UNIVERSIDADE ABERTA INSTITUTO SUPERIOR TÉCNICO

Risk assessment model in compliance with GDPR

Pedro Miguel Nunes Oliveira Machado

Mestrado em Informação e Sistemas Empresariais

(mestrado em associação)

Ano de conclusão

2021

Esta página foi intencionalmente deixada em branco

UNIVERSIDADE ABERTA INSTITUTO SUPERIOR TÉCNICO

Risk assessment model in compliance with GDPR

Pedro Miguel Nunes Oliveira Machado

Mestrado em Informação e Sistemas Empresariais

(mestrado em associação)

Tese orientada pelo Professor Doutor José Henrique Pereira São Mamede e coorientada pelo Professor Doutor Miguel Leitão Bignolas Mira da Silva

Ano de conclusão

2021

Esta página foi intencionalmente deixada em branco

RESUMO

Hodiernamente, a sociedade é incitada a aderir a novas tendências tecnológicas, que tornam os cenários de risco de privacidade cada vez mais complexos. Sem Privacidade não há Liberdade, e sem Liberdade não há Democracia. Em suma, sem Privacidade é a própria Democracia e o Estado de Direito que estão em risco.

Não obstante do Regulamento Geral sobre a Proteção de Dados (RGPD) vir harmonizar conceitos e regras, nem todos resultam claro, quer na definição quer na aplicabilidade, existindo uma ausência de orientações práticas no RGPD e demais legislação aplicável, bem como na doutrina existente, promovendo incerteza jurídica e conduzindo a dificuldades de implementação em conformidade com a legislação.

A gestão de risco é decisiva para a correta aplicação dos princípios legais e regulamentares da proteção de dados pessoais, assumindo-se como instrumento impreterível ao cumprimento das obrigações legais, a fim de garantir os direitos, liberdades e garantias fundamentais, constitucionalmente previstas. Todavia, não resulta indubitavelmente evidente para o mercado, quais as diferenças entre o risco para a(s) empresa(s) e risco para o(s) titular(es) dos dados pessoais, levando muitas organizações a focar unicamente nos penosos regimes sancionatórios, danos reputacionais, financeiros, entre outros. Embora estes sejam relevantes para as organizações, não cumprem a totalidade das obrigações previstas na lei.

O desenvolvimento de um modelo de avaliação de risco centrado nos titulares dos dados, permite orientar no cumprimento das obrigações legais em matérias de privacidade/dados pessoais, contribuindo para a conformidade e como os regimes indemnizatórios podem vir a ser aplicados mais adequadamente, tendo em conta os reais efeitos na esfera jurídica dos titulares dos dados, contribuindo deste modo para uma melhor harmonização e transparência na gestão dos dados pessoais.

Palavras-chave: Gestão de Risco, Privacidade, Proteção de Dados, Conformidade, Direitos Fundamentais, Titular de Dados, RGPD.

Esta página foi intencionalmente deixada em branco

ABSTRACT

Nowadays, society is incited to adhere to new technological trends, which make privacy risk scenarios increasingly complex. Without Privacy there is no Freedom, and without Freedom there is no Democracy. In short, without Privacy it is Democracy itself and the Rule of Law that are at risk.

Despite the General Data Protection Regulation (GDPR) is harmonizing concepts and rules, not all are clear, either in definition or in its applicability, and there is an absence of practical guidelines in the GDPR and other applicable legislation, as well as in the existing doctrine, promoting legal uncertainty and leading to difficulties of implementation in accordance with the legislation.

Risk management is decisive for the correct application of legal and regulatory principles of personal data protection, assuming itself as an indispensable instrument for the fulfillment of legal obligations, to guarantee the fundamental rights, freedoms and guarantees, constitutionally provided.

However, it is not undoubtedly clear to the market what the differences are between the risk to the company(ies) and the risk to the holder(s) of the personal data, leading many organizations to focus solely on the painful sanctioning regimes, reputational and financial damages. While these are relevant to the organizations, they do not meet the full obligations under the law.

The development of a data subject-centric risk assessment model provides guidance on how to comply with legal obligations in privacy/personal data matters, contributing to compliance and how compensation regimes can be applied more appropriately, taking into account the real effects on the data subjects' legal sphere, contributing to a better harmonization and transparency in the management of personal data.

Keywords: *Risk Management, Privacy, Data Protection, Compliance, Fundamental Rights, Data Owners, GDPR.*

Esta página foi intencionalmente deixada em branco

AGRADECIMENTOS

Agradeço a Deus o Seu infinito Amor e a Sua Presença na minha vida!

À minha esposa Raquel e aos meus filhos; Afonso, Constança e Carminho, pelo amor, apoio e compreensão que manifestaram, durante todo o tempo que dediquei à produção deste trabalho. Amo-vos incondicionalmente!

O meu reconhecimento e agradecimento aos meus pais, pelo apoio permanente.

Os meus profundos e sinceros agradecimentos ao Professor Doutor José Henrique Pereira São Mamede e ao Professor Doutor Miguel Leitão Bignolas Mira da Silva, pela orientação e coorientação, respetivamente, bem como nas suas pessoas, expresso os meus sinceros agradecimentos a todos os docentes da Universidade Aberta e do Instituto Superior Técnico, que tanto conhecimento ministraram ao longo das cadeiras do mestrado.

Agradeço à Associação de Encarregados de Proteção de Dados, seus associados e demais reconhecidos especialistas nacionais e internacionais consultados, de perfis diversos, entre advogados de reconhecidas sociedades, quadros de órgãos de regulação, engenheiros, consultores, etc., a quem também procurei obter opiniões técnicas especializadas, para melhor elaborar a presente tese.

Finalmente, gostaria de agradecer aos meus amigos e colegas, especialmente os que me sendo mais chegados, manifestaram o seu apoio e encorajamento reiterado, para o sucesso e bom cumprimento desta missão.

Esta página foi intencionalmente deixada em branco

ÍNDICE

ÍNDICE DE TABELAS

ÍNDICE DE FIGURAS

ACRÓNIMOS

AEPD - Agencia Española de Protección de Datos

CEDP - Comité Europeu de Proteção de Dados

CIPL - Centre for Information Policy Leadership

CNIL - Commission Nationale de l'Informatique et des Libertés

CNPD - Comissão Nacional de Proteção de Dados

DLG - Direitos, Liberdades e Garantias

DPIA - Data Protection Impact Assessment

EDPB - European Data Protection Board

EDPS - European Data Protection Supervisor

EIPD - Evaluación de Impacto en la Protección de Datos Personales

ENISA - European Network and Information Security Agency

FMI - Fase da Metodologia de Investigação

GDPR - General Data Protection Regulation

ICO - Information Commissioner's Office

IoT - Internet of Things

ISO - International Organization for Standardization

M_o_R - Management of Risk

NIST - National Institute of Standards and Technology

OECD - Organisation for Economic Co-operation and Development

PbD - Privacy by Design

PIA - Privacy Impact Assessment

RGPD - Regulamento Geral sobre a Proteção de Dados

UDHR - Universal Declaration of Human Rights

WEF - World Economic Forum

WP29 - Article 29 Working Party

1 INTRODUÇÃO

Uma das mais importantes referências históricas à Privacidade, surge em 1890 nos EUA, num artigo jurídico publicado pela prestigiada revista "*Harvard Law Review*", subordinado ao tema "*The Right to Privacy*", Samuel Warren e Louis Brandeis definem "a proteção do domínio privado como o fundamento da liberdade individual na era moderna"[1]. Não obstante de passados 130 anos, reitera-se o princípio e a importância que a privacidade assume "na era moderna", aquando a adesão a novas tendências tecnológicas, são naturalmente majorados os cenários de risco, em número e em complexidade.

Conforme previsto na Declaração Universal dos Direitos Humanos[2], nos seus artigos 12.º e 17.º, torna-se, pois, fundamental, a consciência de que *sem Privacidade não há Liberdade, e sem Liberdade não há Democracia. Em suma, sem Privacidade é a própria Democracia e o Estado de Direito que estão em risco*[3].

A proteção de dados pessoais é, pois, fundamental, no cumprimento dos direitos, liberdades e garantias, previstos na Constituição da República Portuguesa[4].

A gestão dos riscos é decisiva para uma correta aplicação dos princípios legais e regulamentares da proteção dos dados pessoais, sendo um instrumento elementar no cumprimento de direitos, liberdades e garantias fundamentais das pessoas singulares.

Todavia, não é claro para o mercado, na sua aplicação regular e nas respostas aos desafios empresariais hodiernos a que o mercado se encontra sujeito, quais as diferenças entre o risco para as empresas e o risco para o(s) titular(s) de dados pessoais, levando muitas organizações a gerir o risco para a privacidade, com potencial de incorrer em regime sancionatório doloroso (multa ou prisão), uma vez que visam; danos reputacionais, impactos financeiros e de solvabilidade, entre outros demais riscos para o negócios, desfocando o âmago dos titulares dos dados pessoais.

Pese embora, as referidas dimensões de negócio se considerem válidas e efetivamente relevante para a organização, não visam o cumprimento das obrigações previstas no ordenamento jurídico em matéria de dados pessoais, que consagram o foco nos titulares dos dados pessoais.

O Regulamento Geral de Proteção de Dados ou "RGPD"[5], bem como as demais obrigações legais aplicáveis em matérias de dados pessoais[6], tornam particularmente evidente a importância da gestão de risco no cumprimento das obrigações de proteção de dados pessoais.

O RGPD é claro na sua definição taxonómica ao risco, afirmando de modo inequívoco que "*o risco para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem variar, pode resultar de operações de tratamento que envolvam dados pessoais suscetíveis de* ***causar danos físicos, materiais ou imateriais****, nomeadamente quando o tratamento possa dar origem a discriminação, roubo de identidade ou perda financeira, danos à reputação, perda de confidencialidade de dados pessoais protegidos por sigilo profissional, pseudonimização não autorizada, ou qualquer outra perda económica ou social importante; quando os sujeitos a dados podem ser privados dos seus direitos e liberdades ou impedidos de exercer o controlo sobre os seus dados pessoais*".[1]

Da mesma forma e para que não restem dúvidas, reitera que "*(...) o avaliar os riscos para a segurança dos dados, deve ser tida em conta os riscos apresentados pelo tratamento de dados pessoais, tais como destruição acidental ou ilícita, perda, alteração e divulgação não autorizada de ou acesso a dados pessoais transmitidos, armazenados ou tratados de outra forma, o que pode dar origem, nomeadamente, a* ***danos físicos, materiais ou imateriais****".* [2]

[1] Considerando 75 do Regulamento Geral de Proteção de Dados (RGPD)
[2] Considerando 83 do Regulamento Geral de Proteção de Dados (RGPD)

RISCO DE TRATAMENTO

- Destruição acidental
- Destruição ilícita
- Perda
- Alteração não autorizada
- Divulgação não autorizada
- Acesso não autorizado

✓ Considerando 83
✓ n.2 do artigo 32.º RGPD

RISCO DE SEGURANÇA DOS DADOS

- Confidencialidade
- Integridade
- Disponibilidade
- Autenticidade
- Resiliência

✓ Considerando 49
✓ Alínea f) n.1 artigo 5.º
✓ Alínea b) n.1 artigo 32.º

RISCO PARA O TITULAR

- Danos físicos
- Danos materiais
- Danos imateriais

✓ Considerando 2
✓ Considerando 4
✓ Considerando 85
✓ n.2 artigo 1.º
✓ n.1 artigo 82.º

Figura 1 - Relação holística dos riscos nos termos do RGPD

Resulta, pois, evidente, a importância de tornar claro o âmbito do termo "*risco*" na proteção de dados pessoais, a fim de obter a conformidade com o RGPD e demais legislação aplicável em matérias de dados pessoais.

A assimetria nas coimas aplicadas no Espaço Europeu e Reino Unido[7] (*pós-brexit*), corporiza a indefinição exata de critérios, prevendo a legislação unicamente os montantes máximos das coimas, sem orientações prescritivas concretas, relativamente aos critérios a considerar. Como resultado, tem-se vindo a observar no Espaço Europeu, a atribuição de variadas sanções assimétricas nos diferentes estados membros da UE.

Está previsto no artigo 82.º do RGPD, que qualquer pessoa que tenha sofrido danos devido a uma violação do RGPD, tem direito a receber indemnização pelos danos sofridos. Apesar destes valores indemnizatórios ao(s) titular(es) afetados, tenderem a ser negligenciados, não deixam de assumir relevância estratégica e operacional.

Urge a definição de uma metodologia de avaliação de risco, que permita uma harmonização e exatidão metodológica, procurando a obtenção de avaliações que considerem uma apreciação dos reais danos envolvidos. Só deste modo, por intermédio de uma visão harmonizada e comum, será possível assegurar a equidade expectável nos montantes de coimas a aplicar, bem como dos valores indemnizatórios que visem compensar/reparar o dano causado.

1.1 MOTIVAÇÃO

Vivemos numa sociedade dependente da tecnologia, sujeita a pressões a curto-prazo que conduzirão à Sociedade 5.0[8] e potencia diversos riscos.

O World Economic Forúm (WEF) conclui no seu relatório[9] "*COVID-19 Risks Outlook*" publicado em maio de 2020, que a moderna adoção abruta e dependência de novas tecnologias, "*promove naturalmente riscos emergentes, que levam a um aumento dos riscos de sobrecarga e desagregação de infraestruturas, cibercrime,* ***violações de privacidade*** *e desigualdades*". Reitera o WEF num outro relatório[10], que "*a pandemia COVID-19 está a ter um impacto dramático na sociedade e forçou todos a ficarem fortemente dependentes da Internet e da sua economia digital – o que normalmente levaria anos aconteceu agora em meses. A situação tem evidenciado as questões sistémicas intrínsecas na conjuntura das infraestruturas digitais, da economia, da geopolítica* ***e da privacidade*** *(…). Se estes não forem tratados de forma holística, os riscos crescentes podem ter um efeito dominó que é suscetível de afetar as funções críticas e os ecossistemas da indústria a nível global*."

Atendendo a que as ameaças referidas são comummente instrumentalizadas para visar dados pessoais, qualquer postura negligente dos efeitos da evolução tecnológica na majoração de riscos de privacidade, corporiza uma falta de consciência, que resultará em comportamentos e decisões promotores de danos.
Segundo relatório[11] da OCDE publicado a 2018, referente a dados de 2015, Portugal surge na oitava posição, nos países em que os indivíduos experienciaram violações de privacidade, verificando-se em 2015 um aumento comparativamente a 2010.

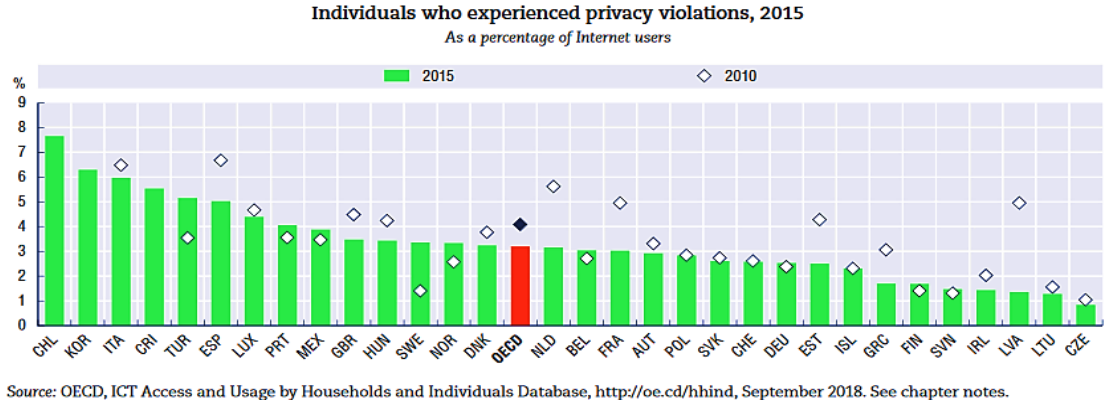


Figura 2 - OECD (2019), "Online privacy", in Measuring the Digital Transformation

As avaliações de risco assumem especial relevância nos termos do contexto hodierno, previamente referenciado, onde as assimetrias nas avaliações de risco, conduzem a diferentes respostas e à aplicação de coimas assimétricas. Esta dificuldade, influencia o mercado no desenvolvimento de ferramentas de gestão da privacidade, e à operacionalização da proteção de dados pessoais, de forma insatisfatória face às reais obrigações legais.

A existência de alguma incerteza jurídica e arbitrariedade[12] no ordenamento jurídico, agravada à falta de orientações e de metodologias concretas na avaliação do risco para a privacidade, permitindo providenciar um resultado harmonizado que sirva de utilidade para a toda a Sociedade, (i.e., Autoridades de Controlo, Governos, Tribunais).

1.2 PROBLEMA DE INVESTIGAÇÃO

A sociedade assume uma dependência crescente da tecnologia, o que torna a conformidade com o RGPD um requisito cada vez mais importante. Todavia, quanto à forma como a avaliação de risco nos dados pessoais deve ser realizada, acresce a incerteza jurídica e a falta de objetividade, que dificulta o seu exercício.

De referir também, a falta de orientação específica, quanto ao cálculo do risco nos dados pessoais, que permita harmonizar a avaliação/cálculo, independentemente da(s) entidade(s) que o avaliem e/ou dos seus respetivos interesses, sendo esperado que a conclusão dos resultados obtidos seja a mesma (i.e., a avaliação realizada por um tribunal, empresa ou Autoridade, sobre o mesmo objeto de avaliação, deve obter as mesmas conclusões, afastando subjetividades). Deste modo, pretende-se responder às seguintes questões de investigação:

Q1. Que processo de avaliação de risco pode uma organização implementar, em conformidade com o RGPD?
Q2. Como calcular o risco na proteção de dados pessoais?
Q3. Como obter orientação do valor indemnizatório potencial a pagar aos titulares?

1.3 OBJETIVOS E RESULTADOS ESPERADOS

O objetivo, pois, desta tese, consiste na apresentação de uma metodologia de avaliação de risco para a privacidade, e de acordo com o RGPD, que aborde de forma objetiva as dimensões legalmente previstas, permitindo orientar uma avaliação adequada do risco, atendendo aos direitos e liberdades fundamentais dos titulares dos dados pessoais, permitindo inclusive a possibilidade de quantificar o potencial valor indemnizatório aos titulares, tendo como objetivos:

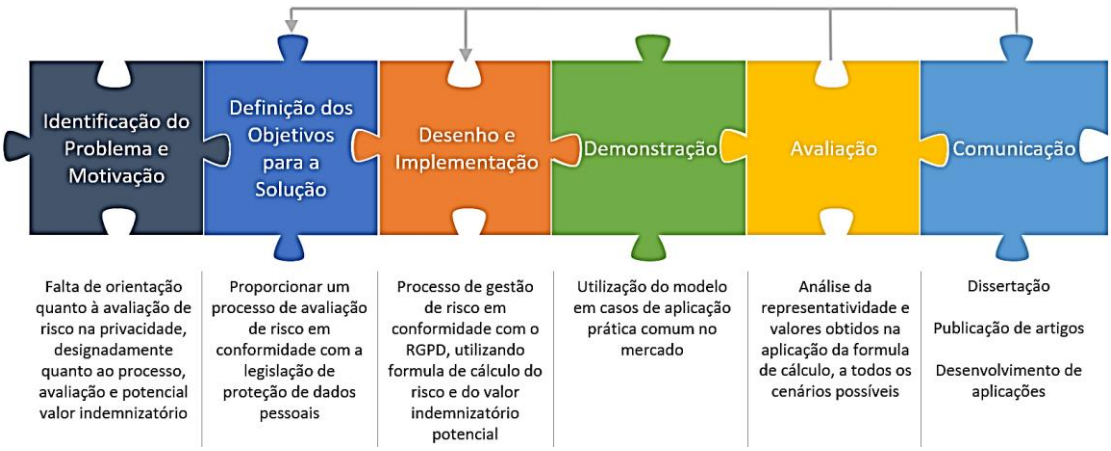
- Desenhar um processo de avaliação de risco para os titulares de dados;
- Orientar o cálculo de risco em conformidade com a legislação de privacidade;
- Providenciar uma orientação para obtenção do valor indemnizatório.

1.4 METODOLOGIA DE INVESTIGAÇÃO

A proteção de dados pessoais deve ser entendida como uma disciplina de investigação aplicada, uma vez que se aplicam teorias de outras disciplinas, tais como a gestão, informática, direito, ciências sociais, entre outras, a fim de resolver os problemas relacionados com os dados pessoais nas organizações, sendo fundamental no cumprimento do RGPD.

Tendo em conta as investigadas[13] semelhanças entre o *Design Science (DS)* e o *Action Research (AR)*, subscritas por prestigiados investigadores[14] [15], conclui-se que as principais distinções[16] fundamentam-se nas suas origens conceptuais, permitindo uma aplicação prática relevante ao objeto de investigação.

Deste modo, é assim utilizada a metodologia de investigação *Design Science Research Methodology (DSRM)*, sendo esta baseada em literatura existente e disciplinas conexas, incorporando princípios, práticas e procedimentos necessários, cumprindo com três objetivos; (i) ser consistente com a literatura existente pela coerência com a teoria e prática de investigações prévias, (ii) proporcionar um processo sequencial nominal e (iii) constituir um modelo mental para as características dos resultados da investigação. Prevê-se deste modo um processo que visa incluir as seguintes seis etapas:



Pretende-se assim, com base em DRSM, contribuir para a investigação em proteção de dados pessoais, num quadro de comum compreensão.

1.5 ESTRUTURA DO DOCUMENTO

A presente dissertação inicia no **Capítulo 1** – Introdução, que explica a motivação, os problemas de investigação, os objetivos e resultados esperados, bem como a metodologia de investigação utilizada e a presente estrutura do documento.

O **Capítulo 2** – Enquadramento teórico, introduz princípios gerais e uma explanação sobre conceitos de risco e de privacidade, respetivamente, corporizando estes uma relevante importância para o correto entendimento da presente investigação.

No **Capítulo 3** – Proposta de investigação, é introduzido uma contextualização seguida do entendimento e opinião técnica obtida por via de questionários. Posteriormente é apresentada a proposta de avaliação do risco de privacidade, seguindo-se um modelo de análise de compensação de danos e uma avaliação e análise observável ao modelo proposta.

Quanto ao **Capítulo 4** – Avaliação e casos de aplicação prática, apresenta a simulação de cenários de aplicação, bem como a demonstração da aplicação em dois casos reais (demonstração #1 e #2).

Finalmente, o **Capítulo 5** – Conclusões, apresenta as principais conclusões, bem como as limitações e proposta de trabalho futuro.

2 ENQUADRAMENTO TEÓRICO

Quando se procede à eleição de uma norma a seguir, a maioria das decisões ocorre de modo episteme, elegendo por motivos de populismo e familiaridade com a mesma, onde raramente se ponderam as definições taxonómicas e terminológicas estruturais, no alinhamento de conceitos e de linguagem.

Não obstante da lei nacional[17] e europeia[18] citar nas últimas décadas a importância dos riscos para os direitos e liberdades das pessoas singulares, exigindo inclusive, em determinados casos, a sua avaliação concreta, promove assim a necessidade de orientações específicas e inequívocas que permitam que a mesma avaliação de risco, ao respeitar critérios comuns, permita a obtenção dos mesmos resultados na avaliação do(s) risco(s) para o(s) titular(es) de dados pessoais.

2.1 PRIVACIDADE

O *Grupo de Trabalho do Artigo 29.º* (WP29), constituído pelas autoridades de controlo em matéria de proteção de dados de cada Estado-Membro e pela Autoridade Europeia para a Proteção de Dados, que veio a dar origem ao atual *Comité Europeu de Proteção de Dados* (CEPD), publicou a 30 de maio de 2014 uma orientação[19] perentória, e que eleva a importância do tema, ao afirma que "a abordagem baseada no risco ganhou muito mais atenção nas discussões no Parlamento Europeu e no Conselho sobre a proposta do Regulamento Geral sobre a Proteção de Dados".

Para além das alterações que o RGPD veio a sofrer desde a publicação dessa orientação em 2014 até à sua versão final, verifica-se que para além das obrigações de segurança (artigo 32º) e da realização de avaliação de impacto sobre a proteção de dados (artigo 35º) já prescrita no projeto do Regulamento, a abordagem baseada no Risco foi amplamente alargada e refletida noutras medidas, tais como a proteção de dados por defeito (PbD), documentação e códigos de conduta (artigo 40º).

Ainda que o RGPD refira instrumentos que, procurem facilitar a avaliação fiável e relativamente objetiva do risco (vide WP218), as diferenças metodologias de avaliação

conduzem naturalmente a assimetrias de perceção e resultados, contribuindo para uma urgente harmonização metodológica.

O *Centre for Information Policy Leadership* (CIPL), procura juntar a indústria, autoridades, reguladores, e decisores políticos, para desenvolver soluções e melhores práticas de privacidade, fundamental na era da informação moderna, publicou igualmente em 2014 e mais tarde em 2016, um conjunto de orientações[20][21][22] bastante completas das obrigações previstas no RGPD em matérias de avaliação de risco.

Importa evidenciar a assimetria na popularidade e pesquisa por estas entidades, enquanto fontes de orientação sobre temas relacionados com proteção de dados pessoais.

Enquanto que, em Portugal o WP29 tornou-se uma entidade de referência, muito pela promoção das suas orientações pela *Comissão Nacional de Proteção de Dados* (CNPD), na qual tem participação, embora o CIPL seja significativamente mais pesquisado em todo o mundo, especialmente pelo facto de não ser estritamente "Europeu", conta com um volume de pesquisas muito significativa dos EUA, Canadá, India e Austrália, conforme se pode constatar nas Figuras 6 e 7 abaixo, obtidas no Google Trends[23]:

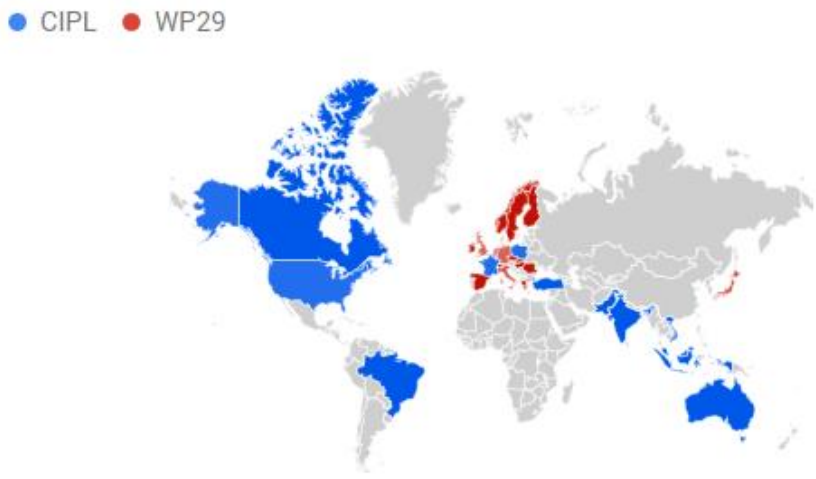


Figura 3 - Análise da origem de pesquisas por região

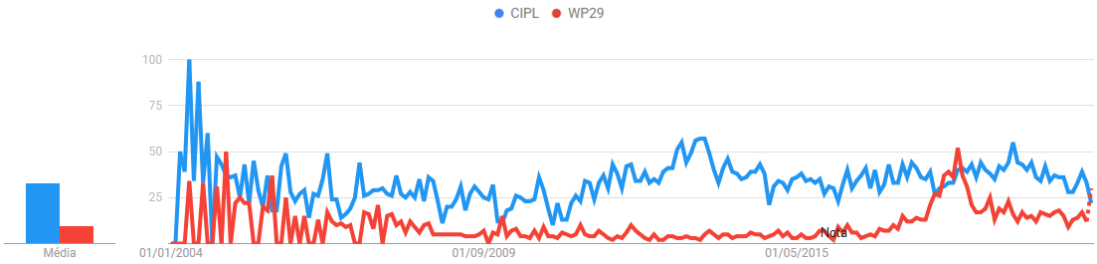


Figura 4 - Relevância do volume de pesquisas em todo o mundo

Figura 5 - Relevância do volume de pesquisas em Portugal

Sem prejuizo das orientações do CIPL e do WP29 (atual CEPD), a Autoridade de Controlo Francesa – *Commission Nationale de l'informatique et des Libertés* (CNIL), para além da publicação de orientações[24]-[25], disponibilizou gratuitamente uma aplicação[26], traduzida em várias línguas, promovendo a sua utilização em diferentes países, facilitando a operacionalização das Avaliação de Impacto da Proteção de Dados (AIPD/DPIA) e proporcionando a realização de um questionário assistido, que vise simplificar a avaliação de risco de proteção de dados pessoais, nos termos do RGPD.

Acontece que, o resultado da metodologia e respetivas conclusões da avaliação da aplicação DPIA da CNIL, incide numa análise do risco para a segurança dos dados (“acesso ilegítimo dos dados”; “modificação indesejada dos dados”; “desaparecimento dos dados”) e não no “risco para os direitos e liberdades das pessoas singulares”, *vide* Figura 9 e 10.

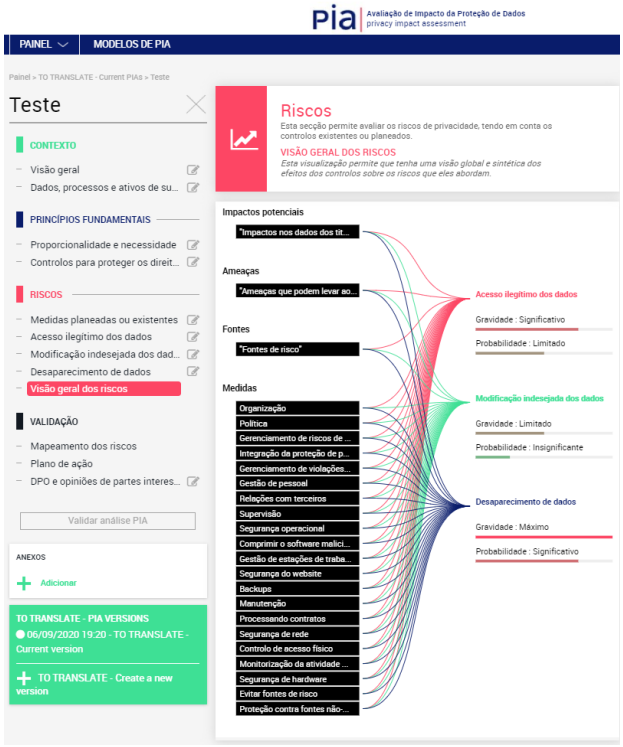


Figura 6 – Perspetiva holística de riscos no PIA v2.3.0

Figura 7 - Mapeamento de riscos PIA v2.3.0

Sem prejuízo do enorme valor e contributo da ferramenta, que a CNIL disponibiliza gratuitamente, resulta claro que, a avaliação dos riscos devia incidir sobre os direitos e liberdades dos titulares dos direitos, conforme previsto na alínea c) nº7 do artigo 35º do RGPD, e não centrado nas medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais, conforme também previsto na alínea d) nº7 do mesmo artigo.

