,21	3	3,95	0	0,00
2	16	11,94	4	5,26	3	21,43
3	27	20,15	6	7,89	3	21,43
4	29	21,64	17	22,37	4	28,57
5	16	11,94	24	31,58	4	28,57
6	18	13,43	12	15,79	0	0,00
<i>Não Responderam</i>	17	12,69	10	13,16	0	0,00
Total de Respostas	134		76		14	

E10) Classifique em que medida considera que a usabilidade do Sistema Informático do Serviço/Escola é ou pode ser importante para as suas actividades laborais, lectivas e de investigação. (6 para muito importante e 1 para pouco importante)						
[Técnicos 9)]	Docentes		Não Docentes		Técnicos	
	nº	%	nº	%	nº	%
1	0	0,00	1	1,32	0	0,00
2	1	0,75	0	0,00	0	0,00
3	1	0,75	2	2,63	1	7,14
4	20	14,93	10	13,16	1	7,14
5	53	39,55	23	30,26	5	35,71
6	52	38,81	39	51,32	7	50,00
<i>Não Responderam</i>	7	5,22	1	1,32	0	0,00
Total de Respostas	134		76		14	