Importa igualmente referir que, além da *framework* de *Privacy Impact Assessment* da CNIL, procurando a conformidade com as orientações do WP29[27], têm sido publicadas outras *frameworks*, por outros países Europeus, nomeadamente:

- Alemanha; publicou a *Standard Data Protection Model* (SDM)[28], com grande foco nos dados, sistemas e processos (denominado por componentes), apresenta orientações relevantes, contudo de muito alto-nível. Não apresenta orientações especificas de como devem ser analisados os riscos para os direitos e liberdades fundamentais;

- Espanha; conta com a publicação do *Guía para una Evaluación de Impacto en la Protección de Datos Personales* (EIPD)[29] da *Agencia Española de Protección de Datos* (AEPD). Sendo uma orientação muito completa, alinhando com a ISO/IEC27005, apresenta limitação na avaliação do risco e aferição da compensação indemnizatória, em cumprimento do artigo 82º do RGPD;
- Reino Unidos; conta com a publicação da *Information Commissioner's Office* (ICO), denominado por *Conducting privacy impact assessments code of practice*[30], proporciona uma visão de alto-nível e sem referência à análise dos direitos e liberdades fundamentais e aferição indemnizatória.

2.2 RISCO

Não obstante da permanente invocação hodierna do termo risco, existem diversas referências, especialmente em normas, que apresentam diferentes definições do termo risco. Na verdade, aquando se procede à eleição de uma norma a seguir, em detrimento de outras semelhantes, a maioria das decisões ocorre de modo episteme, elegendo por motivos de populismo e familiaridade com a norma, onde raramente se ponderam as definições taxonómicas e terminológicas estruturais, no alinhamento de conceitos e de linguagem.

Quando se procede à aplicação de uma norma, esta deve ser realizada de um modo contextualizado ao âmbito em causa, procurando proporcionar o melhor ajustamento e adequação ao contexto, seja ele endógeno ou exógeno, que permita a mais adequada aplicação e obtenção dos seus melhores resultados.

A definição de termos e a adequada gestão do risco e respetiva avaliação, assumem um papel fundamental no cumprimento das obrigações previstas no RGPD. Todavia e sem prejuízo da definição que o risco e a avaliação de risco assumem no contexto da proteção de dados pessoais, a qual terá o seu estudo profundado na presente tese, assume-se como fundamental a definição e compreensão genérica do termo "risco" e "avaliação de risco".

Genericamente, à avaliação de risco assume especial relevância, por ser onde se procura identificar preditivamente os eventos futuros, identificando os ativos

relevantes, as vulnerabilidades e ameaças, e por fim calculando o seu nível de risco. Naturalmente que esta fase exige uma visão holística, procurando entender os cenários de risco como um todo e não pela individualidade das suas partes.

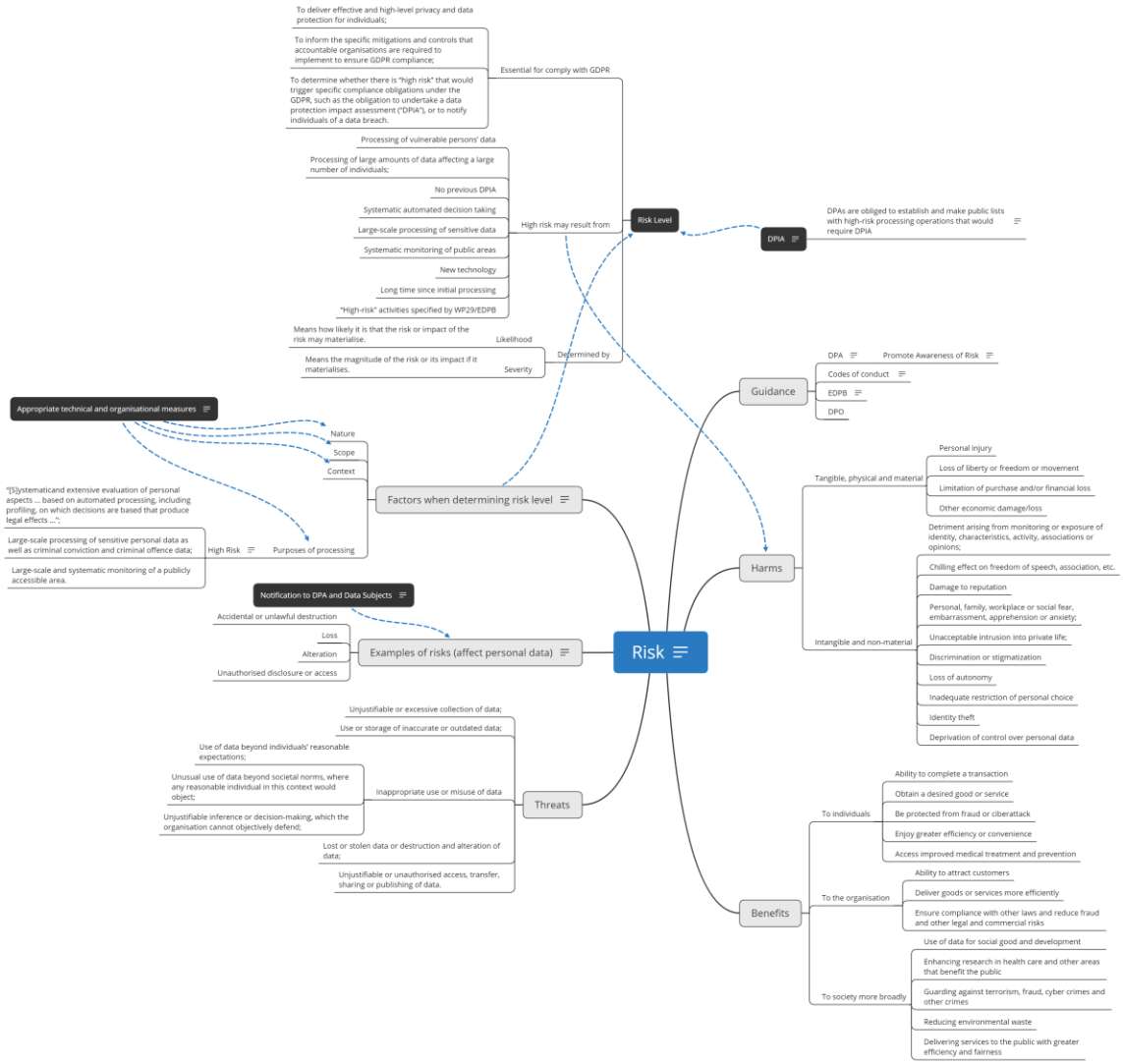


Figura 8 - Morfologia do risco na privacidade

Conforme resulta visível na Figura 8, a realização de uma adequada avaliação de risco constitui um exercício complexo, que depende muitas vezes da qualidade da informação obtida pela: realização de questionários; workshops; entrevistas; exercícios de observação; e/ou simulação de cenários, que permitam um levantamento exato e rigoroso de informação, que vise a identificação e a avaliação dos eventos de risco.

Orientação de acordo com as normas ISO

As normas ISO, têm assumido uma importante referencia internacional, contribuindo naturalmente com relevância para a elaboração do presente estudo.

Não obstante, importa clarificar que as normas ISO estão organizadas em diferentes tipos, de acordo com o seu propósito, podendo assumir as seguintes diferentes naturezas;

- Vocabulários: visa uniformizar e definir termos, cabendo nesta categoria as seguintes;
    - ISO/IEC 27000:2018
    - ISO/Guide 73:2009
- Requisitos: proporcionam uma estrutura de alto nível, de requisitos genéricos com referências normativas e vocabulários que vise uma linguagem comum. Como exemplo consta a;
    - ISO/IEC 27001:2013
- Princípios e linhas de orientação: fornecem orientações gerais aplicadas ao longo da vida de uma organização, respeitando as suas especificidades, numa harmonização com normas existentes e futuras;
    - ISO 31000:2018
    - ISO/IEC 27005:2018

Encontrando-se a ISO/IEC 27005:2011 referencialmente alinhada com a ISO 31000:2018, é possível obter as seguintes conclusões:

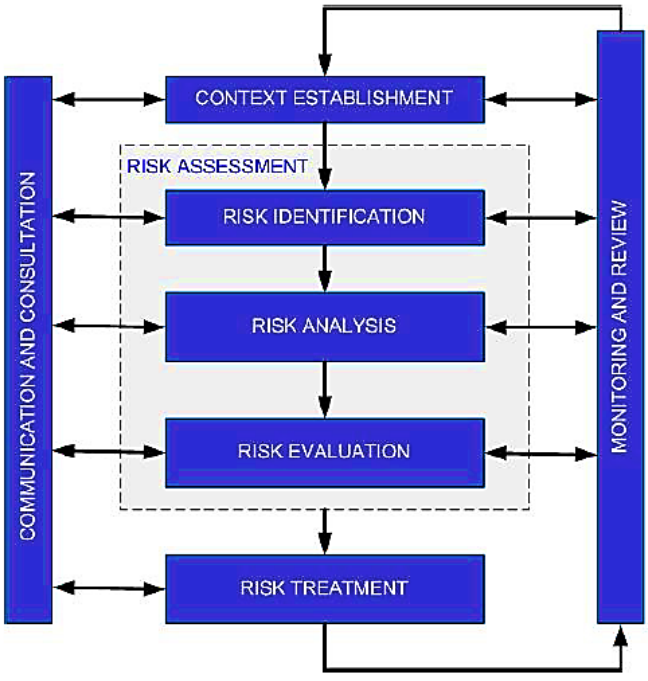
- **Risco** surge definido na clausula 3.9, como o "*efeito da incerteza nos objetivos*". Adicionalmente, importa realçar a Nota 6 apresentada na Norma, na qual acresce à definição a clarificação de que "*o risco de segurança da informação está associado ao potencial de que as ameaças irão explorar vulnerabilidades de um ativo de informação ou de um grupo de ativos de informação e, assim, causar danos a uma organização*".

  Ora, assumindo esta definição uma posição de arquétipo, porquanto define um dos principais termos da norma, independentemente do contexto em que se invoca, conclui-se a sua limitação e inadequabilidade aquando de

privacidade e/ou dados pessoais se tratar, porquanto nos termos da lei, o risco deve visar pessoas singulares e não as organizações (pessoas coletivas).

Não significa isto que, na perspetiva de gestão de risco de uma organização, sejam ignorados os demais riscos a que esta se encontra exposta, todavia importa não confundir com os riscos para as pessoas singulares (clientes, colaboradores, prestadores de serviços, etc.), que decorrente da atividade da organização, possam vir a ser afetadas, nomeadamente ao nível dos seus direitos fundamentais;

- **Avaliação de risco** resulta claro na cláusula 3.11, enquanto "*processo global de identificação de risco (3.15), análise de risco (3.10) e avaliação de riscos (3.14)*", proporcionando uma representação do seguinte processo:



[31]

Figura 9 - Processo de gestão de risco conforme a ISO31000

Aprofundando as orientações previstas na norma, conclui-se que o processo representado na figura 9, decompõe-se nas seguintes atividades;

Macro atividade	Referencia normativa	Atividade	Descrição
Risk Identification	ISO/IEC 27005, clausula 8.2.2	Identificação dos Ativos	Definindo "ativo", como algo que constitua valor, deverão ser identificados e tipificados todos os ativos relevantes.

Risk Identification	ISO/IEC 27005, clausula 8.2.3	Identificação de Ameaças	Potencial causa que possa provocar incidente, o qual resulte em dano ou perda (conforme previsto na ISO/IEC 27000:2018, clausula 3.74), deve ser devidamente identificado.
Risk Identification	ISO/IEC 27005, clausula 8.2.4	Identificação de Controlos existentes	De modo a compreender a eficiência e/ou eficácia dos controlos existentes, estes deverão ser identificados e analisados adequadamente.
Risk Identification	ISO/IEC 27005, clausula 8.2.5	Identificação de Vulnerabilidades	Toda a fraqueza verificada em ativo(s) ou controlo(s), que possam ser exploradas por uma ou mais ameaças (nos termos da ISO/IEC 27000:2018, clausula 3.77), devem ser devidamente identificadas.
Risk Identification	ISO/IEC 27005, clausula 8.2.6	Identificação de Consequências	Qualquer resultado de um ou mais eventos que afetem os objetivos (conforme previsto na ISO/IEC 27000:2018, clausula 3.12), deverá ser devidamente identificada.
Risk Analysis	ISO/IEC 27005, clausula 8.3.2	Avaliação de Consequências	Atendendo aos potenciais cenários de incidente, incluindo as ameaças identificadas, vulnerabilidades e respetivos efeitos, será possível avaliar a consequência prevista.
Risk Analysis	ISO/IEC 27005, clausula 8.3.3	Avaliação da Probabilidade de ocorrência	A avaliação da probabilidade de ocorrência deverá ser realizada por intermédio de técnicas de análise qualitativa ou quantitativa, tendo em conta a facilidade de materialização.
Risk Analysis	ISO/IEC 27005, clausula 8.3.4	Determinação do nível de risco	A determinação do nível de risco é obtida pela consequência e sua probabilidade de ocorrência/materialização.
Risk Evaluation	ISO/IEC 27005, clausula 8.4	Avaliação do Risco	O nível de risco deverá ser comparado com os critérios de avaliação de risco e níveis de aceitação.

Tabela 1 – Decomposição do Processo previsto na ISO/IEC 27005

As normas ISO, são também referencia no mercado, tendo vindo a procurar contribuir com soluções para a gestão da privacidade, através da recente publicação da ISO/IEC 27701:2019. No entanto, a família ISO/IEC 27xxx, sendo específica para a Segurança da Informação, não está estruturalmente ajustada aos requisitos de proteção de dados pessoais, nomeadamente;

- O vocabulário é inaplicável; ao analisar a ISO/IEC 27000:2018 na Cláusula 3.61, a definição do termo "Risco", apresenta como nota adicional 6 "*O risco de segurança em formação está associado ao potencial de que as ameaças irão explorar vulnerabilidades de um ativo de informação ou de um grupo de ativos de informação e, assim, causar* ***danos a uma organização****.*".

  Ora, atendendo que o foco das obrigações legais e regulatórias de proteção de dados pessoais é centrada nas pessoas singulares, nomeadamente nos seus direitos e liberdades fundamentais, compromete desde logo a sua aplicabilidade;
- O âmbito é limitado; analisando a Cláusula 3.74 da ISO/IEC27000:2018, na definição do termo "*Ameaça*", é dada a definição de "*causa potencial de um incidente indesejado, que pode resultar em* ***danos a um sistema ou organização*** *(3.50)*".

  Para além da dimensão taxonómica, as referências à "*avaliação de risco*" na recente ISO/IEC27701:2019, remete para a ISO/IEC27001:2013, sendo, por isso, limitadas no seu âmbito (de acordo com as suas cláusulas 5.4.1.2 e 5.6.2).

Verifica-se que, conceptualmente as referidas normas ISO não abrangem as dimensões legalmente prescritas em relação a:

- **Danos materiais/tangíveis, físicos ou económicos**: danos pessoais; perda de liberdade ou liberdade de circulação; limitação da compra e/ou perda financeira; outros prejuízos económicos, por exemplo, por furto de identidade;
- **Danos incorpóreos/não materiais**: danos resultantes da monitorização ou exposição de identidade/características/atividades/opiniões; condicionando a liberdade de expressão; danos à reputação; medo pessoal, familiar, de

trabalho ou social, constrangimento ou ansiedade; intrusão inaceitável na vida privada; discriminação ou estigmatização; perda de autonomia; restrição inadequada da escolha pessoal; roubo de identidade; limitação do controlo sobre os seus dados pessoais.

Orientação de acordo com a NIST SP800-30/39

- **Risco** surge definido como "*Uma medida das extensões a que uma entidade é ameaçada por uma circunstância ou evento potencial, e tipicamente uma função: (i) dos impactos adversos que surgiriam se a circunstância ou acontecimento ocorresse; e (ii) da probabilidade de ocorrência*";
- **Avaliação de Risco** é descrito como o *processo de identificação, estimativa e priorização de riscos para operações organizacionais (incluindo missão, funções, imagem, reputação), bens organizacionais, indivíduos, outras organizações, e a Nação, resultantes do funcionamento de um sistema de informação*.

  Parte da gestão de riscos, incorpora a análises de ameaças e de vulnerabilidades, e considera as atenuações fornecidas pelos controlos de segurança planeados ou em vigor.

  Ora, apesar de se verificar uma definição centrada nas entidades coletivas, a referência a indivíduos (pessoas singulares), corporiza uma adequação em aplicações específicas na privacidade e proteção de dados pessoais.

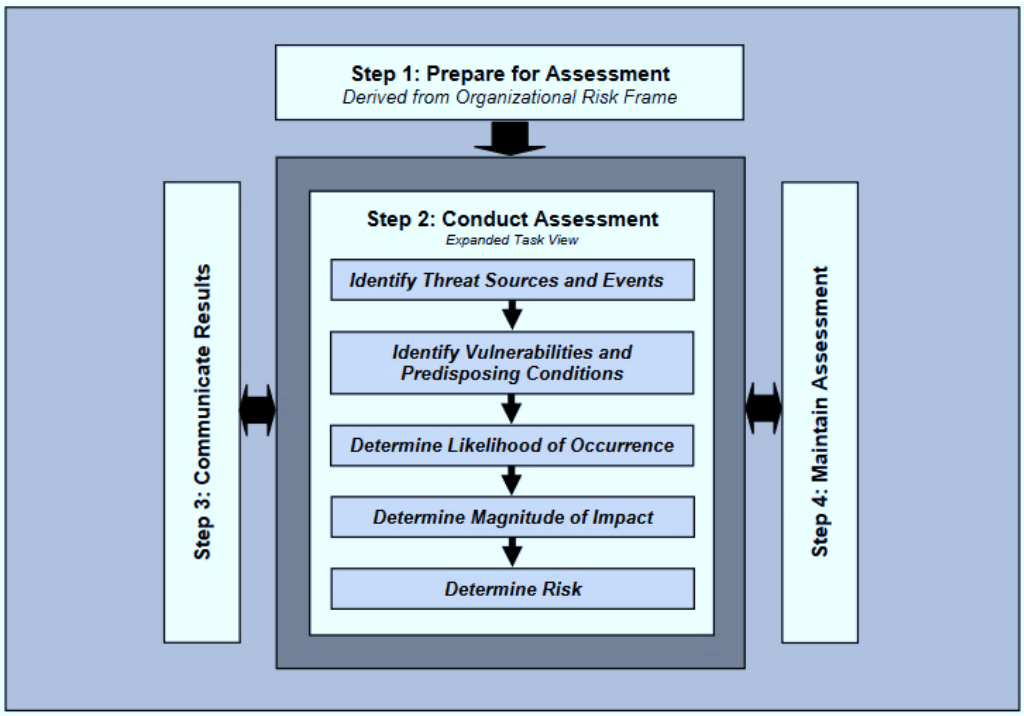


Figura 10 - Processo de Risk Assessment de acordo com a NIST SP800-30

Conforme se pode verificar na figura 14, existe uma relativa similaridade com o processo descrito na figura 13 relativo à ISO/IEC 27005, quanto às atividades, evidenciando assim a existência do um âmbito comum a atingir.

Orientação de acordo com o M_o_R (Management of Risk)

- **Risco** entendido como "*um evento incerto ou conjunto de eventos que, caso ocorram, terão um efeito na realização de objetivos*".
  Adicionalmente, refere-se de que é "*medido pela combinação da probabilidade de uma ameaça ou oportunidade percebida e pela magnitude do seu impacto nos objetivos*" [32].
- **Avaliação de Risco** resulta como parte da definição de gestão de risco, na qual se considera relevante a "*aplicação sistemática de princípios, numa abordagem e processo para as tarefas de; identificar e avaliar os riscos*".

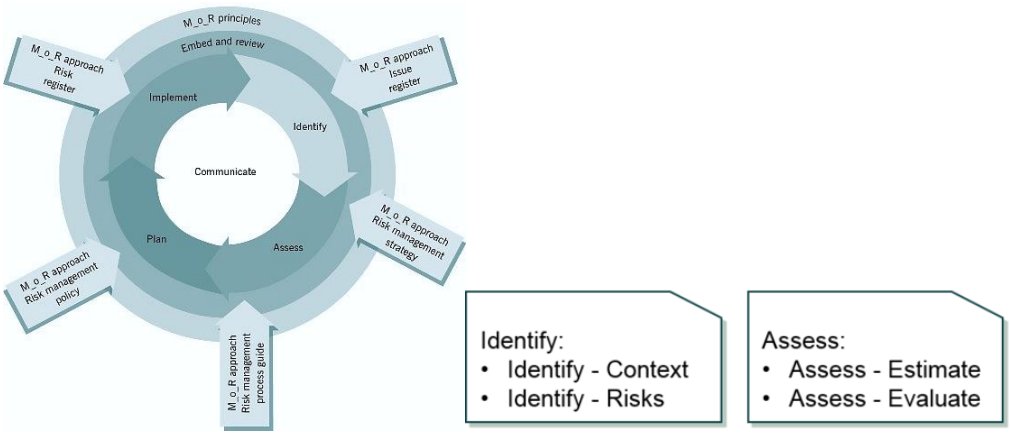


Figura 11 – Processo segundo o M_o_R da AXELOS

Das atividades relevantes do processo, nomeadamente "*identificar*" e "*avaliar*", cada uma destas irá dissecar no dobro, resultando assim em quatro diferentes atividades a considerar no processo. Deste modo, obter-se-á a seguinte tabela;

Fase	Atividade	Ações
Identificar	Contexto	▪ Estabelecer objetivos/âmbito ▪ Analisar pressupostos ▪ Validar completude da informação ▪ Análise das partes interessadas ▪ Avaliar documentação relevante
	Riscos	▪ Identificar ameaças e oportunidades
Avaliar	Estimativa	▪ Avaliar clareza da descrição dos riscos ▪ Avaliar probabilidade, impacto, proximidade e valor esperado do risco
	Avaliação	▪ Avaliar exposição ao risco ▪ Avaliar necessidade de modelo de risco

Tabela 2 - Decomposição do Risk Assessment segundo M_o_R

Orientação de acordo com a ENISA

- A Agência Europeia ENISA publicou e colaborou, na produção em conjunto com peritos das autoridades de controlo da Grécia e da Alemanha, na elaboração de uma metodologia de avaliação[33], na qual apresenta uma

abordagem de avaliação de risco de privacidade que, apensar de estar orientada às violações de dados pessoais, serve de orientador na forma como o risco é calculado.

Este trabalho também contou com a participação do Grupo de Trabalho do Artigo 29 (WP29), nos quais estão representadas as diferentes autoridades de controlo dos estados-membros da EU, os quais por princípio, espera-se que subscrevam a orientação que ajudaram a construir.

- A avaliação considera os seguintes critérios para avaliação:
    - **Contexto do tratamento de dados (DPC - *data processing context*)**; procurando identificar os tipos de dados afetados, adicionando informações relacionadas com o contexto no qual o tratamento dos dados pessoais ocorreu;
    - **Facilidade de identificação (EI - *ease of identification*);** procura determinar a facilidade de identificação das pessoas singulares, por via dos dados envolvidos na violação;
    - **Circunstâncias da violação (CB – *circunstances of breach*);** procura determinar especificidades das circunstâncias da violação, especialmente ao nível da segurança dos dados afetados, assim como as motivações envolvidas.

Quanto ao cálculo da severidade, a ENISA propõe a seguinte fórmula:

$$\boldsymbol{Severidade = DPC * EI + CB}$$

Com base no resultado obtido, conclui-se o nível de risco, o qual deve ser analisado com base na seguinte tabela:

Matriz de análise da severidade de uma violação de dados pessoais		
Critério	Nível de risco	Descrição
SE < 2	Baixo	Prevê-se que os titulares de dados não sejam afetados ou que ocorra uma marginal inconveniência que será ultrapassada facilmente (tempo dispensado, constrangimentos, irritação, etc.).

2 ≤ SE < 3	Médio	Os titulares de dados, podem encontrar inconvenientes significativos, podendo ultrapassar os mesmos, apesar de algumas dificuldades (custos, limitação de serviços, medo, stress, indisposição, etc.).
3 ≤ SE < 4	Alto	Os titulares de dados, podem encontrar consequências significativas, que podendo ultrapassar, provocará sérias dificuldades (custos, discriminação, perda material, perda de emprego, intimidação, agravamento da saúde, etc.).
4 ≤ SE	Muito alto	Espera-se que os titulares de dados, encontrem consequências significativas, possivelmente irreversíveis, que não poderão ultrapassar (dificuldades financeiras, dividas ou incapacidade de trabalhar, doença psicológica ou física a longo prazo, morte, etc.).

Tabela 3 - Matriz de severidade da ENISA

2.3 RGPD

A famosa definição de privacidade de Warren e Brandeis, já referida no presente estudo, como "*right to be let alone*" e descrita como o direito mais valorizado pelo Homem civilizado, retrata proficuamente a importância da privacidade no conceito de Liberdade.

Como resulta evidente deste estudo, a proteção de dados pessoais é fundamental, no cumprimento dos direitos, liberdades e garantias, previstos na Constituição da República Portuguesa.

Não obstante do referido na Constituição da República Portuguesa, surge publicada em 1991 a Lei n.º 10/91 de 29 de abril, como legislação específica sobre Proteção de Dados Pessoais no contexto do uso da informática, que introduz importantes conceitos e definições de Proteção de Dados Pessoais no ordenamento jurídico, como o caso da definição de “dados pessoais” na sua alínea a) artigo 2.º.

Todavia, surge em 1994 a Lei 28/94, de 29 de agosto, como Lei de alteração de vários artigos da anterior Lei, que procura proporcionar uma melhoria ao previsto em 1991.

Importa referir que a Lei de 1991, não fazendo referência ao termo "risco", surge na Lei de 1994 a sua única referência no n.2 do artigo 17.º aquando apresenta limites e exceção no tratamento de dados pessoais, desde que "*esse tratamento não possa implicar risco de intromissão na vida privada ou de discriminação*".

A Directiva n.º 95/46/CE, do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados, resulta transposta para a ordem jurídica Portuguesa em 1998, sob a forma da Lei 67/98 de 26 de outubro.

Após 20 anos da vigência da Lei 67/98 de 26 de Outubro, com a aplicação do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho de 27 de abril de 2016 (RGPD), a partir de 25 de maio de 2018 vem revogar no seu artigo 94.º a Diretiva 95/46/CE, todavia, a Lei que transpôs a Diretiva mantém-se simultaneamente vigente, até à publicação da Lei n.º 58/2019 de 8 de agosto, com o seu n.1 do artigo 66.º, enquanto lei de execução na ordem jurídica nacional.

Ora com isto, verifica-se que entre 25 de maio de 2018 e 8 de agosto de 2019, coabitaram vigentes na ordem jurídica Portuguesa, obrigações legais contraditórias, como o caso de obrigação de notificação à CNPD previsto no artigo 27.º da Lei 67/98, versus o principio de responsabilização do Responsável pelo Tratamento e seus mecanismos de Avaliação de impacto sobre a proteção de dados (DPIA) previsto no artigo 35.º do RGPD.

Uma vez que, a licitude do tratamento previsto na lei de proteção de dados pessoais, pode ser fundamentada no cumprimento de obrigações legais, torna-se perentório conhecer as obrigações sectoriais, uma vez que o cumprimento de obrigações, pode intrinsecamente legitimar o tratamento de dados pessoais, atendendo às obrigações previstas legalmente nos diversos sectores económicos (saúde, imobiliário, telecomunicações, banca, seguros, etc.).

Risco na conformidade com o RGPD

A gestão de risco é essencial no cumprimento das obrigações de proteção de dados pessoais, a fim de que se satisfaçam os critérios exigidos nas obrigações legais e regulamentares vigentes.

Existe, uma relação intrínseca entre a gestão de risco e as ferramentas de suporte ao tratamento de dados pessoais. Nos tempos modernos, esta relação torna-se ainda mais relevante, quando analisamos a importância que a gestão de risco tem na proteção eficaz da privacidade, num mundo em constante desenvolvimento e evolução tecnológica, especialmente desafiada por novas tendências, como "big-data", Internet das Coisas ("IoT"), videovigilância, especialmente potenciadas pelo aumento da capacidade de processamento e redução do custo de armazenamento, entre outros benefícios importantes que, naturalmente, são promotores de riscos para a privacidade.

A fim de se identificar a importância do risco na privacidade e dados pessoais, realizou-se primeiramente o ensaio de identificação das referências existentes nos considerandos do RGPD, tendo-se obtido a seguinte tabela de resultados:

Referencia RGPD	**Citação observada**
Considerando 9	*(…) sentimento generalizado da opinião pública de que subsistem **riscos** significativos para a proteção das pessoas singulares.*
Considerando 15	*A fim de se evitar (…) **risco** sério de ser contornada a proteção das pessoas singulares, esta deverá ser neutra em termos tecnológicos e deverá ser independente das técnicas utilizadas.*
Considerando 28	*A aplicação da pseudonimização aos dados pessoais pode reduzir os **riscos** para os titulares de dados.*
Considerando 35	*Deverão ser considerados dados pessoais relativos à saúde (…) quaisquer informações sobre, por exemplo, uma doença, deficiência, um **risco** de doença (…)*
Considerando 38	*As crianças merecem proteção especial quanto aos seus dados pessoais, uma vez que podem estar menos cientes dos **riscos**, consequências e garantias em questão e dos seus direitos.*

Considerando 39	*As pessoas singulares a quem os dados dizem respeito deverão ser alertadas para os **riscos**, regras, garantias e direitos associados ao tratamento dos dados pessoais e para os meios de que dispõem para exercer os seus direitos relativamente a esse tratamento.*
Considerando 51	*Merecem proteção específica os dados pessoais que sejam, pela sua natureza, especialmente sensíveis do ponto de vista dos direitos e liberdades fundamentais, dado que o contexto do tratamento desses dados poderá implicar **riscos** significativos para os direitos e liberdades fundamentais.*
Considerando 65	*Esse direito assume particular importância quando o titular dos dados tiver dado o seu consentimento quando era criança e não estava totalmente ciente dos **riscos** inerentes ao tratamento, e mais tarde deseje suprimir esses dados pessoais, especialmente na Internet.*
Considerando 71	*(…) **risco** de erros é minimizado, e proteger os dados pessoais de modo a que sejam tidos em conta os potenciais **riscos** para os interesses e direitos do titular dos dados e de forma a prevenir, por exemplo, efeitos discriminatórios contra pessoas singulares em razão da sua origem racial ou étnica, opinião política, religião ou convicções, filiação sindical, estado genético ou de saúde ou orientação sexual, ou a impedir que as medidas venham a ter tais efeitos.*
Considerando 74	*Essas medidas deverão ter em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como o **risco** que possa implicar para os direitos e liberdades das pessoas singulares.*
Considerando 75	*O **risco** para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis.*
Considerando 76	*A probabilidade e a gravidade dos **riscos** para os direitos e liberdades do titular dos dados deverá ser determinada por referência à natureza, âmbito, contexto e finalidades do tratamento de dados. Os **riscos** deverão ser aferidos com base numa avaliação objetiva, que determine se as operações de tratamento de dados implicam **risco** ou **risco** elevado.*

Considerando 77	*(…) identificação dos **riscos** relacionados com o tratamento, à sua avaliação em termos de origem, natureza, probabilidade e gravidade, bem como à identificação das melhores práticas para a atenuação dos **riscos**.*
Considerando 80	*(…) **riscos** para os direitos e liberdades das pessoas singulares, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento (…).*
Considerando 81	*(…) **risco** em relação aos direitos e liberdades do titular dos dados.*
Considerando 83	*(…) avaliar os **riscos** que o tratamento implica e aplicar medidas que os atenuem, como a cifragem. Essas medidas deverão assegurar um nível de segurança adequado, nomeadamente a confidencialidade, tendo em conta as técnicas mais avançadas e os custos da sua aplicação em função dos **riscos** e da natureza dos dados pessoais a proteger. Ao avaliar os **riscos** para a segurança dos dados, deverão ser tidos em conta os **riscos** apresentados pelo tratamento dos dados pessoais, tais como a destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou o acesso não autorizados a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento, **riscos** esses que podem dar azo, em particular, a danos físicos, materiais ou imateriais.*
Considerando 84	*(…) as operações de tratamento de dados sejam suscetíveis de resultar num elevado **risco** para os direitos e liberdades das pessoas singulares, (…) avaliação de impacto da proteção de dados para determinação, nomeadamente, da origem, natureza, particularidade e gravidade desse **risco**.* *(…) tratamento apresenta um elevado **risco** que o responsável pelo tratamento não poderá atenuar através de medidas adequadas, atendendo à tecnologia disponível e aos custos de aplicação (…).*
Considerando 85	*(…) essa violação não é suscetível de implicar um **risco** para os direitos e liberdades das pessoas singulares (…).*
Considerando 86	*(…) resulte um elevado **risco** para os direitos e liberdades da pessoa singular, a fim de lhe permitir tomar as precauções necessárias.*

Considerando 89	*(…) operações de tratamento suscetíveis de resultar num elevado **risco** para os direitos e liberdades das pessoas singulares, devido à sua natureza, âmbito, contexto e finalidades.*
Considerando 90	*(…) avaliar a probabilidade ou gravidade particulares do elevado **risco**, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento e as fontes do **risco**. Essa avaliação do impacto deverá incluir, nomeadamente, as medidas, garantias e procedimentos previstos para atenuar esse **risco**, assegurar a proteção dos dados pessoais e comprovar a observância do presente regulamento.*
Considerando 91	*(…) afetar um número considerável de titulares de dados e sejam suscetíveis de implicar um elevado **risco**, por exemplo, em razão da sua sensibilidade, nas quais, em conformidade com o nível de conhecimentos tecnológicos alcançado, seja utilizada em grande escala uma nova tecnologia, bem como a outras operações de tratamento que impliquem um elevado **risco** para os direitos e liberdades dos titulares dos dados, em especial quando tais operações dificultem aos titulares o exercício dos seus direitos. (…) controlo de zonas acessíveis ao público em grande escala, nomeadamente se forem utilizados mecanismos optoeletrónicos, ou para quaisquer outras operações quando a autoridade de controlo competente considere que o tratamento é suscetível de implicar um elevado **risco** para os direitos e liberdades dos titulares dos direitos, em especial por impedirem estes últimos de exercer um direito ou de utilizar um serviço ou um contrato, ou por serem realizadas sistematicamente em grande escala.*
Considerando 94	*(…) falta de garantias e de medidas e procedimentos de segurança para atenuar os **riscos**, implica um elevado **risco** para os direitos e liberdades das pessoas singulares e o responsável pelo tratamento considerar que o **risco** não poderá ser atenuado através de medidas razoáveis, atendendo à tecnologia disponível e aos custos de aplicação, a autoridade de controlo deverá ser consultada antes de as atividades de tratamento terem início. Provavelmente, esse elevado **risco** decorre de determinados tipos de tratamento e da*

	extensão e frequência do tratamento, que podem originar igualmente danos ou interferir com os direitos e liberdades da pessoa singular.
Considerando 96	*(…) atenuar o respetivo **risco** para o titular dos dados.*
Considerando 98	*(…) tendo em conta o **risco** que poderá resultar do tratamento dos dados no que diz respeito aos direitos e às liberdades das pessoas singulares.*
Considerando 116	*Sempre que dados pessoais atravessarem fronteiras fora do território da União, aumenta o **risco** de que as pessoas singulares não possam exercer os seus direitos à proteção de dados, nomeadamente para se protegerem da utilização ilegal ou da divulgação dessas informações (…).*
Considerando 122	*(…) realização de investigações sobre a aplicação do presente regulamento e a promoção da sensibilização do público para os **riscos**, regras, garantias e direitos associados ao tratamento de dados pessoais.*

Tabela 4 - Citações ao risco em considerandos

De seguida, procedeu-se ao ensaio de identificação das referências existentes a risco, nos artigos do RGPD, tendo sido possível obter a seguinte tabela de resultados:

Referencia RGPD	**Citação observada**
Artigo 4.º, n.º 24)	*(…) demonstrando claramente a gravidade dos **riscos** que advêm do projeto de decisão para os direitos e liberdades fundamentais dos titulares dos dados e, eventualmente, para a livre circulação de dados pessoais no território da União;*
Artigo 23.º, n.º 2 alínea g)	*(…) Aos **riscos** específicos para os direitos e liberdades dos titulares dos dados;*
Artigo 24.º, n.º 1	*Tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento dos dados, bem como os **riscos** para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, o responsável pelo tratamento aplica as medidas técnicas e organizativas que forem adequadas (…).*
Artigo 25.º, n.º 1	*Tendo em conta as técnicas mais avançadas, os custos da sua aplicação, e a natureza, o âmbito, o contexto e as finalidades do*

	*tratamento dos dados, bem como os **riscos** decorrentes do tratamento para os direitos e liberdades das pessoas singulares, cuja probabilidade e gravidade podem ser variáveis, (…)*
Artigo 27.º, n.º 2 alínea a)	*(…) suscetível de implicar **riscos** para os direitos e liberdades das pessoas singulares, tendo em conta a natureza, o contexto, o âmbito e as finalidades do tratamento;*
Artigo 30.º, n.º 5	*(…) o tratamento efetuado seja suscetível de implicar um **risco** para os direitos e liberdades do titular dos dados, não seja ocasional ou abranja as categorias especiais de dados a que se refere o artigo 9.º, n.º 1, ou dados pessoais relativos a condenações penais e infrações referido no artigo 10.º.*
Artigo 32.º	*1. Tendo em conta as técnicas mais avançadas, os custos de aplicação e a natureza, o âmbito, o contexto e as finalidades do tratamento, bem como os **riscos**, de probabilidade e gravidade variável, para os direitos e liberdades das pessoas singulares, o responsável pelo tratamento e o subcontratante aplicam as medidas técnicas e organizativas adequadas para assegurar um nível de segurança adequado ao **risco**, incluindo, consoante o que for adequado:* *(…)* *2. Ao avaliar o nível de segurança adequado, devem ser tidos em conta, designadamente, os **riscos** apresentados pelo tratamento, em particular devido à destruição, perda e alteração acidentais ou ilícitas, e à divulgação ou ao acesso não autorizados, de dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento.*
Artigo 33.º, n.º 1	*(…) a menos que a violação dos dados pessoais não seja suscetível de resultar num **risco** para os direitos e liberdades das pessoas singulares.*
Artigo 34.º, n.º 1	*(…) violação dos dados pessoais for suscetível de implicar um elevado **risco** para os direitos e liberdades das pessoas singulares.* *(…) tomado medidas subsequentes que assegurem que o elevado **risco** para os direitos e liberdades dos titulares dos dados.*

Artigo 35.º	*Quando um certo tipo de tratamento, em particular que utilize novas tecnologias e tendo em conta a sua natureza, âmbito, contexto e finalidades, for suscetível de implicar um elevado* ***risco*** *para os direitos e liberdades das pessoas singulares. (…) Se um conjunto de operações de tratamento que apresentar* ***riscos*** *elevados semelhantes, pode ser analisado numa única avaliação. (…) Uma avaliação dos* ***riscos*** *para os direitos e liberdades dos titulares dos direitos. (…) As medidas previstas para fazer face aos* ***riscos****, incluindo as garantias, medidas de segurança e procedimentos destinados a assegurar a proteção dos dados pessoais e a demonstrar a conformidade com o presente regulamento, tendo em conta os direitos e os legítimos interesses dos titulares dos dados e de outras pessoas em causa.*
Artigo 36.º	*(…) nos termos do artigo 35.º indicar que o tratamento resultaria num elevado* ***risco*** *na ausência das medidas tomadas pelo responsável pelo tratamento para atenuar o* ***risco****. (…) se o responsável pelo tratamento não tiver identificado ou atenuado suficientemente os* ***riscos*** *(…)*
Artigo 39.º, n.º 2	*(…) devida consideração os* ***riscos*** *associados às operações de tratamento, tendo em conta a natureza, o âmbito, o contexto e as finalidades do tratamento.*
Artigo 57.º, n.º 1 alínea b)	*Promove a sensibilização e a compreensão do público relativamente aos* ***riscos****, às regras, às garantias e aos direitos associados ao tratamento. As atividades especificamente dirigidas às crianças devem ser alvo de uma atenção especial;*
Artigo 70.º, n.º 1 alínea h)	*(…) circunstâncias em que as violações de dados pessoais são suscetíveis de resultar num* ***risco*** *elevado para os direitos e liberdades das pessoas singulares a que se refere o artigo 34.º, n.º 1;*

Tabela 5 - Citação ao risco em artigos

Após esta análise, verifica-se a referência ao risco na conformidade com o RGPD, em 27 considerandos e 14 artigos, resultando como indubitável, a sua elevada importância.

A proteção dos dados pessoais, não pode ser alcançada sem a correta aplicação da gestão de risco, num processo sistemático de cumprimento dos requisitos legais e regulamentares, garantindo que os dados pessoais são tratados corretamente e que os direitos e liberdades das pessoas singulares, são protegidos.

Conforme previsto no MoR, conforme referido no capítulo 2.2 acima, espera-se que a gestão de risco assente numa análise sistemática e objetiva, não só sobre a ameaça, mas também sobre os benefícios, permitindo que sejam avaliados e compreendidos no início do processo/tratamento, uma vez que, sem compreender os benefícios, será impossível determinar o nível adequado de equilíbrio entre os benefícios e as ameaças do tratamento.

Mesmo que não seja tão comumente referido, os benefícios no tratamento são vários, tais como a capacidade de obter um bem ou serviço desejado, ser protegido contra fraudes, usufruir de serviços médicos mais eficientes ou convenientes ou prevenção de doenças, etc.

Os benefícios devem ser considerados como parte da avaliação dos riscos, conjuntamente com a avaliação de ameaças.

O objetivo da gestão de risco na proteção de dados pessoais, será de avaliar as ameaças e oportunidades, com especial foco nas atividades que representam maior risco para a privacidade, identificando que medidas melhor podem ser implementadas para reduzir a ameaça e aumentar a oportunidade, numa abordagem prática e prudente, sendo explícito sobre os riscos residuais e como estes deverão ser doravante geridos.

Fatores determinantes do nível de risco na privacidade

A **natureza** dos dados pessoais, assume-se como fator determinante do nível de risco, havendo uma relação direta entre o tipo de dados e o nível de risco associado. Isto deve-se à relação de quanto mais "privado" for o dado, maior a motivação (probabilidade) do seu uso, numa ação de relevante impacto nos seus direitos e liberdades.

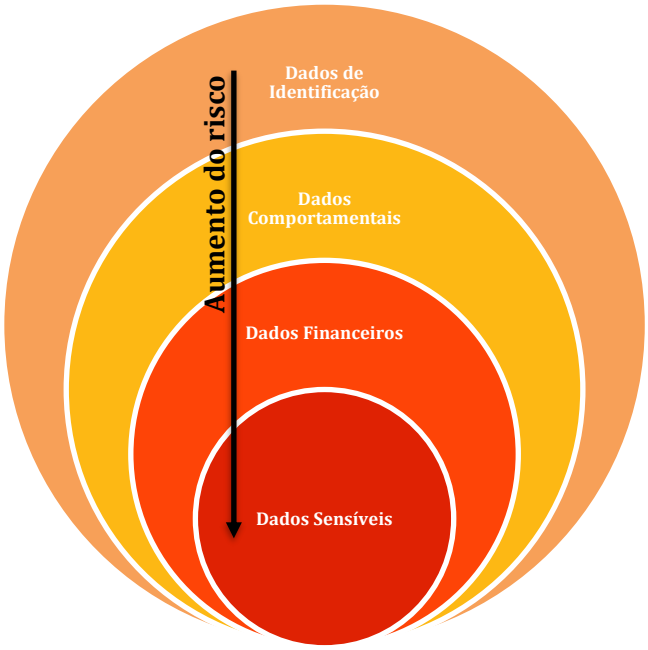


Figura 12 - Escala representativa do risco nos dados pessoais

Tudo o que possa ser indiciado direta ou indiretamente pela natureza dos dados pessoais, contribui de modo muito relevante para o cálculo do risco na privacidade.

O **contexto** são as diferenças de circunstância, conjuntura e enquadramento em que o tratamento de dados pessoais ocorre, sendo este considerado também como fator relevante do nível de risco.

A determinação do contexto pode ser variada, estando este normalmente associado à relação entre os participantes/envolvidos no tratamento (i.e., contexto laboral), no qual depende que sejam;

- Estabelecidos os objetivos pretendido com o tratamento;
- Analisados todos os pressupostos relevantes a ter em conta;
- Validada a completude e qualidade dos dados pessoais;
- Analisados os intervenientes envolvidos;
- Avaliada toda a documentação relevante;

A **finalidade** está associada ao motivo jurídico que justifica o tratamento, é condição fundamental para o tratamento de dados pessoais (i.e., fins estatísticos ou investigação científica). Estas devem ser específicas e limitadas, devendo apenas serem tratados os dados para os fins que inicialmente foram definidos.

O tratamento deverá respeitar que os dados pessoais estejam minimizados, ou seja, devem ser restringidos unicamente aos dados estritamente necessários para o cumprimento da(s) finalidade(s) pretendidas.

O **dano** é a determinação do nível de risco na privacidade e depende de vários fatores, especialmente do potencial dano causado ao(s) titular(s) de dados, de modo que se torna impreterível decompor os diferentes danos a que as pessoas singulares poderão ser alvo.

De acordo com o exposto nos considerandos 75 e 83 do RGPD, é possível sistematizar as dimensões que se seguem e criar deste modo uma compreensível correlação entre o tipo de risco, a dimensão e alguns exemplos do seu efeito.

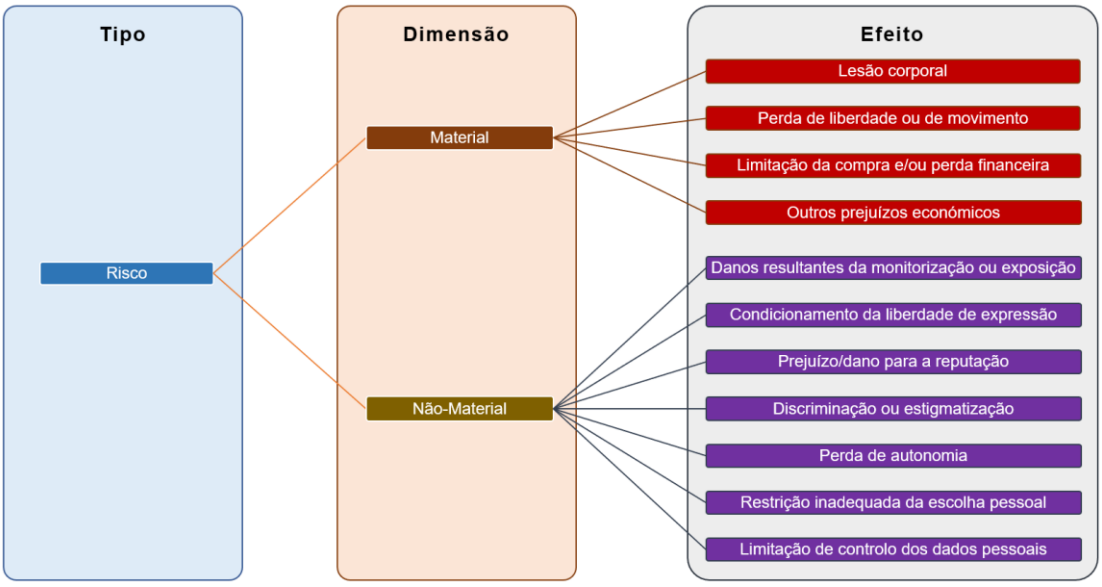


Figura 13 - Trinómio relacional do risco de privacidade

Importa realçar que os referidos efeitos na figura 13 são representativos de eventos relacionados com direitos, liberdades e garantias fundamentais, as quais poderão nos termos da Constituição da República Portuguesa (CRP), ser decompostos de acordo com a seguinte representação gráfica, com referência aos respetivos artigos:

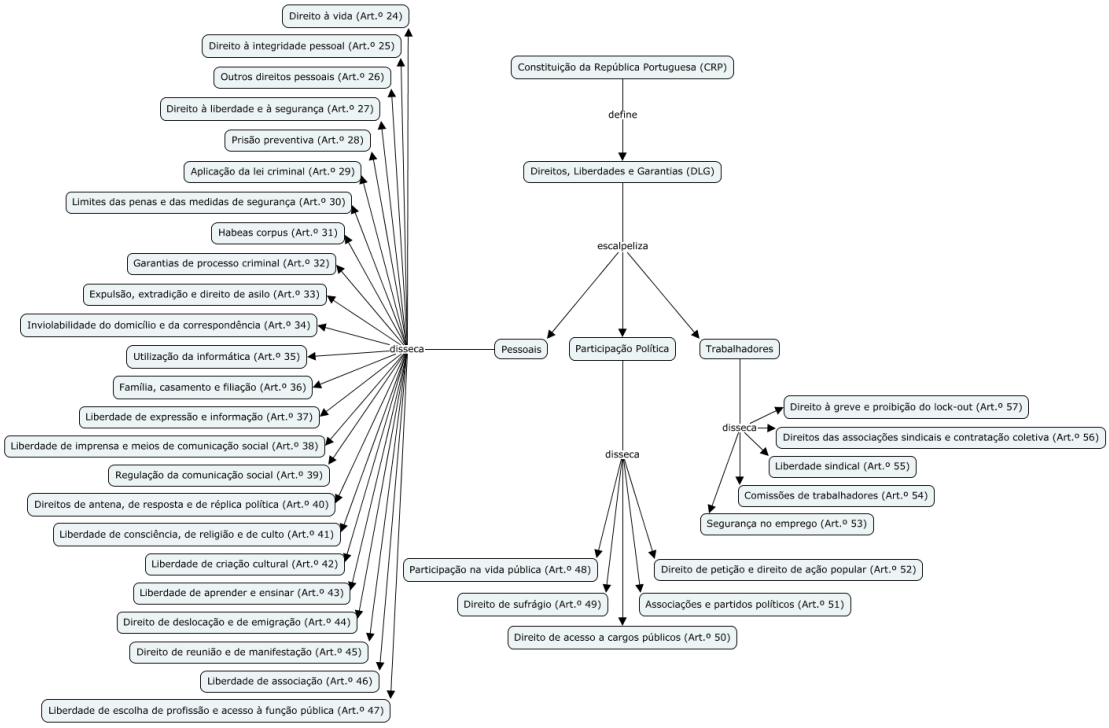


Figura 14 - Arvore relacional dos Direitos, Liberdades e Garantias

Conforme resulta claro de acordo com a figura 17, os Direitos, Liberdades e Garantias (DLG) previstos na Constituição da República Portuguesa, estão organizados por três diferentes tipos; pessoais, participação política e trabalhadores, os quais se expandem nos diferentes tipos, conforme representado na figura.

Importa igualmente realçar que, não obstante das referencias normativas existentes em matéria de segurança de informação e proteção de dados pessoais, o próprio RGPD no seu artigo 32.º, n.º 1, alínea b), preveem a importância da "confidencialidade, Integridade e disponibilidade", as quais se consideram relevantes e a ter em conta na determinação do risco, conforme se diversos considerandos e artigos, podendo deste modo ser produzida a seguinte relação:

Propriedade	Causa/efeito potencial associado
Confidencialidade	Acesso ilegítimo a dados pessoais
	Comprometimento no tratamento de dados pessoais
Integridade	Alterações inesperadas no decorrer do tratamento
	Alteração não pretendida nos dados pessoais
Disponibilidade	Indisponibilidade de processos
	Desaparecimento de dados pessoais
	Inacessibilidade ao tratamento de dados pessoais

Tabela 6 - Relação da segurança dos dados e respetiva causa/efeito

Consequências para o(s) titular(es) de dados e calculo indemnizatório

Sem prejuízo dos demais efeitos que um evento de proteção de dados pessoais pode provocar numa organização, independentemente da sua natureza jurídica (fins lucrativos ou não), quer ao nível da reputação, financeiro/solvência, entre outras dimensões, o foco da proteção de dados pessoais deve estar sempre primeiramente no titular de dados, especialmente na forma como os seus Direitos, Liberdades e Garantias (DLG) podem ser afetados/condicionados, os quais têm a seguinte distribuição, nos termos da Constituição da República Portuguesa (CRP):

- **Direitos, Liberdades e Garantias Pessoais**
  - Direito à vida (Art.º 24)
  - Direito à integridade pessoal (Art.º 25)
  - Outros direitos pessoais (Art.º 26)
  - Direito à liberdade e à segurança (Art.º 27)
  - Prisão preventiva (Art.º 28)
  - Aplicação da lei criminal (Art.º 29)
  - Limites das penas e das medidas de segurança (Art.º 30)
  - Habeas corpus (Art.º 31)
  - Garantias de processo criminal (Art.º 32)
  - Expulsão, extradição e direito de asilo (Art.º 33)
  - Inviolabilidade do domicílio e da correspondência (Art.º 34)
  - Utilização da informática (Art.º 35)
  - Família, casamento e filiação (Art.º 36)
  - Liberdade de expressão e informação (Art.º 37)
  - Liberdade de imprensa e meios de comunicação social (Art.º 38)
  - Regulação da comunicação social (Art.º 39)
  - Direitos de antena, de resposta e de réplica política (Art.º 40)
  - Liberdade de consciência, de religião e de culto (Art.º 41)
  - Liberdade de criação cultural (Art.º 42)
  - Liberdade de aprender e ensinar (Art.º 43)
  - Direito de deslocação e de emigração (Art.º 44)
  - Direito de reunião e de manifestação (Art.º 45)

- Liberdade de associação (Art.º 46)
- Liberdade de escolha de profissão e acesso à função pública (Art.º 47)

- **Direitos, Liberdades e Garantias de Participação Política**
  - Participação na vida pública (Art.º 48)
  - Direito de sufrágio (Art.º 49)
  - Direito de acesso a cargos públicos (Art.º 50)
  - Associações e partidos políticos (Art.º 51)
  - Direito de petição e direito de ação popular (Art.º 52)

- **Direitos, Liberdades e Garantias dos Trabalhadores**
  - Segurança no emprego (Art.º 53)
  - Comissões de trabalhadores (Art.º 54)
  - Liberdade sindical (Art.º 55)
  - Direitos das associações sindicais e contratação coletiva (Art.º 56)
  - Direito à greve e proibição do lock-out (Art.º 57)

Nos últimos anos, tem vindo ao conhecimento público, várias noticias que retratam a importância da privacidade e a forma como facilmente podem afetar Direitos e Liberdades fundamentais.

O famoso caso "Verónica"[34] que ocorreu em Espanha, no qual a vítima passou a sofrer de humilhação no local de trabalho, pela publicação em grupos de WhatsApp de vídeo de teor sexual, que teria gravado no passado com um colega de trabalho, aquando solteira, com o qual teria tido uma relação. A rápida partilha do vídeo entre diversos colegas da empresa, promoveu vários comentários jocosos, que provocaram ansiedade, discriminação e uma pressão psicológica imensa, que levou a que esta triste situação, culmine com o seu suicido por enforcamento, deixando o marido e dois filhos, um de nove meses e outro de quatro anos.

Um outro caso famoso, ocorreu em *Duesseldorf*, na Alemanha, onde um paciente morre como resultado de um ataque de ransomware[35]. Um ataque informático a um hospital universitário, provocou o fecho das urgências, para além da interrupção das

operações da instituição. Uma paciente que seria atendida no local, morreu ao ter ficado retida, a aguardar pela transferência para um outro estabelecimento de saúde, a cerca de 32 km de distância, uma vez que os dados clínicos ficaram indisponíveis (cifrados) e limitando a sua transferência e tratamento em tempo útil.

Ambos os casos acima referidos, exemplificam situações de dano para os direitos, liberdades e garantias pessoais, estando em causa o condicionamento e/ou restrição de vários direitos.

Com a publicação do RGPD, especialmente no seu artigo 83.º, o mercado ficou apavorado com os montantes máximos previstos para os regimes sancionatórios, onde a coima pode atingir 20 Milhões de euros ou 4% do volume de negócio anual a nível mundial, consoante o montante que for mais elevado.

Apesar de se verificar um efeito pedagógico na captura da atenção, de dedicação e investimento das organizações na obtenção da conformidade com o RGPD, apesar do foco estar nos montantes sancionatórios a pagar ao Estado, o RGPD também prevê a compensação aos titulares de dados pessoais, nos termos do artigo 82.º do RGPD. Para além da obrigação legal, moralmente assume-se como fundamental, na busca de compensar quem realmente sofreu o dano, procurando a reposição do prejuízo causado ao titular(es) e não apenas o pagamento de coimas por não conformidade com a lei.

Esta consciência de cumprir com o artigo 82.º, procurando compensar o titular pela indeminização dos seus danos, identifica a necessidade de calculo do montante indemnizatório, tal como se de uma apólice de seguro se tratasse. Ora, tal como acontece nas apólices de seguro[36], na qual a lei estabelece os montantes, em função dos danos para o segurado, pelo que, em caso de violação de dados pessoais, por exemplo, espera-se ser possível identificar o valor da indemnização, que se destina a compensar pecuniariamente pelos danos causados.

Ao procurar por devida e acrescida fundamentação, foi possível observar o caso dos seguros em Portugal, tendo sido no passado publicada a Portaria n.º 679/2009 de 25 de junho, na qual são definidos os critérios e os montantes para indeminização a

vítimas de acidentes de viação. Todavia, assumindo que os valores apresentados são considerados como referência, não vinculando Tribunais[37], podem ser considerados de referência para os valores indemnizatórios nos termos do RGPD.

Este exemplo de obrigação legal, torna claro o montante de referência a ser pago em caso de materialização do risco (sinistro), o qual igualmente, igualmente de referência, quer pela semelhança dos danos, quer pelo objetivo de compensação, neste caso associado a danos decorrentes de tratamento de dados pessoais.

A Portaria n.º 679/2009 de 25 de junho, prevê deste modo a compensação pelos seguintes danos:

- **Danos morais complementares**
  - **Internamento** – aferido com base no número de dias de internamento, estando previsto um valor que pode variar entre 20,52€ a 30,78€.
    Com base no critério (intervalo) definido, é possível a sua representação pela seguinte expressão:

$$x \in Q_+ , \qquad 20{,}52 \leq x \leq 30{,}78$$

    Neste sentido, assumindo x o valor diário (em EUR) e a variável *n* o número de dias de internamento, o valor indemnizatório é obtido por:

$$y = n.x$$

  - **Dano estético** – calculado em função do número de pontos atribuídos relativamente ao dano estético causado, com base na seguinte tabela:

Dano estético	Até
1 ponto	820,80 €
2 pontos	1.641,60 €
3 pontos	2.462,40 €
4 pontos	4.104,00 €
5 pontos	5.745,60 €
6 pontos	7.438,50 €
7 pontos	10.260,00 €

Tabela 7 – Compensação de danos morais complementares

Os referidos valores na tabela, podem ser representados graficamente:

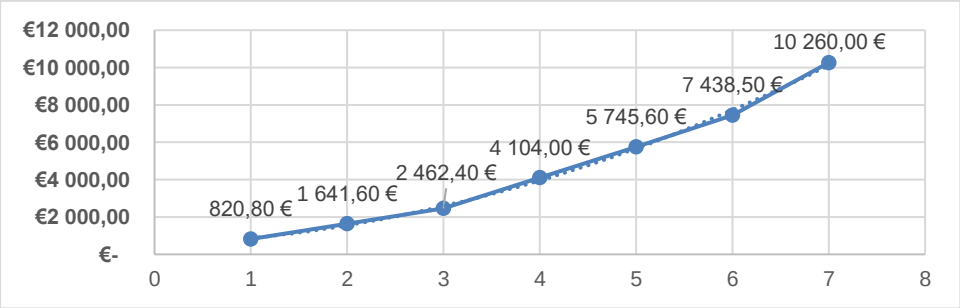


Figura 15 - Compensação de danos morais complementares

Ainda que não seja possível a sua representação de modo exato, é possível projetar o cálculo aproximado, com base na seguinte equação:

$$y = 171x^2 + 174{,}66x + 520{,}33, \qquad x \in \mathrm{N}_+ \mid x > 0$$

- ***Quantum doloris*** – respeita ao conjunto de sofrimentos, como consequência de lesões e sequelas, incluindo danos físicos e demais consequências ou repercussões psíquicas, assim como sofrimentos morais[38]. Quanto ao cálculo, este pode ser obtido com base na tabela:

Quantum doloris	Até
4 pontos	820,80 €
5 pontos	1.641,60 €
6 pontos	3.283,20 €
7 pontos	5.335,20 €

Tabela 8 - Compensação por Quantum doloris

Podendo esta ser representada graficamente da seguinte forma:

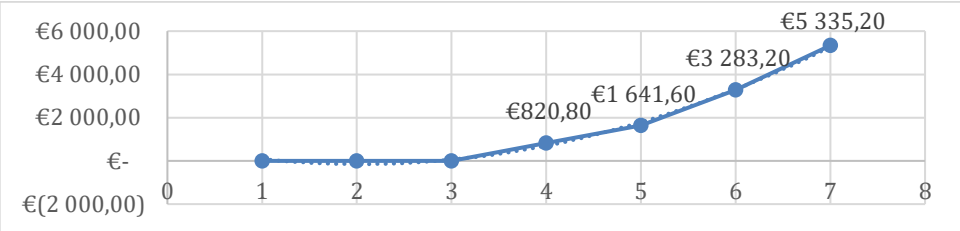


Figura 16 - Compensação por Quantum doloris

Não sendo possível a sua projeção exata, é possível projetar o cálculo aproximado com base na seguinte equação:

$$y = 219{,}86x^2 - 894{,}09x + 762{,}17, \qquad x \in \mathrm{N}_+ \mid x > 3$$

- **Repercussão na vida laboral** – obtido em função da avaliação do número de pontos que respeitam à dimensão da repercussão, é apenas indemnizável se for superior a 10 pontos e prevê a reparação do dano apenas e só quando a incapacidade seja impeditiva da atividade profissional, habitual ou outra. Neste sentido, é, pois, calculado com base na seguinte tabela:

Repercussão na vida laboral	<= 30 anos	31-45 anos	46-60 anos	61-70 anos
>10P e <=35P, máximo até:	25.650 €	20.520 €	15.390 €	10.260 €
>35P e <=70P, máximo até:	64.125 €	51.300 €	38.475 €	25.650 €
>70P, valor máximo até:	102.600 €	82.080 €	61.560 €	41.040 €

Tabela 9 - Compensação por Repercussão na vida laboral

Neste sentido, são representados graficamente os seguintes casos:

- <u>Para uma avaliação superior a 10P e menor ou igual a 35P:</u>

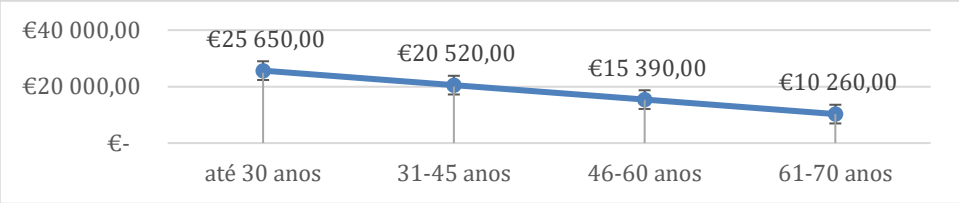


Figura 17 - Repercussão na vida laboral superior a 10P

Nestes termos, o valor é obtido por meio da seguinte equação,

$$y = -5130x + 30780\,, \qquad x \in \mathrm{N}_+ \mid x > 0$$

- <u>Para uma avaliação superior a 35P e inferior ou igual a 70P:</u>

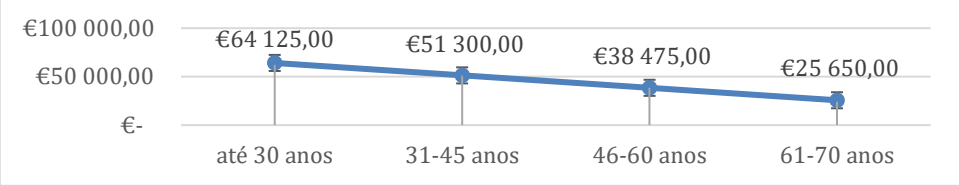


Figura 18 - Repercussão na vida laboral superior a 35P e menor que 70P

Nestes termos, o valor é obtido por meio da seguinte equação,

$$y = -12825x + 76950\,, \qquad x \in \mathrm{N}_+ \mid x > 0$$

- Para uma avaliação superior a 70P:

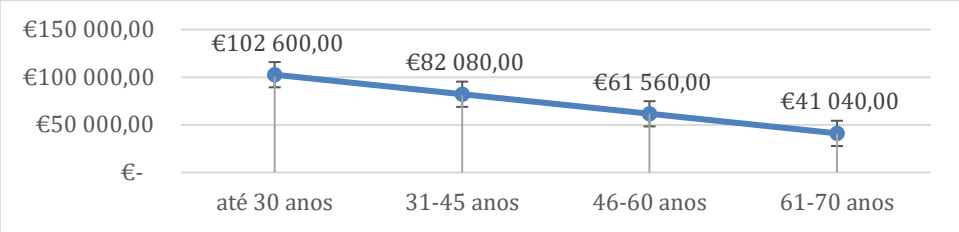


Figura 19 - Repercussão na vida laboral superior a 70P

Nestes termos, o valor é obtido por meio da seguinte equação,

$$y = -20520x + 123120\,, \qquad x \in \mathrm{N}_+ \mid x > 0$$

- **Incapacidade Permanente Absoluta (IPA)** – o valor de referência previsto apenas prevê jovem que não iniciou a vida laboral, contemplando um valor previsto máximo de até 200.000,00 € (EUR).

$$y = 200000$$

- **Danos em caso de morte e a título de danos morais aos herdeiros**
  - **Dano moral por perda de feto** – atendendo ao número de filhos existentes, caso seja ou não o primeiro filho, bem como o tempo de gravidez ocorrido. O valor indemnizatório é atribuído de acordo com a seguinte tabela, atendendo ao fator de majoração, caso a perda do feto (1º filho) ocorra em mãe com idade igual ou superior a 40 anos, no qual apenas a mãe sobreviva:

	N.º Filhos	
Tempo de gravidez	1º filho	2º filho ou posterior
Até às 10 semanas de gravidez, para ambos os pais divido em partes iguais.	Até 7.695 €	Até 2.565 €
A partir da 10º semana de gravidez, para ambos os pais divido em partes iguais.	Até 12.825 €	Até 7.695 €
Majorações		Até
Perda de feto (1º filho) com idade da mãe >= 40 anos, apenas para a mãe sobreviva		50%

Tabela 10 - Compensação por Dano moral por perda de feto

- Para o 1º filho, o valor é obtido por meio da seguinte equação,

$$y = -5130x + 12825\,, \qquad x \in \mathrm{N}_+ \mid 1 \leq x \leq 2$$

- Para o 2º filho ou posterior, é obtido por meio da equação,

$$y = -5130x + 17955\,, \qquad x \in \mathrm{N}_+ \mid 1 \leq x \leq 2$$

- **Direito à vida** – o valor apurado é obtido em função da idade da vítima, resultando dos critérios definidos na seguinte tabela:

	Idade da vítima			
	Até 25 anos	Entre 25 e 49 anos	Entre 50 e 75 anos	Mais de 75 anos
Aos herdeiros, em partes iguais (até):	61.560 €	51.300 €	41.040 €	30.780 €

Tabela 11 - Compensação por Direito à vida

Os referidos valores na tabela, podem ser representados graficamente da seguinte forma:

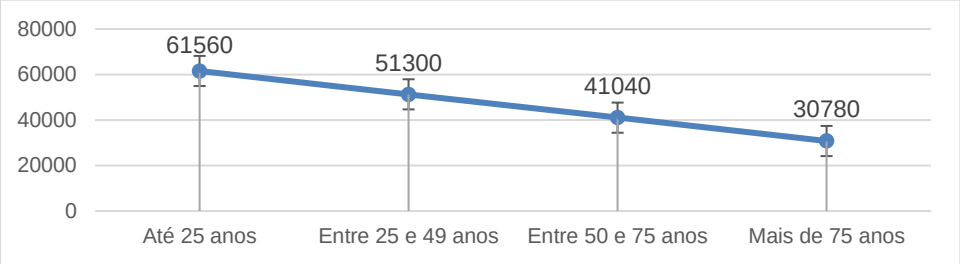


Figura 20 - Compensação por Direito à vida

Nestes termos, o valor é obtido por meio da seguinte equação,

$$y = -10260x + 71820\,, \qquad x \in \mathrm{N}_+ \mid 1 \leq x \leq 4$$

- **Dano moral da própria vítima** – calculado com base na seguinte tabela, em função do tempo de sobrevivência:

	Tempo de sobrevivência		
	Até 24 horas	Até 72 horas	Mais de 72 horas
Aos herdeiros, em partes iguais	Até 2.052 €	Até 4.104 €	Até 7.182 €
Nota: 72H é considerado clinicamente o período critico de sobrevivência.			
Majorações			Até
Os valores podem ser alvo de majoração, em função do nível de sofrimento e antevisão da morte.			50%

Tabela 12 - Compensação por Dano moral da própria vítima

A tabela acima, pode ser graficamente representada da seguinte forma:

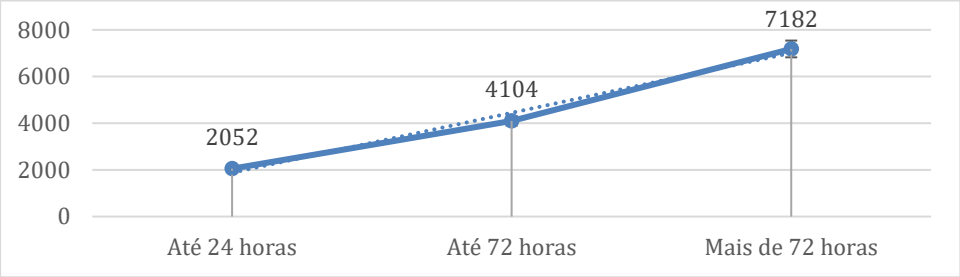


Figura 21 - Compensação por Dano moral da própria vítima

De acordo com o apresentado, conclui-se que o valor pode ser obtido por meio da seguinte equação:

$$y = 2565x - 684\,, \qquad x \in \mathrm{N}_+ \mid 1 \leq x \leq 2$$

Mesmo sendo exemplificativo e baseado em obrigações aplicáveis aos seguros, constitui uma boa orientação para estabelecer os montantes a serem pagos aos titulares de dados visados, servindo como referência indemnizatória sobre o valor que deve ser pago de acordo com o seu caso/natureza.

Este modelo, assenta na transparência, orientando as organizações na avaliação e quantificação de potenciais riscos indemnizatórios.

3 PROPOSTA DE INVESTIGAÇÃO

Um modelo de avaliação de risco de privacidade, que cumpra com as obrigações legais e regulatórias de proteção de dados pessoais, é morfologicamente complexo, todavia promove a oportunidade de orientações específicas, nomeadamente quanto ao cálculo indemnizatório para o(s) titular(es) de dados pessoais visado(s), e não apenas orientando quanto ao valor das coimas a aplicar.

3.1 CONTEXTUALIZAÇÃO

À semelhança do que se verifica nas normas de risco para a Segurança de Informação, *vide* ISO/IEC 27005, a avaliação recai sobretudo na ameaça, levando a que muitas vezes se ignore a valorização do benefício implícito no evento.

Ora, uma vez que a boa gestão de risco visa minimizar as ameaças e simultaneamente maximizar as oportunidades, potenciando e valorizando os benefícios, ao focar unicamente nas ameaças, quer na sua natureza/tipo e quantidade, perdem-se oportunidades e descoram-se benefícios que, podem justificar a aceitação de risco e naturalmente as suas respetivas ameaças.

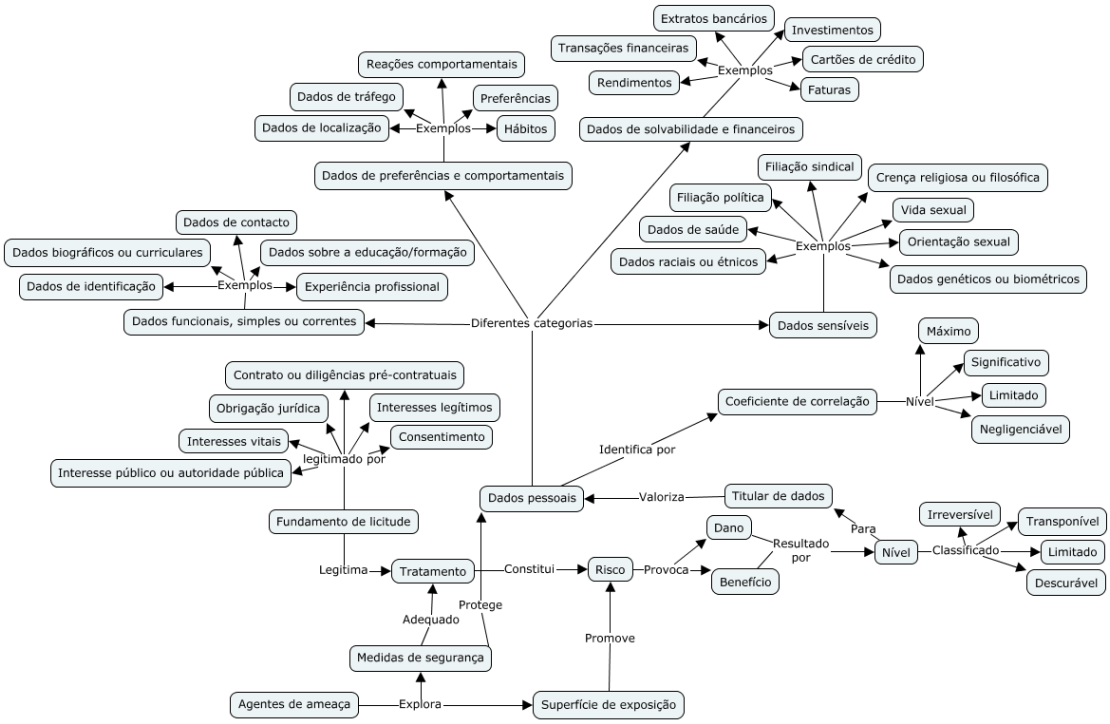


Figura 22 - Risco no RGPD – perspetiva holística

Caso a proteção de dados seja gerida em função de uma avaliação com foco único nas ameaças, descorará os benefícios/oportunidades no tratamento, que muitas vezes são a razão da sua realização, obtendo consequentemente, sempre, um resultado negativo na avaliação, uma vez que os critérios de avaliação apenas contemplam parte limitada dos critérios relevantes a analisar.

3.2 INQUÉRITO A PROFISSIONAIS

Atendendo à multidisciplinariedade da proteção de dados pessoais, foram realizados vários questionários a diferentes perfis, procurando identificar o entendimento e opinião de cada inquirido. Deste modo, foi solicitado a alguns distintos especialistas nacionais que simultaneamente detenham relevante curriculum em Proteção de Dados Pessoais, bem como à Associação de Encarregados de Proteção de Dados, a divulgação de um questionário que permita obter a opinião técnica especializada de notáveis atores do mercado, que sirva de orientação à presente tese.

A seguinte tabela, apresenta a distribuição dos diferentes perfis profissionais consultados que preencheram o referido questionário:

Função profissional	Frequência absoluta	Frequência relativa (%)	Frequência absoluta acumulada	Frequência relativa acumulada (%)
Encarregado de Proteção de Dados / *Data Protection Officer* (DPO)	11	28,9	11	28,9
Analista/Especialista/ Consultor(a) de Proteção de Dados	10	26,3	21	55,2
Analista/Especialista/ Consultor(a)/Engenheiro(a) Informática	3	8,0	24	63,2
Advogado(a)	6	15,8	30	79,0
Analista/Especialista de Segurança	4	10,5	34	89,5
Administrador (C-level)	3	7,9	37	97,4
Gestor de Projetos	1	2,6	38	100
Total	**38**	**100**		

Tabela 13 - Perfil dos inquiridos

Verificam-se considerações observáveis relevantes, designadamente o facto de mais de **55% dos inquiridos** atuam profissionalmente em função relevante de proteção de

dados pessoais, os quais são diariamente desafiados pelo objeto de estudo da presente tese. De realçar também, que o perfil profissional dos inquiridos, é direta ou indiretamente relacionado com a prática de proteção de dados, conferindo-lhes experiência quanto às questões suscitadas.

Não obstante da função exercida, verificou-se a seguinte distribuição de anos de experiência profissional:

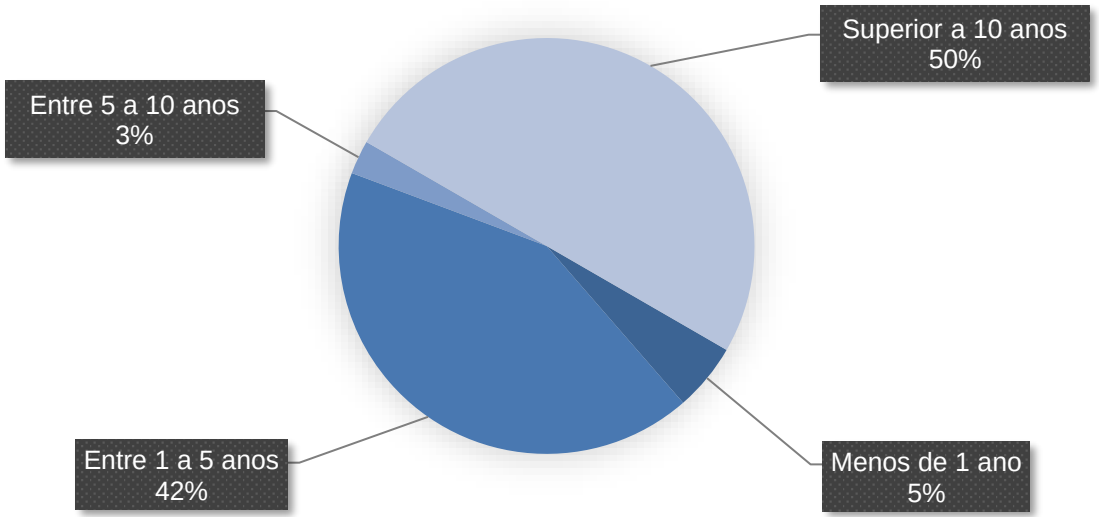


Figura 23 - Experiência profissional dos inquiridos

Como considerações observáveis, destaca-se que metade dos inquiridos possuem mais de **10 anos de experiência profissional**.

Por forma a assegurar a representatividade multissectorial, garantindo que a sensibilidade e experiência dos inquiridos não se circunscreve unicamente a um sector específico, procurou-se inquirir quanto à sectorialidade do exercício da atividade profissional.

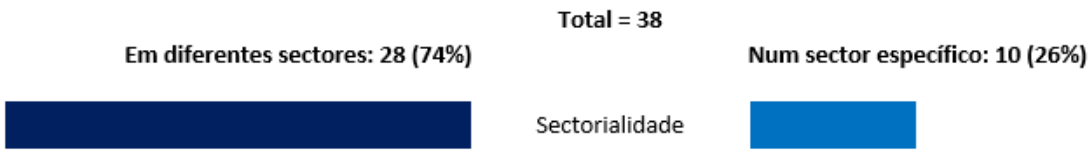


Figura 24 - Representatividade sectorial

Observa-se assim, uma muito significativa representatividade de atuação multissectorial, permitindo assim uma **visão mais inclusiva do mercado**.

Procurando obter a sensibilidade dos inquiridos, quanto à sensibilidade que o mercado tem para as diferenças entre o risco para o negócio e risco para a privacidade/proteção de dados pessoais, procurou-se inquirir os participantes da opinião que possuem, relativamente ao mercado distinguir as diferenças entre risco para o negócio e risco para a privacidade, tendo sido possível verificar as seguintes respostas:

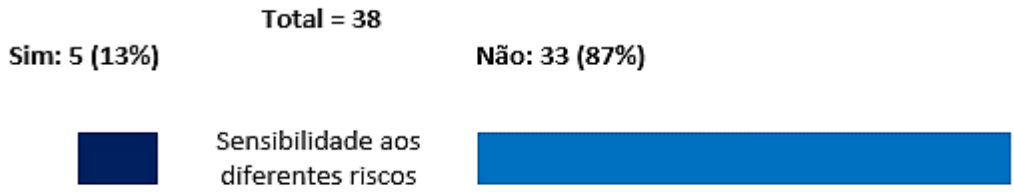


Figura 25 - Diferenciação entre risco para o negócio e para a privacidade

Conclui-se assim que a opinião de **87% dos inquiridos**, é de que o mercado não distingue as diferenças, confundindo e conflituando entre o risco para o negócio e o risco para a privacidade. Ora, tendo em conta a senioridade dos perfis inquiridos, conclui-se que o mercado não está devidamente consciente do previsto no RGPD em matéria de risco, realçando a importância de algumas considerações previamente destacadas, e do quão tempestivo se assume o presente estudo.

Não obstante de resultar claro nos termos da lei, a importância que a avaliação de risco assume na conformidade com o RGPD, procurou-se inquirir sobre esta questão, tendo-se verificado as seguintes respostas:

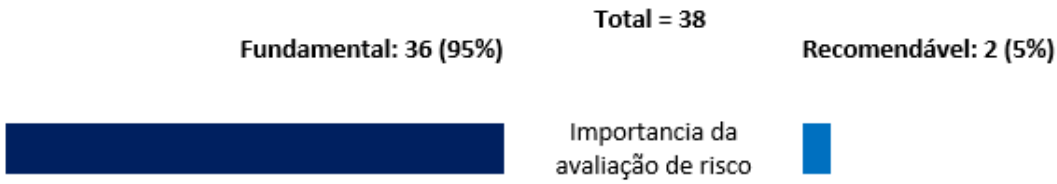


Figura 26 – Importância do risco na conformidade com o RGPD

A opinião resulta unanime, com **95% dos inquiridos** a considerarem fundamental, a importância da avaliação de risco na conformidade com o RGPD.

Atendendo à falta de orientação objetiva, quanto às diferentes dimensões e critérios a ter em conta na avaliação do risco para a privacidade/proteção de dados pessoais,

em conformidade com o RGPD, procurou-se obter a opinião técnica especializada dos participantes do questionário, quanto aos dados a ter em consideração para a avaliação de risco, tendo sido possível obter as seguintes conclusões:

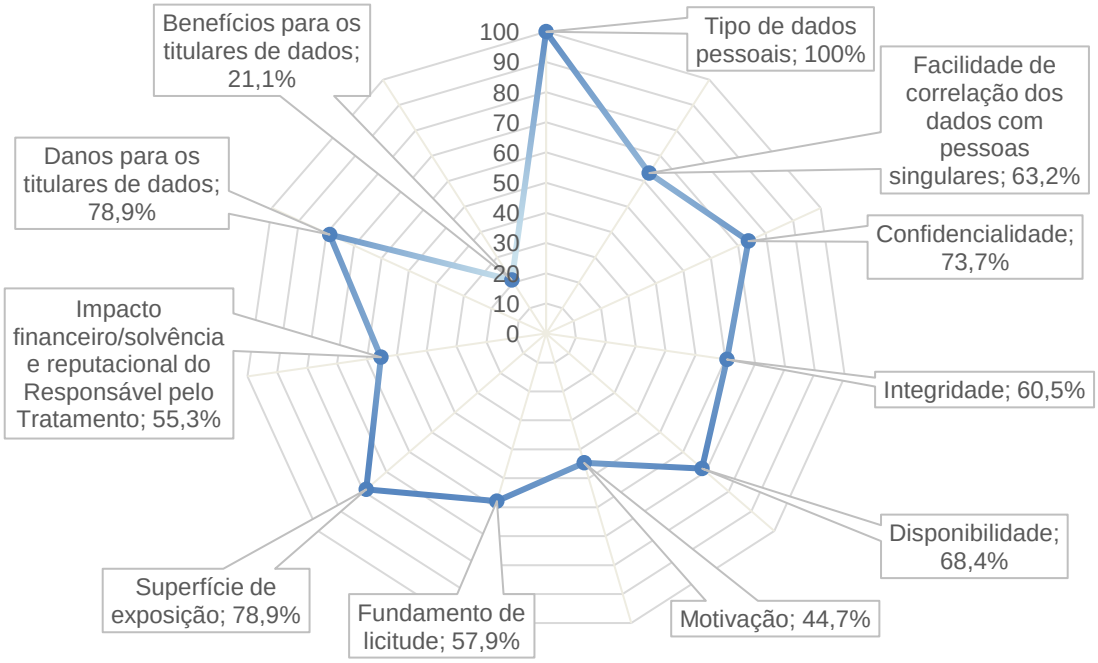


Figura 27 – Dimensão e critérios relevantes para avaliação de risco

Verifica-se deste modo que a **opinião dos inquiridos é equilibrada**, tendo sido assinalada com representatividade para a maioria dos dados, mesmo quanto para a "motivação" que se aproxima dos 50%, destacando-se apenas como exceção o "Benefício para os titulares de dados", que foi o menos votado, contando apenas com 21,1% dos votos.

Sem prejuízo das referências citadas no presente estudo, quanto à relevância dos danos materiais e não-materiais, designadamente se a sua importância deve ou não ser igualável, procurou-se inquirir se os danos materiais devem ter a mesma importância que os não-materiais, por exemplo: se a perda de liberdade ou de movimento pode ter a mesma importância que o prejuízo ou dano para a reputação, tendo com esta questão sido possível verificar as seguintes respostas:

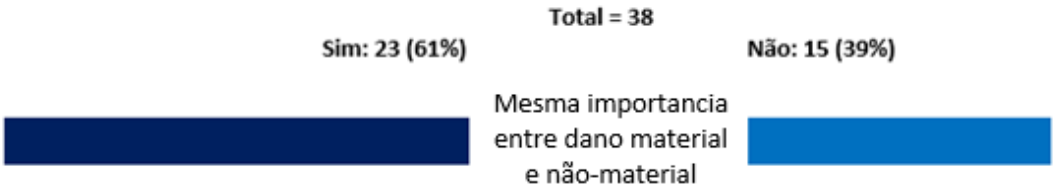


Figura 28 - Valorização igualável entre dano material e não-material

Deste modo, com base nas respostas obtidas, foi assim possível concluir que 61% dos inquiridos considera que independentemente de o dano ser material ou não-material, estes **devem ter a mesma importância**, pois, não obstante do seu tipo, ambos constituem dano para o titular.

Foi igualmente questionada à proficiência dos inquiridos, designadamente se já teriam implementado alguma metodologia de avaliação de risco para a privacidade, quer na sua organização ou clientes para quem prestem serviços, na qual verificou-se os seguintes resultados:

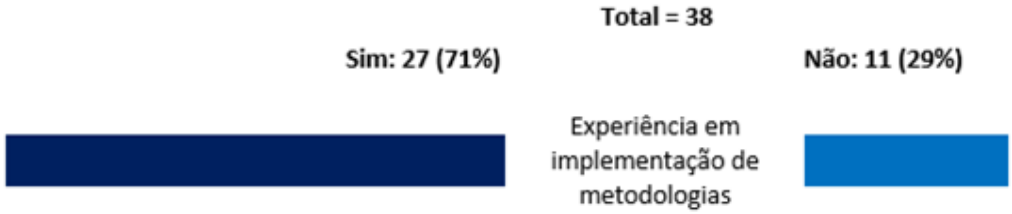


Figura 29 - Experiência em implementação de metodologias de risco

Neste sentido, uma vez que é verificável a comum **familiaridade e experiência** que os inquiridos têm **ao nível de metodologias e/ou *frameworks*** de avaliação de risco, procurou-se identificar quais as que mais usam nos seus trabalhos e experiência, tendo sido possível obter as seguintes respostas:

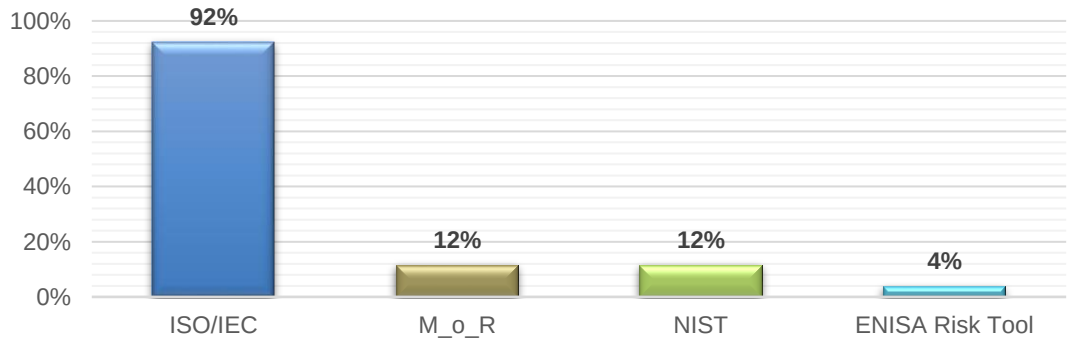


Figura 30 - Familiaridade com metodologias ou frameworks

Apesar de se verificar que vários inquiridos assinalaram experiência com mais de uma metodologia ou *framework*, as **ISO resultam como as mais familiares e utilizadas** pelos inquiridos. Todavia, sem prejuízo das metodologias adotadas, por uma questão de adequabilidade e exatidão, houve igualmente a preocupação de aferir se a definição da metodologia de avaliação de risco para a privacidade, teve o envolvimento de profissionais e/ou especialistas de risco, tendo-se verificado que as respostas obtiveram a seguinte distribuição:

Figura 31 - Participação/contribuição de profissionais de risco

Ora, de acordo com os resultados verificáveis, o "sim" assume-se com mais 8% de votos do que o "não", todavia é de realçar que ambos são demasiadamente próximos, concluindo desta forma a existência de **muitas implementações que não contam com a participação de profissionais e/ou especialistas em risco**, que garantam o cumprimento rigoroso das normas/melhores práticas.

Para uma correta e adequada implementação da avaliação de risco na organização, em conformidade com o RGPD, considera-se de absoluta importância a informação que o mercado dispõe. Assim, foi igualmente questionada a disponibilidade de informações profícuas, tendo sido possível obter as seguintes respostas:

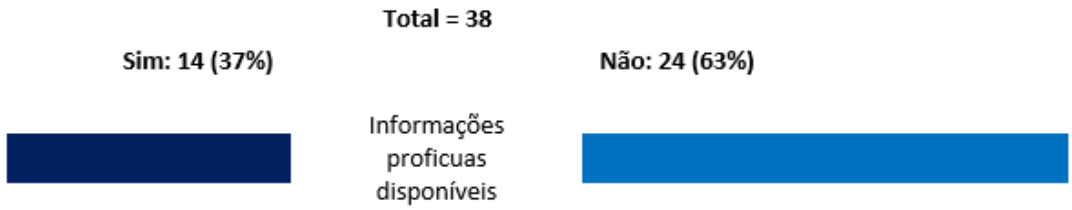


Figura 32 - Informação/recursos disponíveis sobre risco RGPD

Conclui-se desta forma que uma maioria com **63% dos inquiridos, conclui a inexistência de informações profícuas no mercado**, quanto à avaliação do risco de conformidade com o RGPD. Ora este indicador é igualmente relevante, pois influencia

a forma como o mercado perceciona o que deve ser uma adequada avaliação do risco, nos termos do RGPD.

Relativamente ao nível de consciencialização do mercado, relativamente ao RGPD prever a possibilidade de indeminização aos titulares de dados pessoais, para além das coimas em situação de não conformidade, verificaram-se as seguintes respostas:

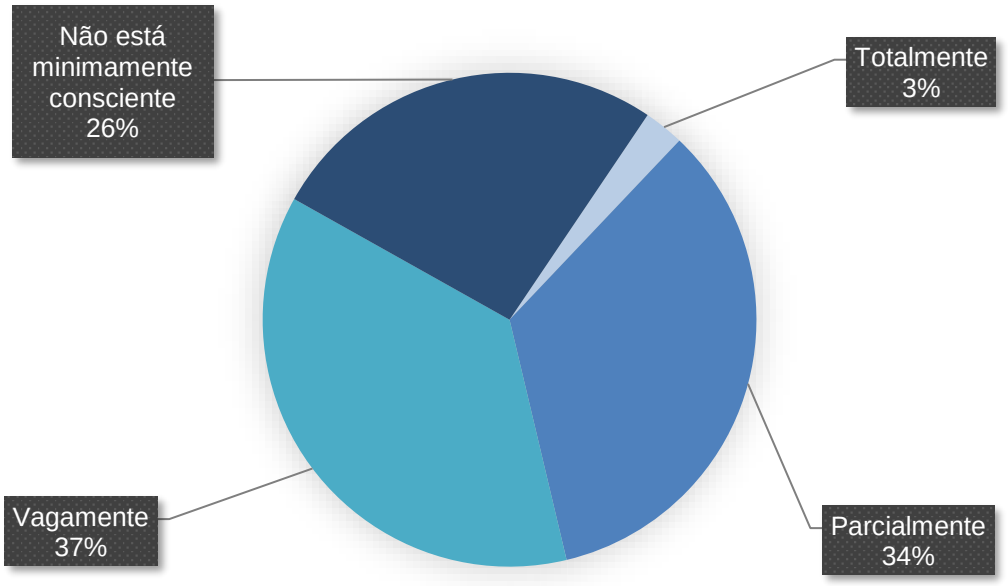


Figura 33 - Consciencialização do mercado à indeminização do titular

Avaliando a distribuição das respostas, observa-se que a indeminização do titular é, segundo os inquiridos, algo **nada ou vagamente consciencializado pelo mercado**, perfazendo **63% da opinião dos inquiridos**.

Ora, apesar da consciência que o mercado tem relativamente ao regime sancionatório, especialmente ao nível de coimas e pena de prisão prevista na lei, a consciencialização da potencial necessidade de indeminização ao(s) titular(es) dos dados é ainda algo desconhecido por muitos agentes do mercado, sendo um importante facto a ter em consideração por parte das organizações.

Questionou-se igualmente os inquiridos, quanto à sua opinião sobre a relevância da avaliação de risco permitir aferir sempre que possível, um valor indemnizatório aos titulares de dados, de caracter indicativo ou de referência. Com isto, as organizações poderiam ter uma mais completa e real perceção do risco, ao adicionar às regulares

avaliações, o potencial indemnizatório envolvido em caso de materialização do risco analisado. Foi assim possível obter as seguintes respostas:

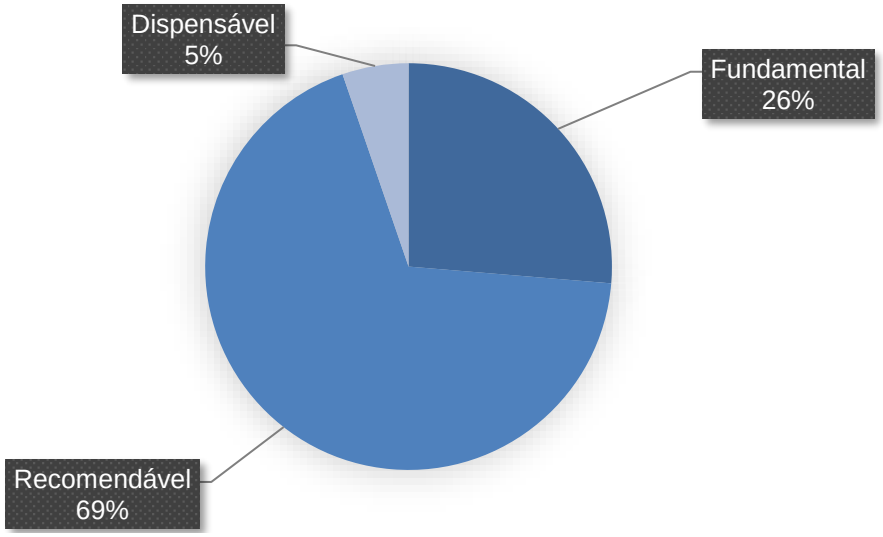


Figura 34 - Relevância da aferição indemnizatória prévia

Como conclusão observável das respostas dos inquiridos, resulta evidente que a opinião da maioria, com **69% dos inquiridos**, é de que a avaliação indemnizatória se **constitui como recomendável**.

Considerou-se igualmente pertinente questionar sobre a exequibilidade de que no momento da celebração de um contrato (ex. aquisição ou subscrição de produto ou serviço), serem solicitados elementos ao titular dos dados pessoais, que permitam dessa forma identificar o nível de apetite e de tolerância ao risco que este(s) se dispõem a experienciar.

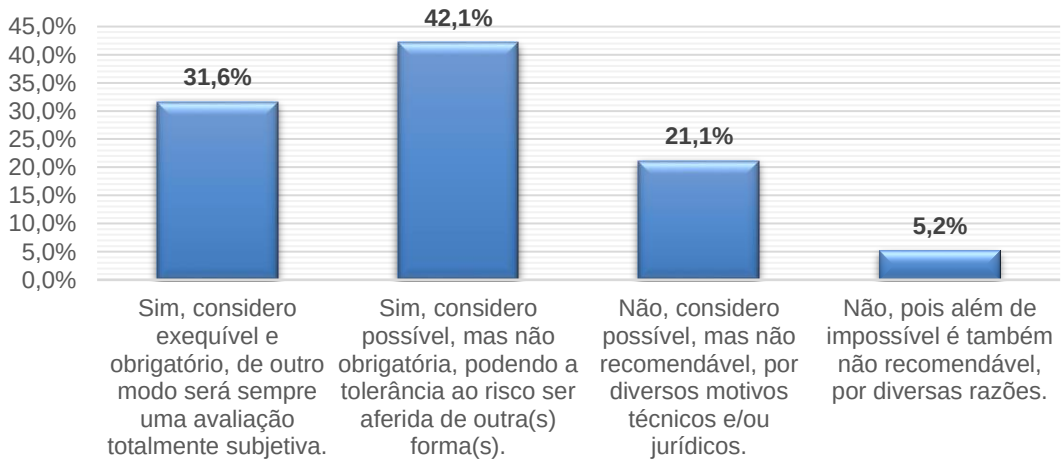


Figura 35 - Definição prévia de apetite e tolerância ao risco pelo titular

Observa-se que a maior concentração de votações, com 42,1% dos inquiridos, recai sobre a opção de ser possível que no momento da celebração de um contrato, seja aferido junto do titular o seu apetite e tolerância ao risco, todavia, consideram não ser obrigatório uma vez que esta pode ser aferida de outras formas. De igual modo, importa realçar que a segunda maior votação, com 31,6% dos inquiridos, considera exequível e obrigatório, pois de outro modo será sempre uma avaliação totalmente subjetiva, ao não ser indicada pelo titular.

Em suma, observa-se que **73,7% manifestam um parecer favorável**, contra 26,3% dos inquiridos.

Por forma a assegurar a inexistência de ambiguidades, os inquiridos que não responderam como "exequível e obrigatório", foi-lhes solicitada justificação à afirmação anterior, tendo sido possível obter as seguintes explicações:

Justificação de inquirido (1)

> "*Tratando-se na essência de direitos fundamentais, eles **são inalienáveis**, não me parece adequado colocar um titular perante essa **questão dilemática**, porquanto isso também significaria que o titular teria de estar perfeitamente consciente dos cenários de risco em causa, o que me parece **pouco exequível face à baixa maturidade** que se perceciona no dia-a-dia."*

Justificação de inquirido (2)

> *"Os Direitos, Liberdades e Garantias, constitucionalmente oferecidos, são **automaticamente adquiridos** pela pessoa singular e, salvo melhor opinião, **não são direitos disponíveis para o exercício ou livre arbítrio de terceiros**, apenas da própria pessoa singular."*

Justificação de inquirido (3)

> "*Implicaria a **recolha de mais dados**, de natureza sensível, cuja justificação/**legitimidade poderá ser questionável**.*"

Justificação de inquirido (4)

"*Resulta da **regulação aplicável** ao setor de atividade da empresa*".

Justificação de inquirido (5)

"*O titular dos dados poderá em muitos casos **nao conseguir avaliar a sua própria tolerância** ao risco, **sem se ver perante a materialização** do mesmo."*

Justificação de inquirido (6)

"*Exemplo disso é o método utilizado pelo Sistema Bancário que avalia o nível de exposição de risco de cada cliente e **solicita uma autoavaliação do mesmo ao seu nível de risco**. O mesmo é classificado entre 3 a 5 níveis. Este sistema poderia facilmente ser utilizado no cálculo do impacto, pois o mesmo tinha **em conta a variável atribuída pelo próprio titular** dos dados no que toca à "importância/valor" que atribui aos dados "disponibilizados" perante aquele Responsável de Tratamento."*

Justificação de inquirido (7)

"*Falamos sempre na **Liberdade e Consciência** da escolha*".

Justificação de inquirido (8)

"*Quantos **mais dados forem solicitados**, maior é o risco de indemnização.*"

Justificação de inquirido (9)

"***Pode ser aferida**, a apetência pelo risco, por inquéritos como os que os bancos têm para **definir o perfil do cliente**."*

Justificação de inquirido (10)

"O limite ao risco poderá ser valorizado no momento contratual, contudo como o risco relevante diz respeito ao risco para os direitos liberdades e garantias dos titulares dos dados, e ***DLG são direitos indisponíveis pelo menos no seu cerne****, a sua* ***valorização não poderá fazer depender da prestação essencial*** *do serviço ou o seu preço,* ***mas sim acessoriamente*** *outros serviços".*

Justificação de inquirido (11)

"Podemos estar ***disponíveis para correr determinados riscos****, independentemente de ser ou nao compensado por isso".*

Justificação de inquirido (12)

"A possibilidade de recolher ***dados pessoais sensíveis*** *para auferir a tolerância ao risco."*

Relativamente às expectativas previstas, e tendo em conta a experiência e sensibilidade dos inquiridos, foi questionado como previam vir a ser o impacto dos eventos de privacidade nos próximos 5 anos, tendo sido possível obter o seguinte:

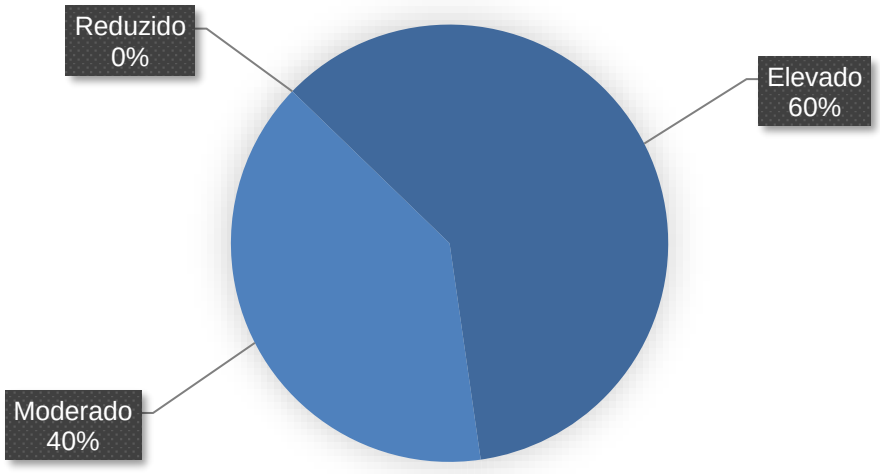


Figura 36 - Impacto dos eventos de privacidade em 5 anos

Observa-se que **60% dos inquiridos**, assumem a expectativa de que os próximos 5 anos terão um **agravamento do impacto dos eventos de privacidade**, o que se considera compreensível, tendo em conta algumas repentinas mudanças a que muitas organizações se viram sujeitas, muito especialmente devido aos impactos do COVID19.

No entanto, importa igualmente realçar que 40% dos inquiridos, embora reconheçam igualmente o agravamento dos eventos, creem que se sentirá um impacto de teor mais moderado, não tendo existido nenhum que tenha manifesto uma previsão de impacto reduzido.

Tendo em conta as tendências tecnológicas e as transformações a que o mercado tem sido forçado nos últimos 3 anos (ex.: aumento das obrigações regulatórias, pandemia COVID19, etc.), os inquiridos foram também convidados a responder sobre como definem/avaliam a evolução do risco para os titulares de dados pessoais.

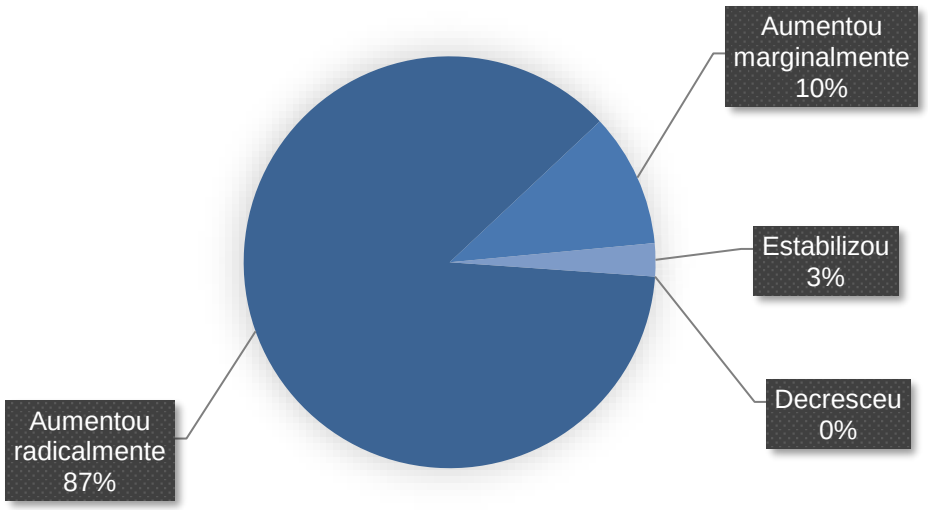


Figura 37 - Evolução do risco de proteção de dados nos últimos 3 anos

Resulta claro que, uma muito expressiva opinião de **87% dos inquiridos**, afirma que nos últimos 3 anos, o risco para os titulares de dados **evoluiu radicalmente**.

Procurando realizar um exercício de avaliação da proporcionalidade entre os benefícios e os danos para o(s) titular(es) num mesmo, foi questionado aos inquiridos, como consideram esta relação, tendo-se obtido as seguintes respostas:

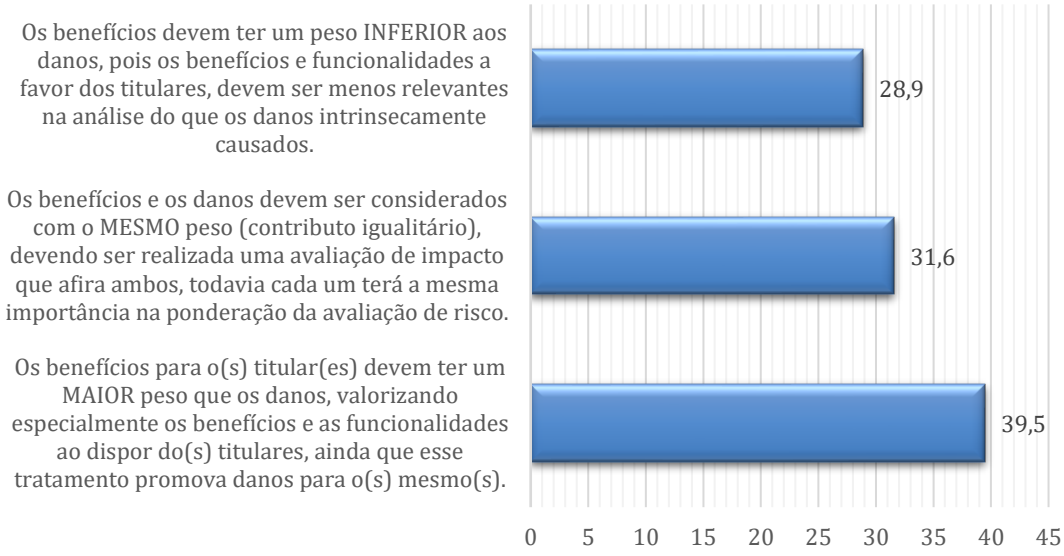


Figura 38 - Proporcionalidade entre benefícios e danos

Apesar dos inquiridos terem já expressado que não consideravam os benefícios para os titulares como elemento a ter em conta na avaliação de risco, surpreendentemente verifica-se que um número muito expressivo de inquiridos, sobrevaloriza os benefícios em detrimento dos danos. Quer com isto dizer que, se um tratamento de dados pessoais, se proporcionalizar um benefício (ex. nova funcionalidade) e esta corporizar igualmente um dano para o titular, cerca de **40% dos inquiridos** crê, que os **benefícios devem contar mais que os danos resultantes**.

Tendo em conta a possível complexidade da avaliação de risco de proteção de dados pessoais, inquiriu-se os participantes desta avaliação, sobre se utilizam algum software para avaliar o referido risco, que facilite o processo ao proporcionar uma avaliação por defeito, dispensando demais configurações específicas. Como resposta, verificou-se o seguinte:

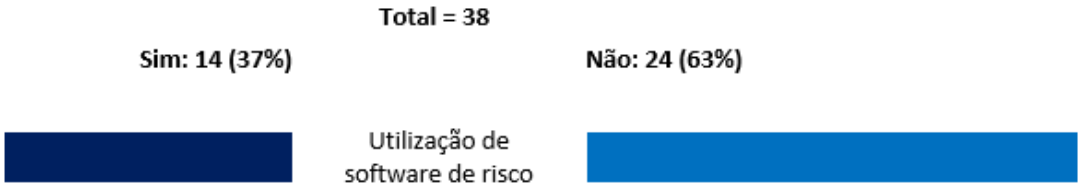


Figura 39 - Utilização de software de risco

Atendendo aos 37% de inquiridos que afirmaram positivamente a utilização de software, foi igualmente questionado a qual software recorrem, permitindo analisar

se os mesmos proporcionam uma avaliação por defeito, dispensando complexas e exigentes configurações, e simultaneamente avaliar numa perspetiva de *market share*, quais são os mais utilizados pelo mercado.

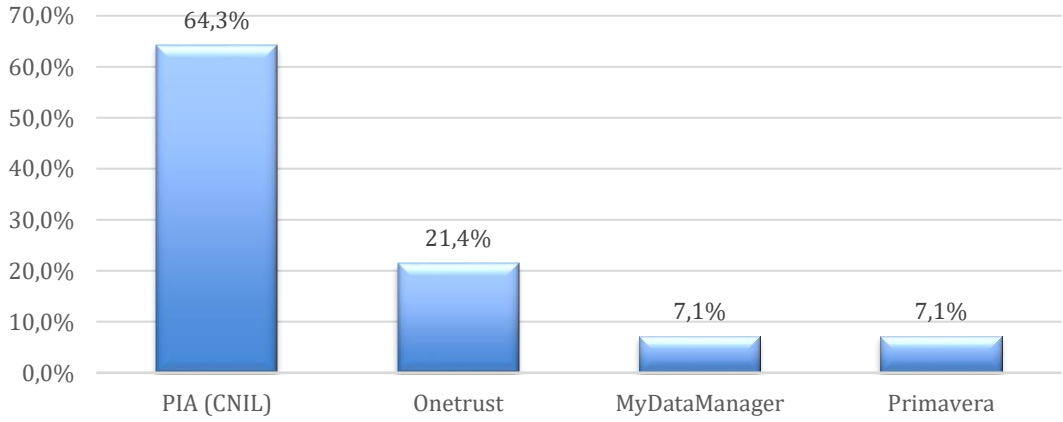


Figura 40 - Detalhe do software de risco utilizado

Ora, foi assim possível verificar que o **software mais utilizado é o PIA da CNIL, com 64,3% de utilização**, que sendo um software gratuito e produzido pela Autoridade de Controlo Francesa, permite um nível de confiabilidade metodológica muito importante para as organizações que procuram nos seus programas de conformidade, o cumprimento com o RGPD. Adicionalmente, o facto de ser um software gratuito, torna-se muito aliciante o seu uso, especialmente para as micro e pequenas empresas, pelas limitações orçamentais que as caracteriza, as quais representam uma significativa maioria do tecido empresarial Português.

De realçar o Onetrust com 21,4% dos inquiridos, que permite a utilização do modelo PIA da CNIL por via de "*assessment templates*", desenvolvido pela Onetrust com a colaboração da CNIL.

3.3 PROCESSO DE AVALIAÇÃO DO RISCO DE PRIVACIDADE

Não obstante das limitações e inadequabilidades das normas ISO, já referidas anteriormente no presente estudo, verificam-se outros importantes benefícios, especialmente ao nível da familiaridade/literacia que o mercado possui das mesmas, as quais se consideram como orientação para a presente proposta de modelo de

avaliação de risco, sendo naturalmente ajustadas, de modo a obter a conformidade com o RGPD e demais obrigações legais aplicável em matéria de dados pessoais.

Com vista a elaborar um processo de avaliação do risco de privacidade, que cumpra com as obrigações previstas no RGPD, foi elaborada uma proposta baseada no processo da ISO/IEC27005, uma vez que os resultados dos inquéritos aos profissionais e especialista, revelam uma (quase) unanime familiaridade com a ISO.

Por outro lado, tendo em conta a publicação da ISO/IEC27701:2019 que procura constituir uma extensão à ISO/IEC27001 e ISO/IEC27002, para a gestão da informação na privacidade, realçando a importância da família ISO2700x, foi especialmente tidas em conta, entre as cláusulas 6.1.1 à 6.1.3 e da 8.2 à 8.3 da ISO/IEC27001:2013, a qual se encontra alinhada com o processo da ISO/IEC27005.

Foram assim elaborados os seguintes processos, os quais serão detalhados paulatinamente ao longo do presente capítulo:

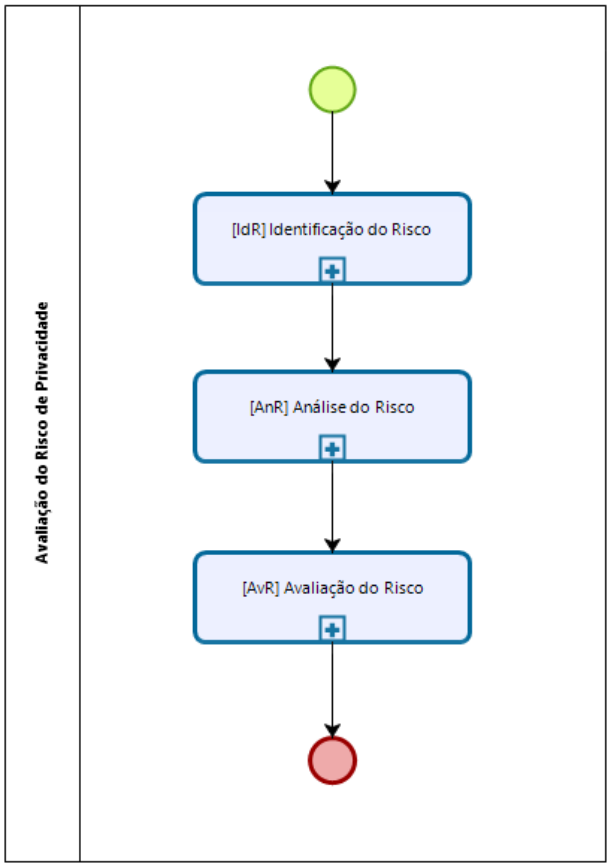


Figura 41 - Macroprocesso de Avaliação de Risco na Privacidade

Macroprocesso: Avaliação do Risco de Privacidade

Dispõe de 3 diferentes subprocessos:

1. **Identificação do risco** – procura identificar:
    a. Dados e respetivo coeficiente de correlação: assim como são identificados os ativos relevantes nas normas arquétipos do presente estudo, como algo que tem valor, sendo naturalmente a informação um ativo primário, foi assim considerado fundamental a identificação dos dados pessoais e a facilidade de correlação destes com pessoas singulares;
    b. Fundamento de licitude utilizado(s): visa identificar a existência de fundamento legítimo para a operação de tratamento de dados pessoais, procurando identificar se o tratamento é lícito, e medindo de acordo com o fundamento invocado;
    c. Danos e/ou benefícios para o titular: procura identificar quais os danos e os benefícios envolvidos, procurando medir a proporcionalidade destes numa base de equilíbrio, compreendendo que existem danos resultantes de benefícios para os titulares (ex. no decorrer da prestação de um serviço);
    d. Segurança dos dados: tendo em conta as propriedades da segurança da informação (ex. confidencialidade, integridade e disponibilidade), procura-se identificar eventuais vulnerabilidades relacionadas, designadamente que promovam respetivamente o acesso ilegítimo, modificação indesejada e/ou perda de dados pessoais.
    e. Superfície de exposição: visa identificar a extensão da exposição, nomeadamente se trata de grande exposição, por exemplo para a Internet, ou se encontra meramente circunscrito a um número limitado de pessoas/organizações/processos. Neste sentido, resulta que para uma correta identificação, seja tido em conta a eventual transferência de dados para países terceiros ou organizações internacionais que possam dificultar o controlo e direitos dos titulares.

2. **Análise do risco** – procura avaliar e determinar:

a. Severidade: tendo em conta os dados pessoais envolvidos e a sua facilidade de correlação com os respetivos titulares, bem como o eventual fundamento de licitude e os danos/benefícios para o titular, resulta assim possível a avaliação do impacto do(s) evento(s);
b. Verosimilhança: atendendo ao risco de segurança dos dados e à superfície de exposição, permite assim avaliar a probabilidade de materialização do(s) evento(s), pela facilidade/propensão de ocorrência.
c. Nível de risco: obtido com base na conjugação da severidade e da verosimilhança previamente avaliada.

3. **Avaliação do Risco** – visa qualificar a avaliação do nível de risco, priorizando em função do risco para os titulares, baseado em critérios.

3.3.1 Identificação do risco

Procurando o alinhamento com o que os inquiridos manifestaram no questionário, ao considerarem ser com a ISO que possuem uma maior familiaridade e experiência, resultou nesse sentido a elaboração do seguinte processo, alinhado com o processo previsto na ISO/IEC27005:

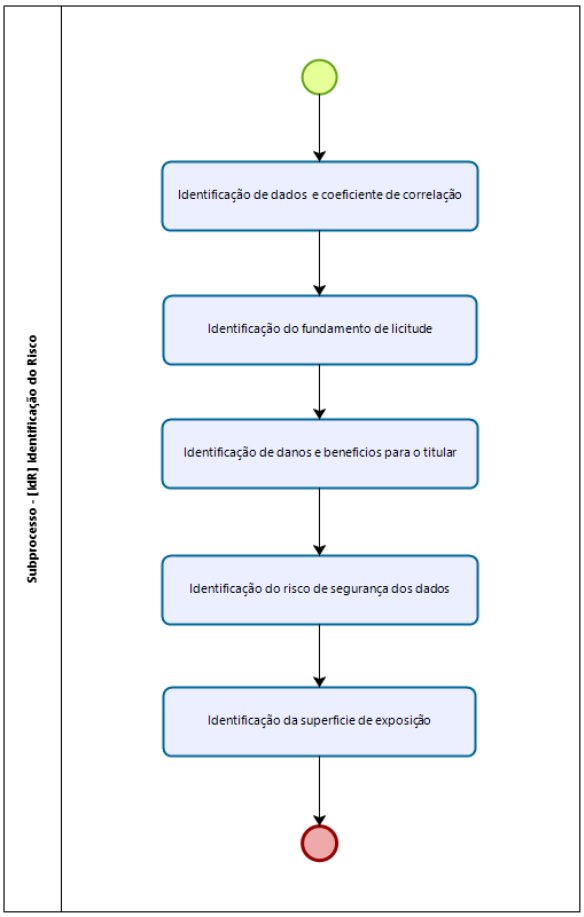


Figura 42 - Processo de identificação de risco

Para que seja realizada uma adequada identificação do risco, deve ser definido e aplicado um processo que:

- Identificação de dados pessoais tratados e coeficiente de correlação

  Tal como definido no normativo arquétipo, considera-se fundamental a identificação dos ativos relevantes, designadamente no contexto do presente processo, os dados pessoais a tratar/tratados. Pode ser devidamente identificado, tendo em conta a seguinte tabela:

Categoria de dados pessoais	Exemplos
Dados funcionais, simples ou correntes	• Dados de identificação • Dados biográficos ou curriculares • Dados de contacto • Dados sobre a educação/formação • Experiência profissional
Dados de preferências e comportamentais	• Dados de localização • Dados de tráfego • Reações comportamentais • Preferências • Hábitos

Dados de solvabilidade e financeiros	• Rendimentos • Transações financeiras • Extratos bancários • Investimentos • Cartões de crédito • Faturas
Dados sensíveis	• Dados raciais ou étnicos • Dados de saúde • Dados genéticos ou biométricos • Crença religiosa ou filosófica • Filiação política • Filiação sindical • Vida sexual • Orientação sexual

Tabela 14 - Tipo de dados pessoais

Para além do tipo de dados pessoais identificados, existe igualmente a necessidade de identificar a facilidade de correlação destes com pessoas singulares, ou seja, quão fácil será identificar pessoas singulares com os dados pessoais do tratamento em causa.

Pode ser devidamente identificado, tendo em conta a seguinte tabela:

Coeficiente de correlação	Descrição
Máximo	A facilidade de identificação com uma única pessoa singular é absoluta e total, não podendo os dados ser relacionados com mais nenhuma outra pessoa singular.
Significativo	Dificilmente os dados podem ser associados a outras pessoas singulares, garantindo uma elevada certeza na atribuição a uma ou poucas pessoas. Restará sempre alguma reduzida incerteza, quanto ao facto dos dados pertencem a uma única pessoa singular ou a um número muito reduzido de titulares.
Limitado	Podem ser associados a algumas (poucas) pessoas no seu contexto (i.e., nome abreviado).
Negligenciável	Podem ser associados a diversas pessoas no seu contexto (i.e., primeiro nome)

Tabela 15 – Coeficiente para a facilidade de identificação da ENISA

- <u>Identificação do fundamento de licitude</u>

  A licitude está relacionada com o fundamento legítimo para a operação de tratamento dos dados pessoais, procurando identificar se o tratamento é

lícito. Deste modo, tendo em conta o fundamento invocado, será atribuído um valor a considerar para avaliação.

Pode ser devidamente identificado, tendo em conta a seguinte tabela:

Fundamento de licitude	Descrição
Consentimento	Quando o titular dos dados tiver dado o seu consentimento de livre vontade, para o tratamento/finalidade em causa, o qual foi obtido de forma clara e concisa, num pedido que especifica a utilização que será dada aos dados pessoais, com disponibilização dos devidos contactos ao dispor do titular.
Contrato ou diligências pré-contratuais	Sempre que o tratamento seja necessário para a execução de um contrato (ex. celebração, execução ou gestão do contrato), no qual o titular é parte, ou para diligências pré-contratuais (ex. propostas) a pedido do titular dos dados.
Obrigação jurídica	Quando o tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito (ex. colaboração com entidades judiciais, fiscais ou reguladores).
Interesses vitais	Sempre que o tratamento é necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular (ex. quando o tratamento não se pode basear manifestamente noutro fundamento jurídico e este é necessário à proteção de um interesse essencial à vida, ex. para fins humanitários).
Interesse público ou autoridade pública	Caso o tratamento seja necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento (ex. exercício de autoridade)
Interesses legítimos	Quando o tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança (ex. melhoria do serviço, deteção de fraude, …).

Tabela 16 – Fundamento de licitude

- Identificação de danos e benefícios para o titular

  Procura identificar os danos e os benefícios envolvidos, designadamente direitos, liberdades e garantias (DLG), por forma a procurando medir a sua proporcionalidade, numa base de equilíbrio, tendo em conta a existência de

danos resultantes de benefícios para os titulares, como por exemplo; no decorrer da prestação de um serviço de cibersegurança (benefício), resultar a necessidade de acesso ao conteúdo de mensagens privadas para análise, e com isto, comprometer o sigilo da comunicação (dano).

Pode ser devidamente identificado, tendo em conta a seguinte tabela:

Resultado do produto entre o dano e o benefício	Descrição
Irreversível	Ainda que existam reais benefícios para o titular, o tratamento promove danos significativos ou de potencial irreversível.
Transponível	Na avaliação, verifica-se a existência de benefícios, porém os danos resultantes são consideráveis e dificilmente ultrapassáveis.
Limitado	Ainda que se identifiquem danos, estes não são significativos e assumem-se francamente ultrapassados pelos benefícios para o titular.
Descurável	Os benefícios são claros e relevantes, porém os danos são muito reduzidos ou mesmo indetetáveis.

Tabela 17 – Resultado do produto entre dano e benefício

- <u>Identificação do risco de segurança dos dados</u>

  Tendo em conta as propriedades da segurança da informação, nomeadamente; confidencialidade, integridade e disponibilidade, procura-se identificar eventuais vulnerabilidades relacionadas, que promovam respetivamente; o acesso ilegítimo, modificação indesejada e/ou perda de dados pessoais. Pode ser devidamente identificado, tendo em conta a seguinte tabela:

Propriedade	Ameaça associada	Descrição
Confidencialidade	Acesso ilegítimo	Quando a informação é acedida por partes não autorizadas ou sem legitimidade para acesso à mesma. Esta dimensão varia de acordo com o potencial de extensão da divulgação, tendo em conta o volume de dados e o tipo de dados em tratamento.
Integridade	Modificação indesejada	Ocorre quando a informação é alterada, promovendo prejuízo para o titular. Varia de acordo com a capacidade e tempo de deteção e com a criticidade da modificação para o titular.

Disponibilidade	Perda de dados	Sempre que os dados são necessários e não podem ser acedidos. Pode ser mais relevante, tendo em conta o potencial da perda ser periódica ou permanente.

Tabela 18 – Dimensões do risco de segurança dos dados

- Identificação da superfície de exposição

  Visa identificar a amplitude de visibilidade e extensão da exposição, nomeadamente se expõe para toda a Internet, ou se encontra circunscrito a um número limitado de pessoas/organizações/processos.

  Deve ter em conta, as transferências de dados para países terceiros, ou para organizações internacionais, que possam de algum modo dificultar o controlo e direitos dos titulares.

  Há igualmente a necessidade de identificar a intenção que levou ao evento, nomeadamente se esta foi acidental (ex. ação inadequada, erro humano ou de software ou configuração incorreta) ou maliciosa (ex. roubo/hacking, venda de dados com obtenção de lucro ou vantagem), esta última deverá constituir um fator agravador, pois influi dano para o titular dos dados.

  Pode ser devidamente identificado, tendo em conta a seguinte tabela:

Dimensão	Descrição
Exposição	Identifica a amplitude de visibilidade do evento, atendendo à sua exposição a pessoas/organizações/processos.
Trânsfuga	Valida a ocorrência de transferências para países terceiros, ou organizações internacionais, que dificulte/limite o controlo e os direitos, podendo vir a instrumentalizar os dados contra os seus próprios titulares (ex. extorsão).
Motivação	Analisa se a causa do evento tem intenção maliciosa ou acidental, pois quando esta é maliciosa, constitui um agravamento do dano para o titular. Assume maior relevância em cenários de avaliação de violação de dados pessoais e/ou incidentes de segurança.

Tabela 19 – Identificação das dimensões da superfície de exposição

3.3.2 Análise do risco

Deve ser definido um processo de análise do risco de privacidade, e não apenas de segurança de informação, a fim de cumprir com as obrigações legais e regulatórias aplicáveis.

Procura-se assim, avaliar a severidade potencial resultante para os titulares de dados pessoais (pessoas singulares), nomeadamente, ao nível dos seus direitos e liberdades fundamentais.

De igual modo, procura-se avaliar a verosimilhança de ocorrência, permitindo determinar deste modo o respetivo nível de risco.

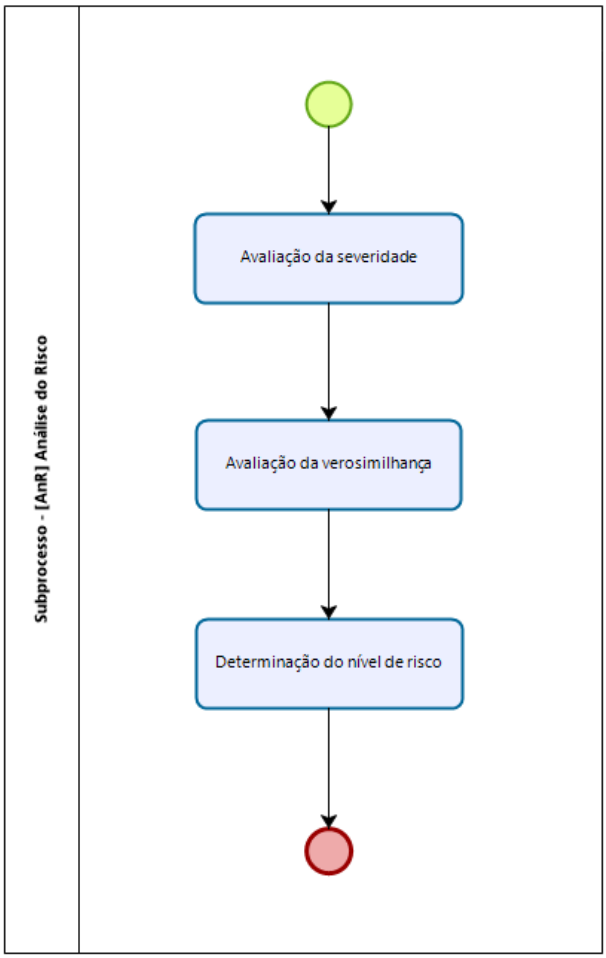


Figura 43 - Processo de análise de risco

- <u>Avaliação da severidade</u>

  Considera a categoria ou os dados pessoais envolvidos e a sua facilidade de correlação com os respetivos titulares.

  De igual modo, tem em conta a existência/tipo de fundamento de licitude e os danos/benefícios para o titular, permitindo assim avaliar a severidade do(s) evento(s).

  A avaliação é obtida pela seguinte formula:

$$Sv = D * F_c * F_l * D\hat{}B$$

Sv – Severidade
D – Dados pessoais envolvidos
F_c – Facilidade de correlação
F_l – Fundamento de licitude
$D\hat{}B$ – Danos e benefícios para o titular

Para isso, logo após a identificação dos dados pessoais relevantes, procede-se à avaliação dos mesmos, tendo em conta os seguintes critérios de classificação, de acordo com as 4 tipologias referidas na tabela 22 e a seguinte atribuição;

Tipo de dados	Valor
Dados funcionais, simples ou correntes	+1
Dados de preferências e comportamentos	+2
Dados de solvabilidade e financeiros	+3
Dados sensíveis	+4

Tabela 20 - Avaliação do tipo de dados com base na ENISA

Sempre que não seja possível obter conclusões comportamentais do titular, e/ou não se anteveja qualquer outro fator de agravamento, pode ser ponderado a diminuição da pontuação em "-1" valor.

De igual modo, se os dados envolvidos no tratamento pertencerem a pessoas vulneráveis (i.e. menores, doentes, idosos, colaboradores ou outro tipo), deve ser aumentado "+1" valor atribuído.

Deve ser avaliada quanto à facilidade de identificação/associação inequívoca de uma determinada pessoa singular.

Neste sentido, a pontuação deverá ser considerada, tendo em conta os seguintes critérios:

Coeficiente de correlação	Valor
Negligenciável	+0,25
Limitado	+0,50
Significativo	+0,75
Máximo	+1

Tabela 21 – Avaliação do coeficiente de correlação

O fundamento de licitude é outro elemento fundamental para cálculo, devendo este ser ponderado, tendo em conta a seguinte referência:

Fundamento de licitude	Valor
Consentimento	+1
Contrato ou diligências pré-contratuais	
Obrigação jurídica	
Interesses vitais	
Interesse público ou autoridade pública	
Interesses legítimos	+2
Inexistência de fundamento	+4

Tabela 22 – Avaliação do Fundamento de licitude

O último elemento do cálculo, é obtido pelo valor relativo ao ponderador resultante dos danos e benefícios para o titular. Este, é obtido com base na seguinte tabela:

Ponderador de dano e benefício	Valor
Descurável	+1
Limitado	+1,5
Transponível	+2
Irreversível	+4

Tabela 23 – Avaliação do dano e benefício

Consideram-se deste modo identificados os critérios e argumentos de avaliação necessários cálculo da severidade, a qual se conclui ter os resultados compreendidos no seguimento domínio:

$$D_{sv} = [\ 0{,}25\ ;\ 64\ ]$$

Dentro do referido domínio, encontram-se todas as possíveis combinações de cenários respeitantes às seguintes propriedades e resultados:

Dimensões	Propriedades	Nível de Risco			
		Baixo	Médio	Alto	Máximo
Severidade	Dados pessoais envolvidos	Funcionais	Preferências	Solvabilidade	Sensíveis
	Facilidade de correlação	Negligenciável	Limitado	Significativo	Máximo
	Fundamento de licitude	Consentimento	Interesses legítimos		Inexistência de fundamento
		Contrato			
		Obrigação jurídica			
		Interesses vitais			
		Interesse público ou autoridade pública			
	Danos e benefícios para o titular	Descurável	Limitado	Transponível	Irreversível

Tabela 24 - Valores de referência da qualificação da "severidade"

Tendo em conta as possibilidades previamente analisadas, e procurando atribuir uma classificação de cor de acordo com o impacto nos direitos, liberdades e garantias dos titulares, em que se atribui a cor verde para “baixo risco”, amarelo para “médio risco”, laranja para “alto risco” e vermelho para “muito alto risco”, conclui-se a seguinte tabela de referência:

Dimensões	Propriedades	Nível de Risco			
		Baixo	Médio	Alto	Máximo
Severidade	Dados pessoais envolvidos	1	2	3	4
	Facilidade de correlação	0,25	0,5	0,75	1
	Fundamento de licitude	1	2		4
	Danos e benefícios para o titular	1	1,5	2	4

Tabela 25 - Valores de referência de quantificação da "severidade"

Procurando avaliar o impacto da classificação das cores no risco, elaborou-se com recurso a uma avaliação completa de todos os cenários possíveis de resposta às variáveis referidas, tendo sido obtido o seguinte resultado de curvas de distribuição:

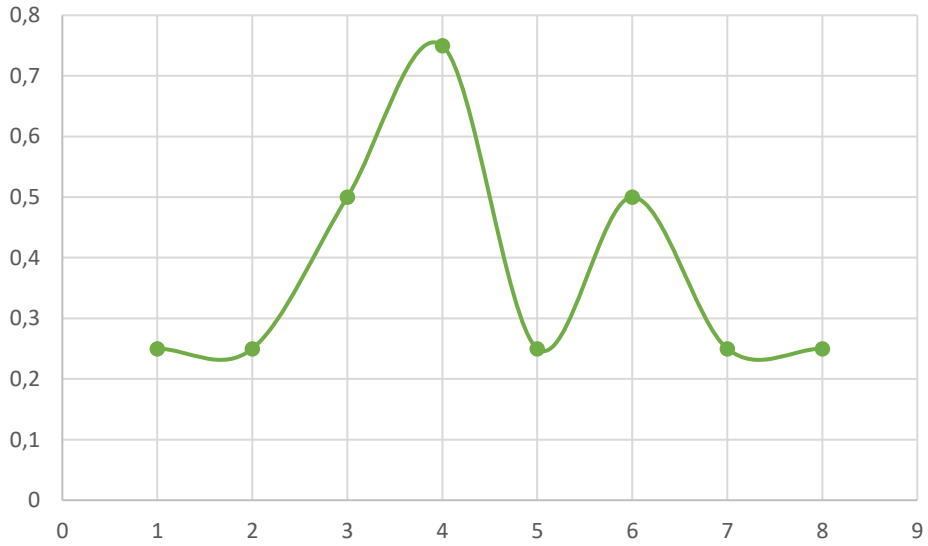


Figura 44 - Curva de dispersão de baixo risco na severidade

Das possíveis combinações de respostas que produzem cenários estritamente enquadráveis em “*baixo risco*”, verifica-se que as opções encontram-se dentro do intervalo de resultados: [0.25 ; 0.75].

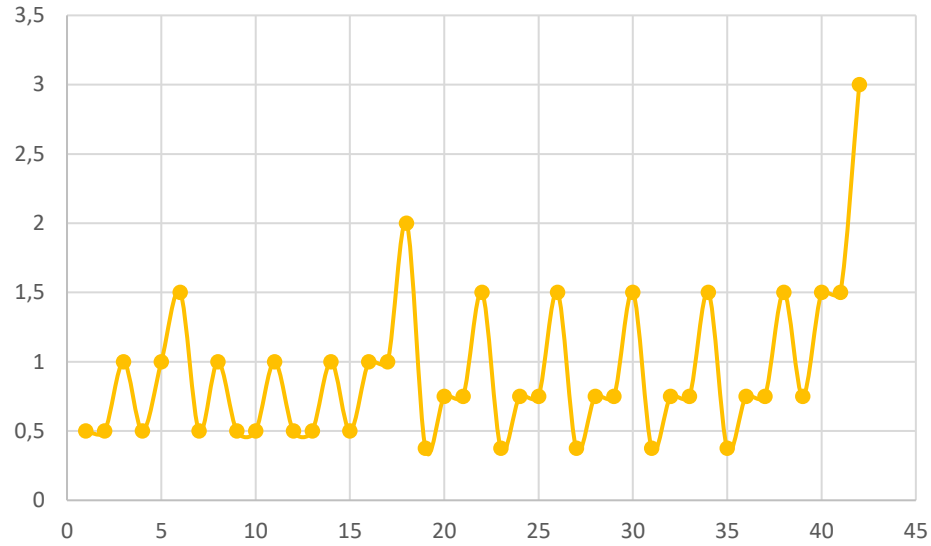


Figura 45 - Curva de dispersão de médio risco na severidade

As possíveis combinações de respostas que produzem cenários estritamente enquadráveis em "*médio risco*", verifica-se que as opções encontram-se dentro do intervalo de resultados: [0.375 ; 3].

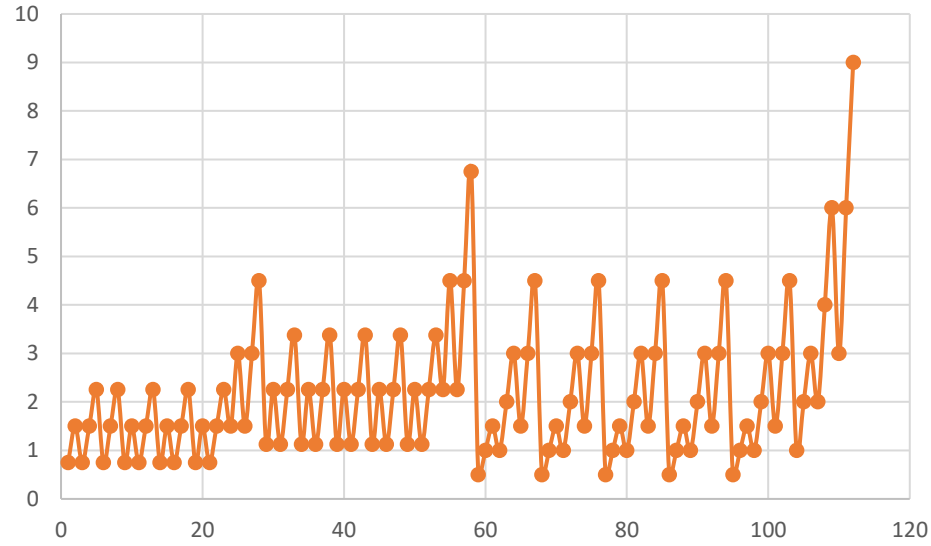


Figura 46 - Curva de dispersão de alto risco na severidade

Quanto às possíveis combinações de respostas que produzem cenários estritamente enquadráveis em "*alto risco*", verifica-se que as opções encontram-se dentro do intervalo de resultados: [0.5 ; 9].

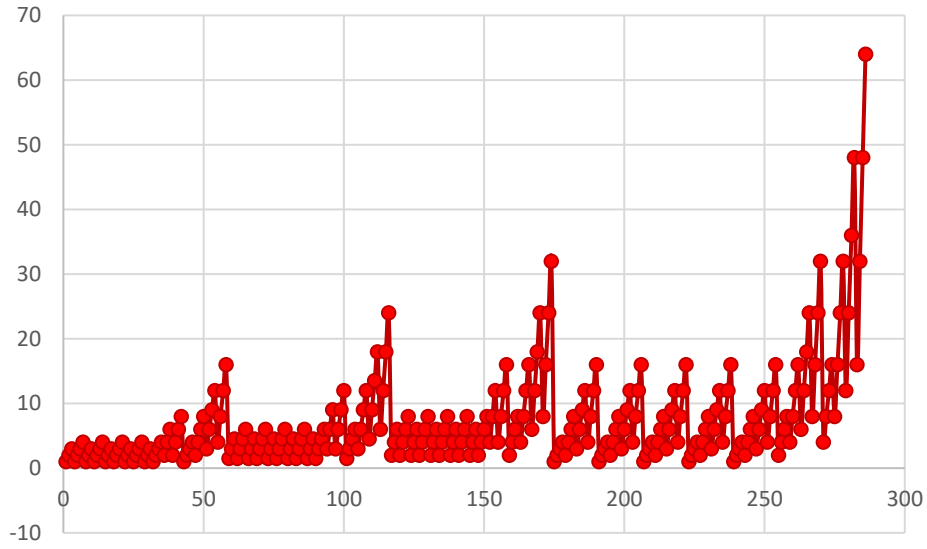


Figura 47 - Curva de dispersão de muito alto risco na severidade

Por fim, as combinações possíveis de respostas que produzem cenários estritamente enquadráveis em "*muito alto risco*", verifica-se que as opções encontram-se dentro do intervalo de resultados: [1 ; 64].

Verificam-se deste modo as seguintes conclusões:

i. De acordo com as curvas de dispersão obtidas por simulação, conclui-se que o volume de combinações possíveis aumenta proporcionalmente ao risco para o titular, conforme seria expectável concluir.

ii. Uma vez que os resultados dos diferentes cenários possíveis de cálculo são de resultados dispares, força à necessidade de consulta das tabelas de referência para aferição do risco para o titular, em função da cor atribuída.

- Avaliação da verosimilhança

  Tendo em conta o risco de segurança dos dados e a superfície de exposição, permite avaliar a probabilidade de materialização do(s) evento(s), pela facilidade/propensão da ocorrência. Deste modo, são considerados os fatores inerentes ao risco de segurança de informação, nomeadamente o seu potencial de; acesso não autorizado, modificação indesejada e perda de dados. Adicionalmente, será considerada a superfície de exposição.

A avaliação é obtida pela seguinte formula:

$$V_{er} = S_i + S_{xp} \Leftrightarrow V_{er} = [\, C + I + D + E \,] + [\, T + M \,]$$

V_{er} – Verosimilhança
S_i – Segurança de informação
S_{xp} – Superfície de exposição
C – Confidencialidade
I – Integridade
D – Disponibilidade
E – Exposição
T – Trânsfuga
M – Motivação

Sendo a segurança de informação um fator importante a calcular, nomeadamente a afetação ao nível das suas propriedades (confidencialidade, integridade e disponibilidade), propõe-se a avaliação conforme previsto na seguinte tabela:

Propriedade	Ameaça associada	Valor	Justificação
Confidencialidade	Acesso ilegítimo	0	Ausência de evidencias que os dados envolvidos afetem a confidencialidade.
		+0,25	Dados disponibilizados a um restrito número de destinatários conhecidos.
		+0,5	Dados disponibilizados a um número desconhecido de destinatários.
+ (valor transita e é adicionado ao seguinte)			
Integridade	Modificação indesejada	0	Dados alterados, mas sem qualquer utilização incorreta ou ilegalmente identificada.
		+0,25	Dados alterados e potencialmente utilizados de forma incorreta ou ilegal, com possibilidade de recuperação.
		+0,5	Dados alterados e potencialmente utilizados de forma incorreta ou ilegal, sem possibilidades de recuperação.
+ (valor transita e é adicionado ao seguinte)			
Disponibilidade	Perda de dados	0	Dados sujeitos a uma indisponibilidade quase impercetível, e recuperados sem qualquer dificuldade.

		+0,25	Dados sujeitos à indisponibilidade temporária.
		+0,5	Dados sujeitos à indisponibilidade total, não podendo ser recuperados ou controlados.

Tabela 26 – Avaliação da Segurança de Informação com base na ENISA

Finalmente, quanto à superfície de exposição, esta contempla os fatores de exposição, trânsfuga e motivação, nos seguintes termos:

Dimensão	Valor	Justificação
Exposição	0	Sem exposição ou muito reduzida, podendo o tratamento ser realizado por máquinas/robots.
	+0,25	Visibilidade/acesso muito restrito a utilizadores conhecidos.
	+0,5	Visível/acessível a elevado número de utilizadores (Internet).
Trânsfuga	0	Transferência para países com acordos de tratamento de dados pessoais.
	+0,25	Transferência para países sem acordos, mas para destinatários confiáveis, com contratos celebrados.
	+0,5	Transferência para países sem acordos, para destinatários de dimensão/representação internacional, com propensão a explorar/capitalizar os dados (ex. redes sociais/SEO/…).
Motivação	0	Sujeito a atos não maliciosos
	+0,5	Sujeito a atos maliciosos

Tabela 27 – Identificação das dimensões da superfície de exposição

Consideram-se deste modo identificados os critérios e argumentos de avaliação necessários cálculo da verosimilhança, a qual se conclui ter os resultados compreendidos no seguimento domínio:

$$D_{ver} = [\,0\,;\,3\,]$$

Dentro do referido domínio, encontram-se todas as possíveis combinações de cenários respeitantes às seguintes propriedades e resultados:

Dimensões	Propriedades		Nível de Risco		
			Baixo	Médio	Máximo
Verosimilhança	Segurança de informação	Confidencialidade	Inexpressivo ou residual	Disponibilizado a restrito grupo conhecido	Disponibilizado a número desconhecido
		Integridade	Sem utilização incorreta ou ilegal	Alterados e/ou utilizados de forma incorreta ou ilegal, mas recuperáveis	Alterados e/ou utilizados de forma incorreta ou ilegal, mas irrecuperáveis
		Disponibilidade	Impercetível e recuperados sem dificuldade	Perceptivel indisponibilidade temporária	Indisponibilidade permanente sem recuperação
	Superfície de exposição	Exposição	Sem exposição ou imperceptível	Visibilidade/acesso a grupo conhecido	Grande visibilidade ou acesso (Internet)
		Trânsfuga	Transferencia para países com acordo	Transferência para países sem acordos, mas confiáveis	Transferência para países sem acordos ou entidades internacionais com propensão a explorar dados
		Motivação	Ato(s) não maliciosos		Ato(s) malicioso(s)

Tabela 28 - Valores de referência da qualificação da "verosimilhança"

Tendo em conta os valores previamente analisados, e procurando atribuir uma classificação de cor de acordo com o impacto nos direitos, liberdades e garantias dos titulares, em que se atribui a cor verde para “baixo risco”, amarelo para “médio risco”, laranja para “alto risco” e vermelho para “muito alto risco”, relativamente ao risco de tratamento e segurança dos dados.

Para uma análise simultânea e profícua aos direitos e liberdades dos titulares, conclui-se a seguinte tabela de referência:

Dimensões	Propriedades		Nível de Risco		
			Baixo	Médio	Máximo
Verosimilhança	Segurança de informação	Confidencialidade	0	0,25	0,5
		Integridade	0	0,25	0,5
		Disponibilidade	0	0,25	0,5
	Superfície de exposição	Exposição	0	0,25	0,5
		Trânsfuga	0	0,25	0,5
		Motivação	0		0,5

Figura 48 - Valores de referência da "verosimilhança"

Procurando avaliar o impacto da classificação das cores no risco, elaborou-se com recurso a uma avaliação completa de todas as possibilidades de resposta às variáveis referidas, a seguinte análise de curvas de distribuição:

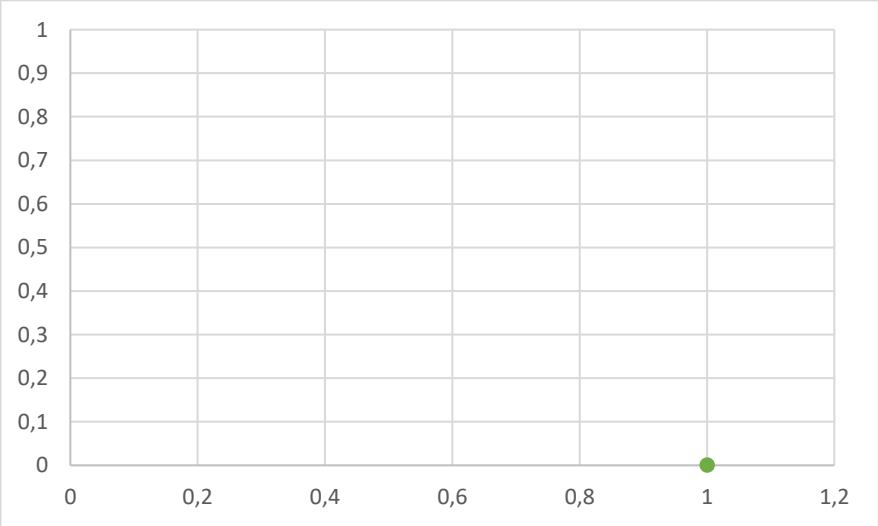


Figura 49 - Curva de dispersão de baixo risco na verosimilhança

Existe uma única possibilidade de combinação de respostas, que produz o cenário estritamente enquadrável em "*baixo risco*", verifica-se assim que a opção encontra-se no resultados: [0].

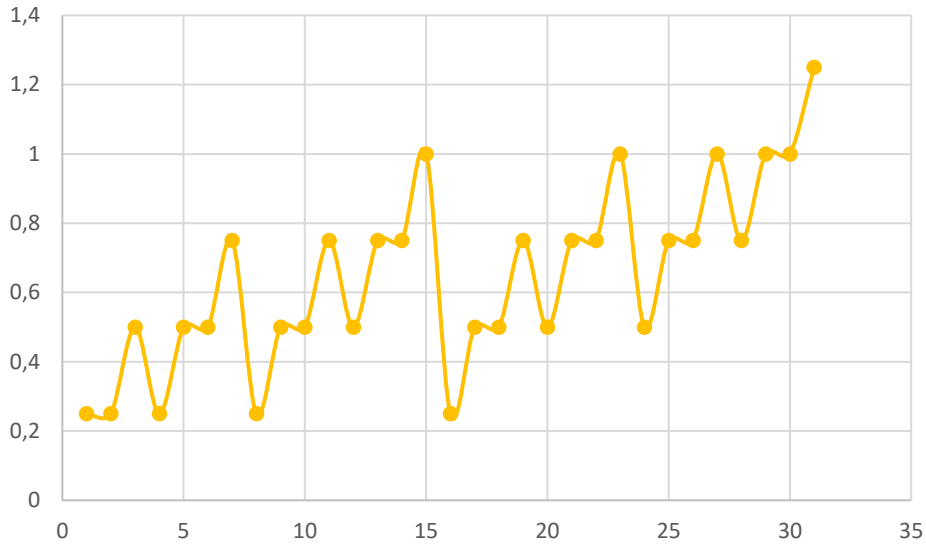


Figura 50 - Curva de dispersão de médio risco na verosimilhança

Das possíveis combinações de respostas que produzem cenários estritamente enquadráveis em "*médio risco*", verifica-se que as opções encontram-se dentro do intervalo de resultados: [0.25 ; 1.25].

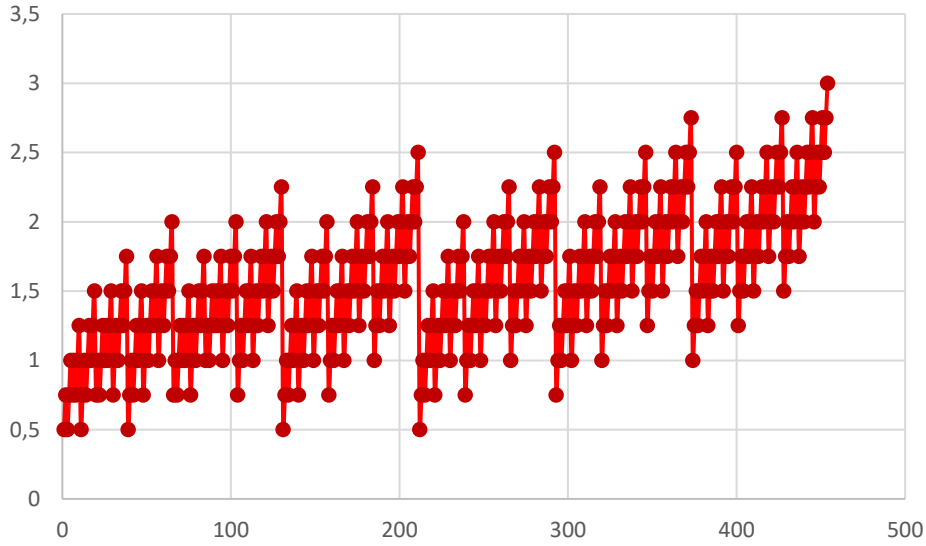


Figura 51 - Curva de dispersão de muito alto risco na verosimilhança

Por fim, das combinações possíveis de respostas que produzem cenários estritamente enquadráveis em "*muito alto risco*", verifica-se que as opções encontram-se dentro do intervalo de resultados: [0.5 ; 3].

<u>Verificam-se deste modo as seguintes conclusões:</u>

i. De acordo com as curvas de dispersão obtidas por simulação, conclui-se que **o volume de combinações possíveis aumenta proporcionalmente ao risco** para o titular, conforme seria expectável concluir.

ii. Uma vez que os resultados dos diferentes cenários possíveis de cálculo são de resultados dispares, força à necessidade de consulta das tabelas de referência para aferição do risco para o titular, em função da cor atribuída.

- <u>Determinação do nível de risco</u>

Para findar o presente subprocesso, restará determinar o nível de risco com base nas avaliações anteriores, designadamente quanto à severidade e verosimilhança. Deste modo, conclui-se que a determinação é obtida pela seguinte função:

$$R = Sv + V_{er} \Leftrightarrow R = Sv + (S_i + S_{xp}) \Leftrightarrow$$

$$R = (D * F_c * F_l * D\text{^}B) + (C + I + D + E) + (T + M)$$

Sv – Severidade
V_{er} – Verosimilhança
D – Dados pessoais envolvidos
F_c – Facilidade de correlação
F_l – Fundamento de licitude
$D\text{^}B$ – Danos e benefícios para o titular
S_i – Segurança de informação
S_{xp} – Superfície de exposição
C – Confidencialidade
I – Integridade
D – Disponibilidade
E – Exposição
T – Trânsfuga
M – Motivação

Deverão ser tidos em conta os critérios previamente definidos para cada uma das variáveis da função, quer ao nível da definição das variáveis, quer ao nível dos valores de referência especificados.

Quanto à operacionalização do cálculo, esta poderá ser obtida em diferentes modos, seja por recurso a folha de *excel*, ou software específico desenvolvido em conformidade com o presente modelo.

3.3.3 Avaliação do risco

O subprocesso de avaliação do risco, tem em conta critérios inerentes à forma como são afetados direitos, liberdades e garantias fundamentais dos titulares de dados.

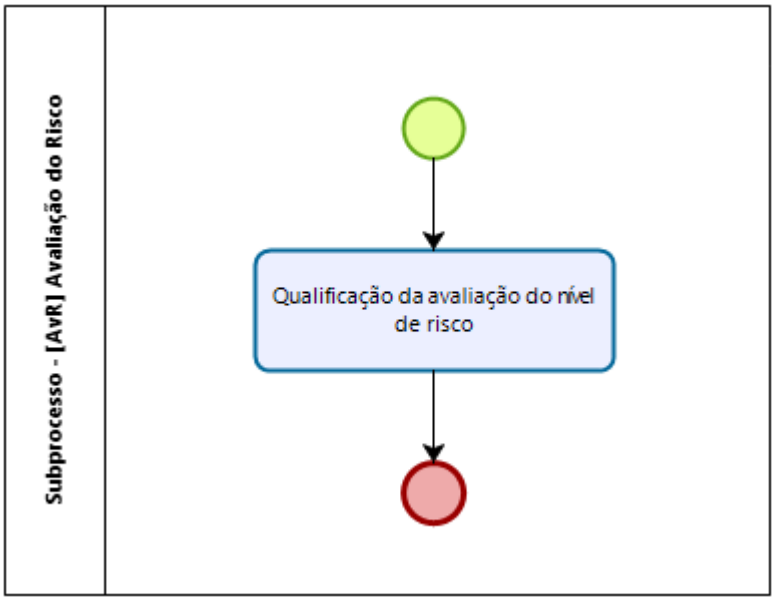


Figura 52 - Processo de avaliação de risco

- Qualificação da avaliação do nível de risco

  Sendo a única atividade prevista no subprocesso que se considera último, foi desenhada uma matriz de referência, que visa qualificar os valores definidos no subprocesso anterior, em matéria de risco para o titular de dados.

  Importa também clarificar, que **a qualificação do risco pressupõe na soma das propriedades, que impera o risco mais elevado**, independentemente do valor em causa.

  Este facto decorre das simulações previamente realizadas, onde se verifica uma dispersão de amplitude não correlacionável ao valor de risco em causa, de modo que deverá prevalecer a qualificação do risco em detrimento do seu valor atribuído.

  Considera-se deste modo o seguinte exemplo:

  P1 (**Risco Alto**) + P2 (Risco Médio) + P3 (Risco Baixo) = **Risco Alto**

Ao qualificar os possíveis resultados de cada variável, foi possível atribuir a seguinte qualificação geral:

Dimensões	Propriedades		Nível de Risco		
			Baixo	Médio	Máximo
Severidade	Dados pessoais envolvidos		Funcionais	Preferências	Sensíveis
	Facilidade de correlação		Negligenciável	Limitado	Máximo
	Fundamento de licitude		Consentimento	Interesses legítimos	Inexistência de fundamento
			Contrato		
			Obrigação jurídica		
			Interesses vitais		
			Interesse público ou autoridade pública		
	Danos e benefícios para o titular		Descurável	Limitado	Irreversível
Verosimilhança	Segurança de informação	Confidencialidade	Inexpressivo ou residual	Disponibilizado a restrito grupo conhecido	Disponibilizado a número desconhecido
		Integridade	Sem utilização incorreta ou ilegal	Alterados e/ou utilizados de forma incorreta ou ilegal, mas recuperáveis	Alterados e/ou utilizados de forma incorreta ou ilegal, mas irrecuperáveis
		Disponibilidade	Impercetível e recuperados sem dificuldade	Perceptivel indisponibilidade temporária	Indisponibilidade permanente sem recuperação
	Superfície de exposição	Exposição	Sem exposição ou imperceptível	Visibilidade/acesso a grupo conhecido	Grande visibilidade ou acesso (Internet)
		Trânsfuga	Transferencia para países com acordo	Transferência para países sem acordos, mas confiáveis	Transferência para países sem acordos ou entidades internacionais com propensão a explorar dados
		Motivação	Ato(s) não maliciosos		Ato(s) malicioso(s)

Tabela 29 - Matriz de referência de qualificação geral do risco

De acordo com a descrição previamente apresentada sob forma de tabela, consideram-se os seguintes valores correspondentes:

Dimensões		Propriedades	Nível de Risco			
			Baixo	Médio	Alto	Máximo
Severidade		Dados pessoais envolvidos	1	2	3	4
		Facilidade de correlação	0,25	0,5	0,75	1
		Fundamento de licitude	1	2		4
		Danos e benefícios para o titular	1	1,5	2	4
Verosimilhança	Segurança de informação	Confidencialidade	0	0,25		0,5
		Integridade	0	0,25		0,5
		Disponibilidade	0	0,25		0,5
	Superfície de exposição	Exposição	0	0,25		0,5
		Trânsfuga	0	0,25		0,5
		Motivação	0			0,5

Tabela 30 - Matriz de referência de quantificação geral do risco

Tendo sido possível avaliar o risco, com base nos critérios anteriormente descritos nas tabelas 30 e 31, torna-se, pois, necessário a aplicação de critérios adicionais que permitam priorizar os riscos, sempre que necessário. Esta necessidade poderá decorrer de vários fatores, designadamente da limitação de recursos humanos, técnicos, orçamentais ou outros, de modo a que após a identificação por tipo de risco (baixo, médio ou alto), possa ser aplicada uma ordenação, tendo em conta o seu valor quantitativo de risco.

Cenário	Severidade	Verosimilhança	Risco	Prioridade
A	2	2	4	2
B	0,25	0,75	1	5
C	0,75	0,5	1,25	3
D	2	2	4	1
E	0,5	0,25	0,75	4
F	0,25	0	0,25	6

Tabela 31 - Matriz exemplificativa de priorização do risco

Conforme resulta claro da tabela exemplificativa anterior, a prioridade terá em consideração os seguintes critérios:

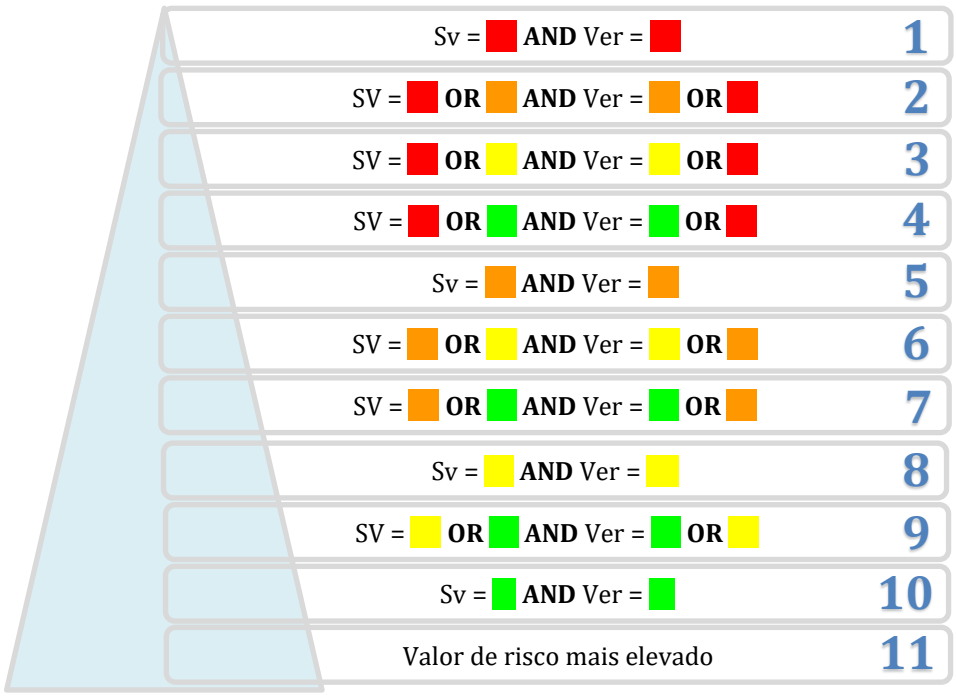


Figura 53 - Escala de critérios de priorização

Tendo sido simulados todos os casos a considerar, foram especificamente analisados os que podem ser considerados como elegíveis a notificação à autoridade de controlo, nos termos do artigo 33.º, bem como os elegíveis a comunicação aos titulares de dados visados, de acordo com o artigo 34.º.

Não obstante das obrigações de notificação, importa igualmente recordar que deve ser documentada quaisquer violações de dados pessoais, acompanhada dos fatos relacionados, bem como dos respetivos efeitos e medidas de reparação adotadas, em cumprimento com o n.5 do artigo 33.º.

Considerando que o nº1 do artigo 33.º considera como elegível a notificação à Autoridade de Controlo, as violações de dados pessoais suscetíveis de resultar num risco para os direitos e liberdades das pessoas singulares, o seguinte cenário/simulacro representa a fronteira, a partir da qual se considera a obrigação de notificação à Autoridade:

Propriedade	Opção	Justificação	Valor
Dados pessoais envolvidos	*Preferenciais*	Esta é a opção que surge após os dados "Dados funcionais, simples ou correntes", os quais pela sua natureza, não assumem risco relevante para o titular, havendo nestes uma natureza simples e muito limitada.	2
Facilidade de correlação	*Máximo*	Atendendo a que esta opção é a única que assegura que os dados se relacionam com uma única pessoa singular.	1
Fundamento de licitude	*Interesse legítimo*	O interesse legítimo pode resultar em risco para o titular, não devendo os direitos do responsável pelo tratamento não podem sobrepor aos direitos dos titulares.	2
Danos e benefícios para o titular	*Transponível*	Resulta na opção onde os danos resultantes são consideráveis e dificilmente ultrapassáveis. As opções anteriores assumem-se como facilmente ultrapassáveis ou negligenciáveis.	2
		Avaliação da severidade	8
Confidencialidade ou Integridade ou Disponibilidade	*"Disponibilizado a restrito grupo conhecido" ou "Alterados e/ou utilizados de forma incorreta ou ilegal, mas recuperáveis" ou "Percetível indisponibilidade temporária"*	Para que exista risco, terá de existir numa ou mais das dimensões desta propriedade, um incidente com relevância, pois as opções inferiores resultam em estados recuperáveis e limitados.	0,25
Exposição	*"Visibilidade/acesso a grupo conhecido"*	A exposição assume dimensão que resulta em risco, as anteriores consideram limitação ou ausência de exposição.	0,25
		Avaliação da verosimilhança	0,5
		Valor Total Final	**8,5**

Tabela 32 - Simulação fronteira para reporte à Autoridade de Controlo

Resulta claro que qualquer **risco igual ou superior a 8.5**, considera a **necessidade de notificação à Autoridade de Controlo (CNPD)**.

Procurando igualmente analisar o nível que exige o cumprimento de comunicação ao(s) titular(res), nos termos do artigo 34.º, procedeu-se à seguinte simulação:

Propriedade	Opção	Justificação	Valor
Dados pessoais envolvidos	*Solvabilidade*	Referindo o n.1 do artigo 34.º "um elevado risco", este resulta a partir desta opção (inclusive), uma vez que os anteriores não cumprem com o critério "elevado".	3
Facilidade de correlação	*Máximo*	Atendendo a que esta opção é a única que assegura que os dados se relacionam com uma única pessoa singular.	1
Fundamento de licitude	*Inexistência de fundamento*	Não existindo fundamento, significa que o tratamento de dados não possui licitude e não é legal.	4
Danos e benefícios para o titular	*Transponível*	Resulta na opção onde os danos resultantes são consideráveis e dificilmente ultrapassáveis. As opções anteriores assumem-se como facilmente ultrapassáveis ou negligenciáveis.	2
		Avaliação da severidade	24
Confidencialidade ou Integridade ou Disponibilidade	*"Disponibilizado a número desconhecido" ou "Alterados e/ou utilizados de forma incorreta ou ilegal, mas irrecuperáveis" ou "Indisponibilidade permanente sem recuperação"*	Para que exista risco, terá de existir numa ou mais das dimensões desta propriedade, um incidente com relevância, pois as opções inferiores resultam em estados recuperáveis e limitados.	0,50
Exposição	*"Visibilidade/acesso a grupo conhecido"*	A exposição assume dimensão que resulta em risco, as anteriores consideram limitação ou ausência de exposição.	0,25
Trânsfuga ou Motivação	*"Transferência para países sem acordos ou entidades internacionais com propensão a explorar dados" ou "Ato(s) malicioso(s)"*	Seja por via de transferência que corporize uma perda de controlo dos dados do titular ou pela motivação maliciosa do ato, resulta em elevado risco.	0,50
		Avaliação da verosimilhança	1,25
		Valor Total Final	**25,25**

Tabela 33 - Simulação fronteira para comunicação aos titulares visados

De acordo com a análise e respetivas justificações, resulta claro que qualquer **risco igual ou superior a 25.25** considera a **necessidade de comunicação aos titulares de dados visados** sem demora injustificada.

Conclui-se deste modo, a seguinte escala de referência:

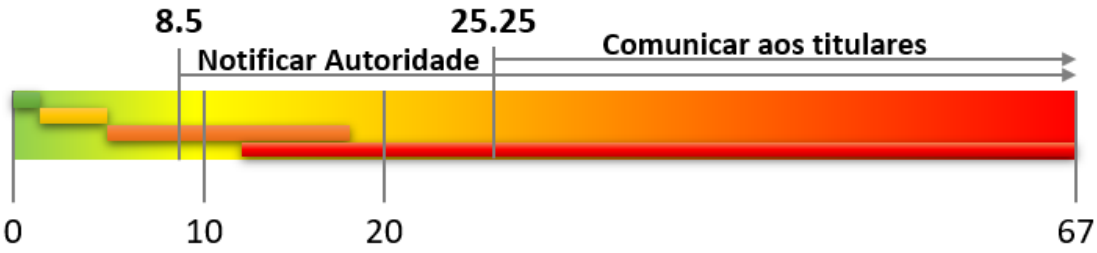


Figura 54 - Escala de referência nas obrigações de notificação

3.4 VALOR DA COMPENSAÇÃO DE DANOS

A proposta de calculo do valor indemnizatório apresentada na tabela abaixo, e que visa o apuramento da compensação pelo dano causado, decorre dos casos de estudo do capítulo 3.4.

Existe, porém, outros cenários de risco que podem servir de objeto do cálculo:

Tipo de dano	Dano concreto	Exemplo de cálculo com base em projeção
Danos morais complementares	Internamento	$x \in Q_+ , \quad 20{,}52 \leq x \leq 30{,}78$ $y = n.x$
	Dano estético	$y = 171x^2 + 174{,}66x + 520{,}33, x \in \mathrm{N}_+ \mid x > 0$
	Quantum doloris	$y = 219{,}86x^2 - 894{,}09x + 762{,}17, x \in \mathrm{N}_+ \mid x > 3$
	Repercussão na vida laboral	▪ Superior a 10P e menor ou igual a 35P $y = -5130x + 30780 , \quad x \in \mathrm{N}_+ \mid x > 0$ ▪ Superior a 35P e inferior ou igual a 70P $y = -12825x + 76950 , \quad x \in \mathrm{N}_+ \mid x > 0$

		▪ Superior a 70P $y = -20520x + 123120\,, \quad x \in \mathrm{N}_+ \mid x > 0$
	Incapacidade Permanente Absoluta (IPA)	$y = 200.000$
Danos em caso de morte e a título de danos morais	Dano moral por perda de feto	▪ Para o 1º filho: $y = -5130x + 12825\,, \quad x \in \mathrm{N}_+ \mid 1 \leq x \leq 2$ ▪ Para o 2º filho ou posterior: $y = -5130x + 17955\,, \quad x \in \mathrm{N}_+ \mid 1 \leq x \leq 2$
	Direito à vida	$y = -10260x + 71820\,, \quad x \in \mathrm{N}_+ \mid 1 \leq x \leq 4$
	Dano moral da própria vítima	$y = 2565x - 684\,, \quad x \in \mathrm{N}_+ \mid 1 \leq x \leq 3$

Tabela 34 - Cálculo exemplificativo de compensação de danos relativos a DLG

4 AVALIAÇÃO

Da presente proposta explanada, resulta claro as seguintes conclusões observáveis:

(I). Tem como foco o risco para os titulares e diferenciando o seu objeto para o negócio, cumpre assim com o RGPD e proporciona um **equilíbrio à falta de consciencialização apontada pelos inquiridos**, representada pela Figura 25;

(II). A proposta **contempla todos os dados assinalados pelos inquiridos** no questionário, enquanto relevantes para avaliação de risco, os quais se encontram descritos exaustivamente na Figura 27;

(III). Proporciona uma avaliação que **não discrimina entre dano material e não-material**, à exceção da aferição indemnizatória para o(s) visado(s), naturalmente, procurando deste modo respeitar a opinião expressa pelos inquiridos, conforme representada na Figura 28;

(IV). Conforme questionado aos inquiridos, relativamente à familiaridade com metodologias e/ou *frameworks* de avaliação de risco, tendo sido apontadas as normas ISO/IEC como familiares para cerca de 92% dos inquiridos, procurou-se estudar uma solução que proporcione **resposta em conformidade com o previsto nas normas ISO/IEC**;

(V). Tendo sido possível verificar a insuficiente disponibilização de informação e recursos sobre riscos RGPD, conforme declarado pelos inquiridos e explanado na Figura 32, foi desde modo desenvolvida uma **proposta completa e autoexplicativa** sobre o tema, que vise proporcionar **soluções de fácil interpretação**, dispensando requisitos exigíveis ao nível de especial literacia neste domínio;

(VI). Quanto à relevância da aferição indemnizatória prévia, tendo 69% dos inquiridos manifestado ser uma medida recomendável, conforme representado pela Figura 34, conclui-se a relevância e utilidade da presente proposta, que, para além da avaliação de risco, permite igualmente responder à **aferição de potencial indemnizatório prévio aos titulares**;

(VII). Com base nos gráficos de dispersão, resultante de simulações, permite concluir que o **volume de combinações possíveis aumenta proporcionalmente ao risco** para o titular, conforme seria expectável concluir;

(VIII). Uma vez que os resultados dos diferentes cenários de risco são dispares, fica assim justificada a **consulta das tabelas de referência, para aferição do risco** para o titular, em função da cor atribuída e não na avaliação quantitativa calculada.

4.1 SIMULAÇÃO DE APLICAÇÃO

A fim de garantir a melhor confiabilidade da proposta deste estudo, foram simulados todos os cenários possíveis de obter, nomeadamente **217.728 casos** possíveis.

Uma vez que o número de casos possíveis é imensamente elevado, procedeu-se a uma análise inicial distinta, da qual resultaram as seguintes conclusões abaixo.

A **severidade é compreendida em 448 casos possíveis**, os quais foram cuidadosamente simulados, tendo sido possível concluir um aumento de possibilidades proporcional ao seu agravamento, conforme representado;

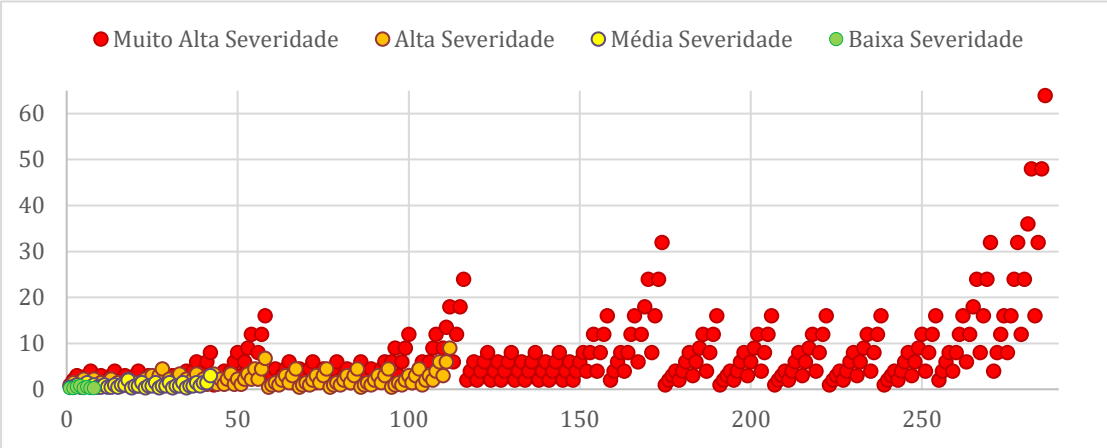


Figura 55 - Gráfico de dispersão geral da Severidade

A **verosimilhança é compreendida em 486 casos possíveis**, tendo sido igualmente verificado um comportamento semelhante do ponto de vista de tendência, agravando proporcionalmente ao aumento do número de possibilidades.

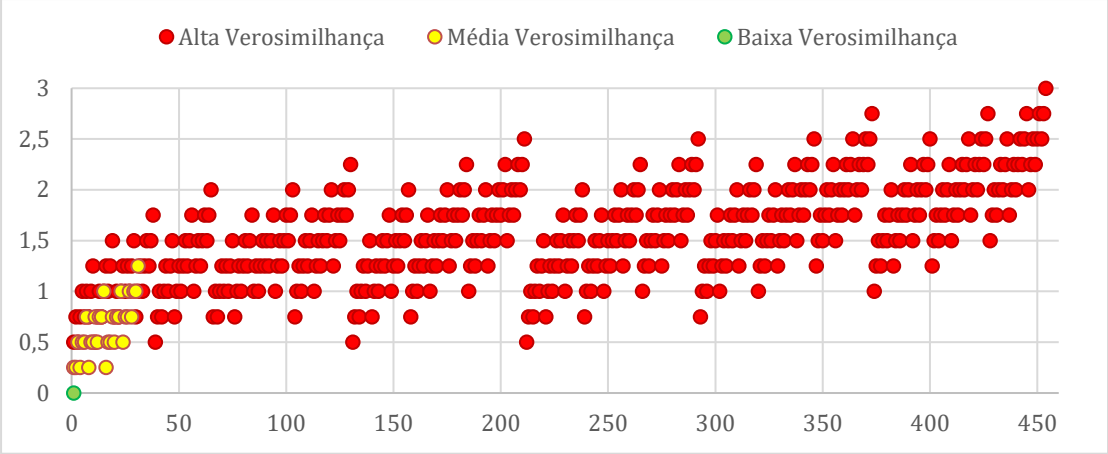
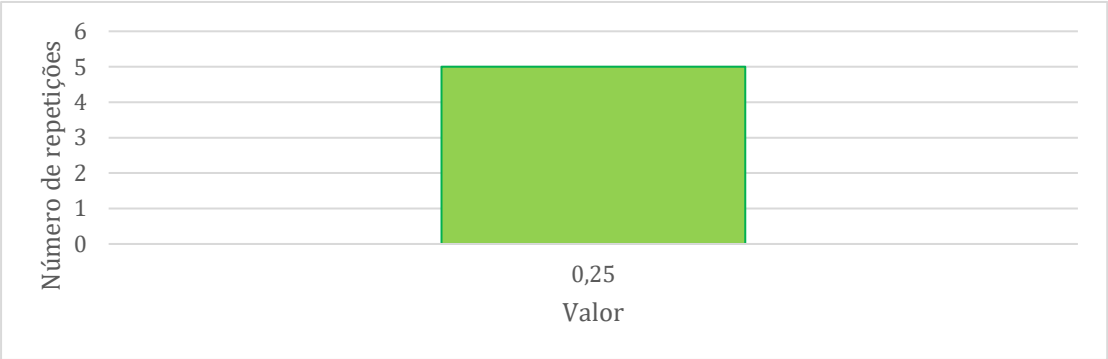


Figura 56 - Gráfico de dispersão geral da Verosimilhança

Da soma da severidade à verosimilhança, foi possível obter a totalidade dos referidos 217.728 casos, os quais sendo objeto de estudo, foram segmentados por nível de risco (baixo, médio e alto).

Risco Baixo

De todos os cenários simulados, procedeu-se à avaliação de todos tendo em conta os critérios de vigorar o risco mais elevado, de modo que só se verificaram 5 cenários, em que o risco é "baixo" – que atendendo ao critério aplicável, exige que todos os argumentos/propriedades tenham o seu valor mínimo possível.



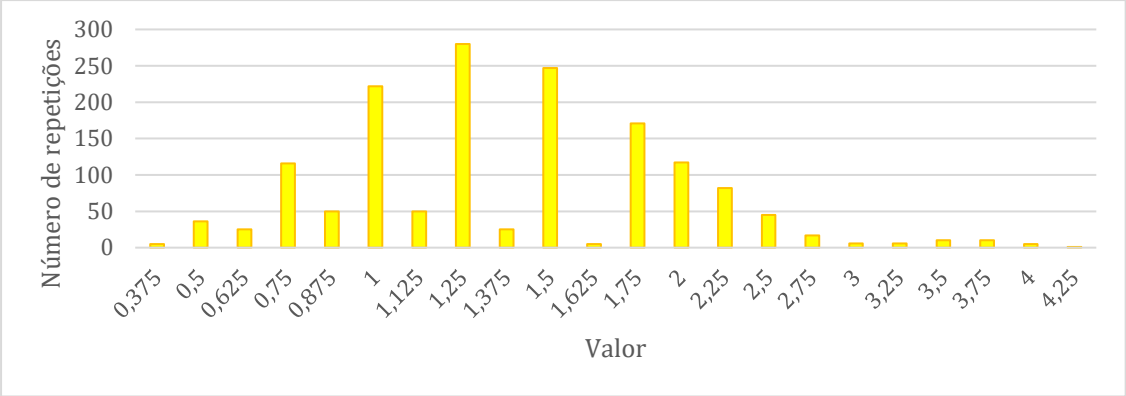
Tendo em consideração o reduzido número de simulações, foi possível obter os seguintes resultados estatísticos:

RISCO BAIXO	
Média	0,25
Mediana	0,25
Moda	0,25
Mínimo	0,25

Máximo	0,25
Soma	1,25
Contagem	**5**

Risco Médio

Tendo em conta que pelo critério aplicável vigora o risco mais elevado, para que os cenários simulados assumam risco médio, os argumentos/propriedades terão de ser compreendidos entre os seus valores "baixo" e "médio", no qual se identificou os seguintes resultados agregados:

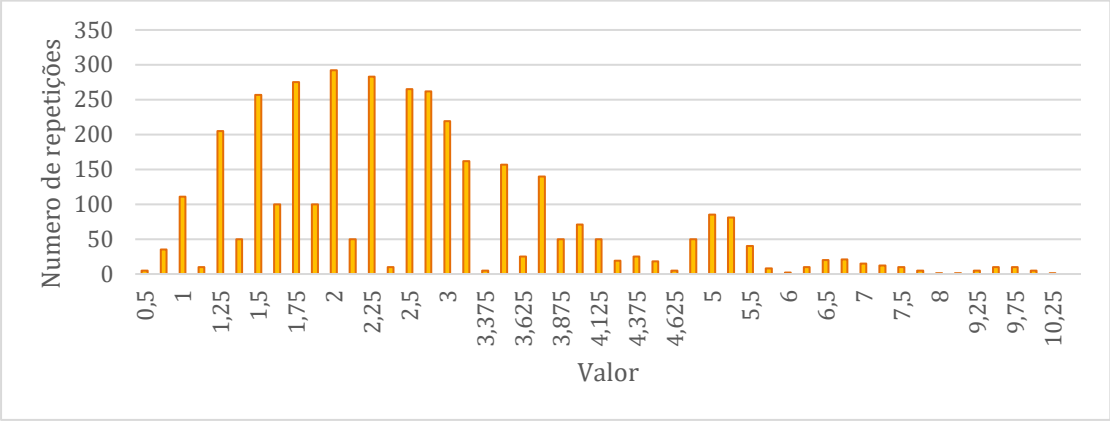


Com base no número de simulações, foi igualmente possível obter a seguinte conclusão estatística:

RISCO MEDIO	
Média	1,449216199
Mediana	1,25
Moda	1,25
Desvio-padrão	0,595044382
Variância da amostra	0,354077817
Curtose	2,584556727
Assimetria	1,249468079
Intervalo	3,875
Mínimo	0,375
Máximo	4,25
Soma	2218,75
Contagem	**1531**

Risco Alto

Do mesmo modo, para que os cenários simulados assumam risco alto, os argumentos/propriedades terão de ser compreendidos entre os seus valores “baixo”, “médio” e “alto”, no qual se identificou os seguintes resultados agregados:

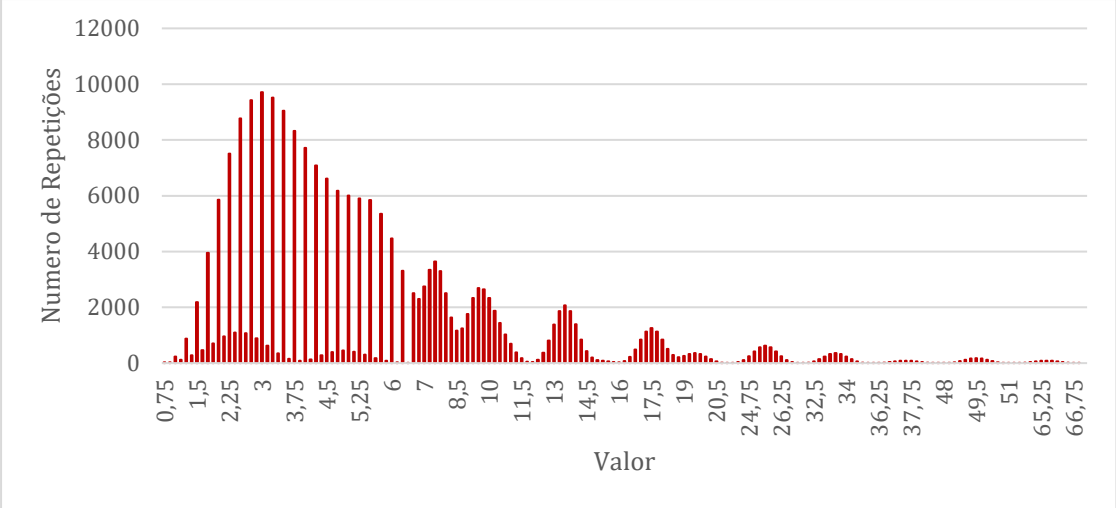


Tendo em conta as simulações, foi possível obter a seguinte conclusão estatística:

RISCO ALTO	
Média	2,766447368
Mediana	2,5
Moda	2
Desvio-padrão	1,450349386
Variância da amostra	2,103513342
Curtose	4,153452061
Assimetria	1,678540427
Intervalo	9,75
Mínimo	0,5
Máximo	10,25
Soma	10092
Contagem	**3648**

Risco Muito Alto

Para que os cenários simulados assumam risco muito alto, os argumentos/propriedades podem ter qualquer valor (“baixo”, “médio”, “alto” ou “muito alto”), de modo que se identificaram os seguintes resultados agregados:



Neste sentido, foi possível obter a seguinte conclusão estatística:

RISCO MUITO ALTO	
Média	6,823551829
Mediana	4,75
Moda	3
Desvio-padrão	6,8287518
Variância da amostra	46,63185115
Curtose	20,84237798
Assimetria	3,798559514
Intervalo	66,25
Mínimo	0,75
Máximo	67
Soma	1450305
Contagem	**212544**

4.2 DEMONSTRAÇÃO #1

Esta demonstração descreve uma situação ocorrida em *Dusseldof* [35], na Alemanha, e é similar a um cenário descrito na recente publicação da EPDB[36], designado por "*CASE No. 03*", permitindo deste modo comparar a avaliação deste caso com as conclusões apresentadas pelo Comité Europeu, aferindo com rigor o nível de harmonização do objeto desta investigação com as conclusões do EDPB.

DESCRIÇÃO: RANSOMWARE SEM EXFILTRAÇÃO NUM HOSPITAL

> *As autoridades confirmaram um ataque de ransomware, que causou a falha nos sistemas informáticos de um Hospital Universitário, inibindo o tratamento*

urgente a uma pessoa de 47 anos, forçando a ser encaminhada para outro hospital, numa cidade a cerca de 32 km de distância, a fim de receber o tratamento necessário. Por motivos de racionalização de custos, o Hospital partilha a mesma infraestrutura, alojada em data-center comum, com base no interesse legítimo – vide considerando (48) RGPD.

O hospital informou que os investigadores descobriram que a fonte do problema resultou de um ataque de hacking, explorando uma vulnerabilidade num "software muito utilizado". Como consequência, os sistemas ficaram inacessíveis gradualmente, no qual o hospital deixou de aceder aos dados; provocando a necessidade de encaminhar os pacientes urgentes para um outro local, assim como adiar todas as operações, mesmo as urgentes.

A polícia comunicou publicamente que, os ataques afetaram gravemente todo o hospital, pondo em perigo todos os doentes. Como resultado, os atacantes forneceram livremente e sem contrapartidas, a chave digital para desencriptar os dados. De acordo com o relatório do Ministro da Justiça, os atacantes, entretanto deixaram de estar contactáveis.

Foi aberta investigação a fim de descobrir a identidade dos atacantes, por suspeita de homicídio involuntário.

AVALIAÇÃO DE MEDIDAS PRÉVIAS E DO RISCO:

A maioria destas violações pode ser evitada, se forem tomadas as medidas de segurança organizacionais, físicas e tecnológicas adequadas.

De realçar a quantidade de dados envolvidos e o elevado número de pessoas afetadas, uma vez que os hospitais tratam grandes quantidades de dados. O tipo de violação, natureza, sensibilidade e volume dos dados pessoais afetados são muito importantes. Mesmo que recuperável, existe um elevado risco para os titulares afetados.

Para melhor compreensão, procede-se ao preenchimento da seguinte tabela:

Proposta de aplicação | Ficha de levantamento de informação
Avaliação da severidade
1. Responsabilidades envolvidas no tratamento:
Responsável autónomo: ☒ Responsável conjunto: ☐ Subcontratante: ☐
2. Dados pessoais envolvidos:
Dados simples/funcionais: ☒ Dados comportamentais ou preferência: ☐ Dados de solvabilidade: ☐ Dados sensíveis: ☒
3. Facilidade de correlação com pessoas singulares:
Negligenciável: ☐ Limitado: ☐ Significativo: ☐ Máximo: ☒
4. Fundamento de licitude:
Consentimento: ☐ Contrato: ☐ Obrigação jurídica: ☐ Interesses vitais ☒ Interesse público ou autoridade pública: ☐ Interesse legítimo: ☒ Inexistente ☐
5. Danos e benefícios para o titular:
Descurável: ☐ Limitado: ☐ Transponível: ☐ Irreversível: ☒
Avaliação da verosimilhança
6. Segurança de Informação
Perda de confidencialidade Inexpressivo ou residual: ☒ Disponibilizado a restrito grupo conhecido: ☐ Disponibilizado a número desconhecido: ☐ Perda de integridade Sem perda, utilização incorreta ou ilegal: ☐ Alterados/utilizados de forma incorreta/ilegal, mas recuperáveis: ☐ Alterados/utilizados de forma incorreta/ilegal, mas irrecuperáveis: ☒ Perda de disponibilidade Impercetível e recuperados sem dificuldade: ☐ Percetível indisponibilidade temporária: ☐ Indisponibilidade permanente sem recuperação: ☒
7. Superfície de exposição
Exposição: Sem exposição ou impercetível: ☒ Visibilidade/acesso a grupo conhecido: ☐ Grande visibilidade ou acesso (Internet): ☐ Trânsfuga: Sem transferência ou realizada para países com acordos: ☒ Transferência para países sem acordos, mas confiáveis: ☐ Transferência para países sem acordos/entidades internacionais: ☐ Motivação: Ato(s) não maliciosos: ☐ Ato(s) malicioso(s): ☒

Para avaliação do risco, foi preenchida a seguinte tabela com base nas informações providenciadas:

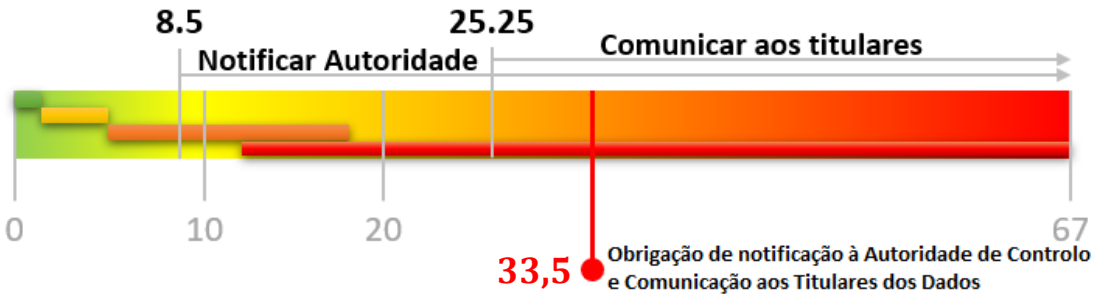
Dimensões		Propriedades	Risco base Nível
Severidade		Dados pessoais envolvidos	4
		Facilidade de correlação	1
		Fundamento de licitude	2
		Danos e benefícios para o titular	4
		Avaliação da severidade	32
Verosimilhança	Segurança de informação	Confidencialidade	0
		Integridade	0,5
		Disponibilidade	0,5
	Superfície de exposição	Exposição	0
		Trânsfuga	0
		Motivação	0,5
		Avaliação da verosimilhança	1,5
		Avaliação final do Risco	**33,5**

Valor indemnizatório de referência para compensação de danos em caso de morte e a título de danos morais aos herdeiros (exemplificativo):

- Direito à vida - vítima de 47 anos [tendo em conta a matriz de referência x=2]

$$y = -10260x + 71820\,, \qquad x \in \mathrm{N}_+ \mid 1 \leq x \leq 4$$

$$y = \mathbf{51.300{,}00}\ \text{€}\ (\mathbf{EUR})$$



Risco de Segurança/Tratamento da Informação	Risco para Direitos, Liberdades e Garantias	Notificação à Autoridade de Controlo	Comunicação aos Titulares de dados	Potencial indemnizatório por titular
Muito Alto	Elevado	☑	☑	€51.300

ANÁLISE DOS RESULTADOS OBTIDOS

Descreve similarmente uma situação ocorrida em *Dusseldof* [35], na Alemanha, a qual veio a promover a morte de um paciente/titular, pela incapacidade de acesso aos dados pessoais, concluindo na inibição do tratamento necessário atempado.

Ainda que não resulte evidente *à priori* a real consequência, os resultados concluem que esta avaliação classificada de "*Risco Muito Alto*", sujeita à obrigação de notificação à Autoridade de Controlo e Comunicado aos Titulares de dados afetados.

A recente publicação da EPDB[36], tem no seu "*CASE Nº 03*" um cenário muito similar, no qual o Comité Europeu apresenta as mesmas conclusões e obrigações, verificando-se deste modo a exatidão do modelo proposto na presente investigação.

É assim considerada como necessária a Notificação à Autoridade de Controlo, pois estão envolvidas categorias especiais de dados, e a recuperação dos mesmos pode demorar algum tempo, resultando em grandes atrasos no tratamento dos pacientes.

A Comunicação aos titulares dos dados é necessária devido ao impacto para os pacientes, especialmente durante a encriptação. Embora os dados relativos a todos os pacientes tratados no hospital durante os últimos anos tenham sido encriptados, foram especialmente afetados os pacientes que estavam programados para serem tratados no hospital durante o tempo em que o sistema informático não funcionou.

4.3 DEMONSTRAÇÃO #2

Esta demonstração descreve similarmente um cenário referido na recente publicação da EPDB[36], designado por "*CASE No. 08*", permitindo deste modo comparar a avaliação e conclusões do mesmo, com as apresentadas pelo Comité Europeu, aferindo deste modo e com rigor técnico, o nível de harmonização do objeto desta investigação com as conclusões do EDPB.

DESCRIÇÃO: EXFILTRAÇÃO DE DADOS COMERCIAIS POR ANTIGO EMPREGADO

> *Ao ter sido notificado e durante o período de pré-aviso, um funcionário de uma empresa, copia todos os dados pessoais dos clientes singulares da base de*

dados da empresa, que está autorizado a aceder no estrito exercício da sua função profissional, a fim de os levar consigo após o términus da relação contractual.

Meses depois, após ter deixado o seu emprego, o ex-colaborador utiliza os dados previamente obtidos, para contactar com os clientes da empresa para quem trabalhou anteriormente, a fim de os atrair para o seu novo negócio.

AVALIAÇÃO DE MEDIDAS PRÉVIAS E DO RISCO:

Tendo em conta que o cumprimento da maioria dos trabalhos de relação com clientes, exige acesso aos dados dos clientes por parte dos funcionários, qualquer limitação de acesso, poderia limitar o desempenho do trabalhador, dificultando a prevenção deste tipo de incidentes.

Todavia, seria de esperar a implementação de políticas de acesso e controlo constante a fim de prevenir este tipo de situações habituais no mercado.

A avaliação do risco requer apreciação do tipo de violação, natureza, sensibilidade e volume dos dados pessoais. Afeta fundamentalmente a confidencialidade, uma vez que a base de dados é mantida como intacta, tendo sido o conteúdo copiado para posterior utilização. Neste caso, não estão envolvidos dados de categoria especial, uma vez que o ex-colaborador apenas pretendia as informações de contacto dos clientes.

Embora o único objetivo do ex-colaborador seria copiar maliciosamente os dados, para promoção comercial subsequente do seu negócio, o responsável pelo tratamento não pode concluir o risco como baixo, uma vez que não dispõe de qualquer tipo de garantia sobre as intenções envolvidas. Deste modo, embora as consequências da violação sejam limitadas à exposição para contactos e divulgação comercial não solicitada, não se pode excluir um tratamento ainda mais abusivo dos dados roubados e com maior risco para os titulares.

Para melhor compreensão, procede-se ao preenchimento da seguinte tabela:

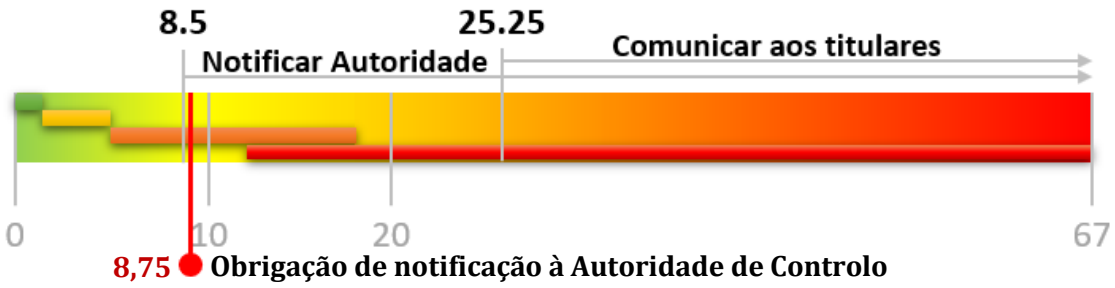
Proposta de aplicação | Ficha de levantamento de informação
Avaliação da severidade
1. Responsabilidades envolvidas no tratamento:
Responsável autónomo: ☒ Responsável conjunto: ☐ Subcontratante: ☐
2. Dados pessoais envolvidos:
Dados simples/funcionais: ☒ Dados comportamentais ou preferência: ☐ Dados de solvabilidade: ☐ Dados sensíveis: ☐
3. Facilidade de correlação com pessoas singulares:
Negligenciável: ☐ Limitado: ☐ Significativo: ☐ Máximo: ☒
4. Fundamento de licitude:
Consentimento: ☐ Contrato: ☐ Obrigação jurídica: ☐ Interesses vitais ☐ Interesse público ou autoridade pública: ☐ Interesse legítimo: ☐ Inexistente ☒
5. Danos e benefícios para o titular:
Descurável: ☐ Limitado: ☐ Transponível: ☐ Irreversível: ☒
Avaliação da verosimilhança
6. Segurança de Informação
Perda de confidencialidade Inexpressivo ou residual: ☐ Disponibilizado a restrito grupo conhecido: ☒ Disponibilizado a número desconhecido: ☐ Perda de integridade Sem perda, utilização incorreta ou ilegal: ☐ Alterados/utilizados de forma incorreta/ilegal, mas recuperáveis: ☐ Alterados/utilizados de forma incorreta/ilegal, mas irrecuperáveis: ☒ Perda de disponibilidade Impercetível e recuperados sem dificuldade: ☐ Percetível indisponibilidade temporária: ☐ Indisponibilidade permanente sem recuperação: ☒
7. Superfície de exposição
Exposição: Sem exposição ou impercetível: ☒ Visibilidade/acesso a grupo conhecido: ☐ Grande visibilidade ou acesso (Internet): ☐ Trânsfuga: Sem transferência ou realizada para países com acordos: ☒ Transferência para países sem acordos, mas confiáveis: ☐ Transferência para países sem acordos/entidades internacionais: ☐ Motivação: Ato(s) não maliciosos: ☐ Ato(s) malicioso(s): ☒

Para avaliação do risco foi deste modo preenchida a seguinte tabela, com base nas informações previamente obtidas/concluídas:

Dimensões		Propriedades	Risco base Nível
Severidade		Dados pessoais envolvidos	1
		Facilidade de correlação	1
		Fundamento de licitude	4
		Danos e benefícios para o titular	2
		Avaliação da severidade	8
Verosimilhança	Segurança de informação	Confidencialidade	0,25
		Integridade	0
		Disponibilidade	0
	Superfície de exposição	Exposição	0
		Trânsfuga	0
		Motivação	0,5
		Avaliação da verosimilhança	0,75
		Avaliação final do Risco	**8,75**

Por forma a aferir o potencial valor indemnizatório a considerar como referência na compensação de danos aos titulares, deverá ser avaliado se houve contactos aos titulares envolvidos – para promoção comercial, e quantas vezes foram os titulares contactados sem o devido consentimento, a fim de aferir o dano para os titulares.

Tendo em conta as informações limitadas do caso apresentado, não se considera existir dados suficientes para aferição do valor.



Risco de Segurança/Tratamento da Informação	Risco para Direitos, Liberdades e Garantias	Notificação à Autoridade de Controlo	Comunicação aos Titulares de dados	Potencial indemnizatório por titular
Muito Alto	Moderado	☑	☐	Por determinar

ANÁLISE DOS RESULTADOS OBTIDOS

A mitigação dos efeitos adversos da violação, pode requerer uma ação legal para evitar que o antigo colaborador conserve, utilize ou divulgue os dados.

Para prevenir semelhantes cenários, o responsável pelo tratamento deve incluir cláusulas contractuais de confidencialidade, a celebrar com os colaboradores.

Não obstante de que a comunicação aos titulares dos dados poderia ter efeitos benéficos de clarificação de responsabilidades, tendo em conta que a violação de dados não resulta num elevado risco para os direitos e liberdades das pessoas singulares, a notificação à Autoridade de Controlo será suficiente.

4.4 DEMONSTRAÇÃO #3

Esta demonstração descreve um cenário referido na recente publicação da EPDB[36], designado por "*CASE No. 06*", permitindo deste modo comparar a avaliação e conclusões com as apresentadas pelo Comité Europeu, aferindo deste modo com rigor técnico, a harmonização desta investigação com as conclusões do EDPB.

DESCRIÇÃO: EXFILTRAÇÃO DE SENHA HASHED A PARTIR DE UM WEBSITE

> *Ao explorar uma vulnerabilidade de SQL Injection um atacante obteve acesso a uma base de dados de um servidor de um website de culinária. Os utilizadores do site só poderiam escolher pseudónimos arbitrários como nomes de utilizador, tendo a utilização de endereços de correio eletrónico sido desencorajada.*
>
> *As palavras-passe armazenadas na base de dados foram cifradas com um algoritmo forte a fim de evitar o seu comprometimento. Os dados afetados por este ataque, foram: as passwords cifradas de 1.200 utilizadores.*
>
> *Por razões de segurança, o responsável pelo tratamento requereu a alteração das passwords aos utilizadores, a fim de evitar a utilização noutros serviços.*

AVALIAÇÃO DE MEDIDAS PRÉVIAS E DO RISCO:

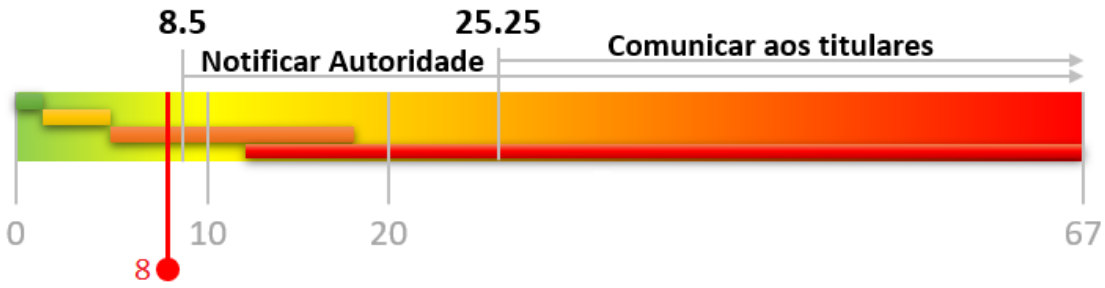
Não obstante da confidencialidade dos dados ter sido comprometida, ao estarem cifrados, não apresenta riscos para os direitos e liberdades das pessoas em causa. De realçar que nenhuma informação de contacto dos titulares foi comprometida, não existindo risco visar os titulares – seja por tentativas de fraude ou contactos de marketing. Não foram igualmente envolvidas categorias especiais de dados pessoais. Para melhor compreensão, procede-se ao preenchimento da seguinte tabela:

Proposta de aplicação | Ficha de levantamento de informação
Avaliação da severidade
8. Responsabilidades envolvidas no tratamento:
Responsável autónomo: ☒ Responsável conjunto: ☐ Subcontratante: ☐
9. Dados pessoais envolvidos:
Dados simples/funcionais: ☒ Dados comportamentais ou preferência: ☐ Dados de solvabilidade: ☐ Dados sensíveis: ☐
10. Facilidade de correlação com pessoas singulares:
Negligenciável: ☐ Limitado: ☐ Significativo: ☒ Máximo: ☐
11. Fundamento de licitude:
Consentimento: ☐ Contrato: ☐ Obrigação jurídica: ☐ Interesses vitais ☐ Interesse público ou autoridade pública: ☐ Interesse legítimo: ☐ Inexistente ☒
12. Danos e benefícios para o titular:
Descurável: ☐ Limitado: ☐ Transponível: ☒ Irreversível: ☐
Avaliação da verosimilhança
13. Segurança de Informação
Perda de confidencialidade Inexpressivo ou residual: ☐ Disponibilizado a restrito grupo conhecido: ☐ Disponibilizado a número desconhecido: ☒ Perda de integridade Sem perda, utilização incorreta ou ilegal: ☒ Alterados/utilizados de forma incorreta/ilegal, mas recuperáveis: ☐ Alterados/utilizados de forma incorreta/ilegal, mas irrecuperáveis: ☐ Perda de disponibilidade Impercetível e recuperados sem dificuldade: ☒ Percetível indisponibilidade temporária: ☐ Indisponibilidade permanente sem recuperação: ☐
14. Superfície de exposição
Exposição: Sem exposição ou impercetível: ☐ Visibilidade/acesso a grupo conhecido: ☐ Grande visibilidade ou acesso (Internet): ☒ Trânsfuga:

Sem transferência ou realizada para países com acordos: ☐
Transferência para países sem acordos, mas confiáveis: ☐
Transferência para países sem acordos/entidades internacionais: ☒
Motivação:
Ato(s) não maliciosos: ☐
Ato(s) malicioso(s): ☒

Para avaliação do risco, foi preenchida a seguinte tabela com base nas informações providenciadas:

Dimensões		Propriedades	Risco base Nível
Severidade		Dados pessoais envolvidos	1
		Facilidade de correlação	0,75
		Fundamento de licitude	4
		Danos e benefícios para o titular	2
		Avaliação da severidade	6
Verosimilhança	Segurança de informação	Confidencialidade	0,5
		Integridade	0
		Disponibilidade	0
	Superfície de exposição	Exposição	0,5
		Trânsfuga	0,5
		Motivação	0,5
		Avaliação da verosimilhança	2
		Avaliação final do Risco	8



Risco de Segurança/Tratamento da Informação	Risco para Direitos, Liberdades e Garantias	Notificação à Autoridade de Controlo	Comunicação aos Titulares de dados	Potencial indemnizatório por titular
Muito Alto	Inexistente	☐	☐	Não aplicável

ANÁLISE DOS RESULTADOS OBTIDOS

Não obstante de poder ser entendido como uma boa prática a comunicação aos titulares dos dados, a fim de que estes tomem as medidas necessárias para evitar mais danos decorrentes da violação, alterando a sua palavra-passe, neste caso a notificação não era obrigatória.

O responsável pelo tratamento deve naturalmente corrigir a(s) vulnerabilidade(s) e implementar medidas de segurança para evitar incidentes semelhantes.

Considera-se, todavia, que esta situação não carece de notificação à Autoridade de Controlo, porquanto não constitui risco para os titulares uma vez que as passwords estão adequadamente cifradas e os dados minimizados.

4.5 DEMONSTRAÇÃO #4

Porquanto as demonstrações anteriores referem violações de dados pessoais, não obstante da sua importância para a avaliação pretendida, procurou-se igualmente diversificar a sua aplicabilidade, ao procurar demonstrar com uma Avaliação de Impacto sobre a Proteção de Dados Pessoais (AIPD/DPIA).

DESCRIÇÃO DO CASO:

No seguimento da intenção de realizar uma campanha de marketing muito oportuna, foi submetido à consideração o seguinte pedido de AIPD/DPIA:

Formulário de Avaliação de Impacto da Proteção de Dados
Informação geral
Finalidade de tratamento no âmbito da análise
Campanha de marketing realizada entre janeiro e abril, promovendo o serviço de entrega de produtos em casa, que sejam oportunos no momento atual (COVID19).
Dados, processos e ativos
Dados pessoais tratados
Dados de identificação e contato (Nome, Telefone e email).
Ciclo de vida dos dados e processos inerentes
Processo web que permite ao titular gerir a qualquer momento os seus dados pessoais.
Ativos de informação utilizados na finalidade de tratamento
Acesso publicado para a Internet, pelo ServidorX e ServidorY, em balanceamento.
Proporcionalidade e necessidade
Natureza e qualidade da finalidade de tratamento

A finalidade do tratamento é específica, explicita e legítima, na medida que é fundamentada no consentimento explicito do titular, obtido antes do tratamento e com a devida informação.
Princípio da minimização
Os dados de identificação solicitados são adequados, relevantes e limitados (minimizados).
Atualização e fidedignidade dos dados
Pressupõe-se criação de rotina para solicitar confirmação/atualização periódica dos dados.
Prazo da conservação dos dados
Até à revogação do consentimento.
Controlos e direitos dos titulares de dados
Informação sobre o tratamento
É prestada a nota informativa aos titulares, providenciada logo no início da recolha.
Direitos
Por intermédio da nota informativa, havendo essas opções na área privada de cliente.
Transferência de dados para fora da União Europeia
Não existirá fluxos transfronteiriços ou envio para organizações internacionais.
Medidas planeadas ou existentes
Contratos
Instrumentos contractuais que regulam a relação entre colaboradores que recolhem os dados junto dos titulares, com clausulas de confidencialidade e regras deontológicas.
Encriptação
Fluxos de comunicação cifrados em AES256, bem como no armazenamento dos dados.
Segregação de acessos
Com recurso a perfilagem.
Políticas
Conjunto de políticas devidamente definidas, aprovadas, implementadas e publicadas.

Tendo por base o formulário anterior, é, pois, possível elaborar a seguinte avaliação:

Dimensões	Propriedades		Nivel
Severidade	Dados pessoais envolvidos		1
	Facilidade de correlação		1
	Fundamento de licitude		1
	Danos e benefícios para o titular		1
	Avaliação da severidade		1
Verosimilhança	Segurança de informação	Confidencialidade	0
		Integridade	0
		Disponibilidade	0
	Superfície de exposição	Exposição	0,5
		Trânsfuga	0
		Motivação	0
	Avaliação da verosimilhança		0,5
	Avaliação final do Risco		1,5

Risco de Segurança/Tratamento da Informação	Risco para Direitos, Liberdades e Garantias	Requer consulta prévia à Autoridade de Controlo	Requer consulta aos Titulares de dados ou seus representantes	Potencial indemnizatório por titular
Muito Alto	Inexistente	☐	☐	Não aplicável

Avaliação dos resultados obtidos

Apesar do potencial de risco para a segurança/tratamento da informação (cor vermelha), conclui-se a inexistência/baixo risco para os Direitos e Liberdades do(s) titular(es) de dados (valor final do risco), tendo em conta a licitude e demais cumprimentos ao nível do tratamento.

A título de avaliação, realizou-se a simulação deste mesmo caso no PIA da CNIL, procurando comparar os resultados, o software não é claro quanto ao risco para os direitos, liberdade e garantias dos pessoais singulares, ou do potencial indemnizatório envolvido no tratamento.

Ainda assim, consideram-se bastante satisfatória as suas conclusões, tendo em conta o cumprimento da minimização, fundamento de licitude, e demais obrigações em conformidade com o RGPD e demais legislação aplicável.

5 CONCLUSÃO

5.1 PRINCIPAIS CONTRIBUIÇÕES

Tendo em conta a falta de orientação específica sobre gestão de risco na proteção de dados pessoais, verificou-se a necessidade de investigar a elaboração de um processo de avaliação de risco, em conformidade com o RGPD, que inclua a possibilidade de calcular o risco para os titulares e se possível, o valor indemnizatório potencial a pagar aos titulares decorrentes de um tratamento com risco assinalável.

Conforme proposto com esta investigação, foi possível elaboração uma proposta que visa harmonizar a avaliação de risco em conformidade com o RGPD, abordando de forma objetiva as dimensões legalmente relevantes, proporcionando um processo detalhado de avaliação tendo como amago os direitos e liberdades do(s) titular(es). Não obstante, cumpre igualmente quanto ao cálculo do risco e à orientação do potencial valor indemnizatório ao titular.

Ora, tendo em conta a especificidade e a complexidade da presente tese, a metodologia adotada foi o DSRM, o qual foi estruturada em 6 diferentes fases:

1. Identificação do Problema e Motivação; nomeadamente a falta de orientação quanto ao processo de avaliação de risco no tratamento dos dados pessoais;
2. Definição dos Objetivos para a Solução; ao procurar proporcionar um processo de avaliação de risco em conformidade com a legislação de proteção de dados pessoais;
3. Desenho e Implementação; procurando elaborar um processo de gestão de risco em conformidade com o RGPD, utilizando formula de cálculo de risco e do valor indemnizatório potencial a favor do titular de dados visado;
4. Demonstração; aquando se utilizou o modelo em casos de aplicação prática comum no mercado;
5. Avaliação; análise da representatividade e valor possíveis de obter na aplicação da fórmula de cálculo, em todos os cenários possíveis de obter;

6. Comunicação; concretizando na presente dissertação, e potenciando futuras publicação de artigos e desenvolvimento de aplicações que autonomizem e simplifiquem a aplicação da presente investigação.

Conclui-se que o presente estudo cumpriu com os objetivos previamente propostos, resultando claro as seguintes conclusões observáveis da proposta desta investigação:

- ✓ Tem como foco o risco para os titulares, cumprindo assim com o previsto no RGPD, proporcionando um **equilíbrio à falta de consciencialização** apontada pelos especialistas inquiridos;
- ✓ Contempla os **dados e propriedades relevantes** para avaliação de risco;
- ✓ N**ão discrimina entre dano material e não-material**, à exceção da aferição indemnizatória para o(s) visado(s), naturalmente, procurando deste modo respeitar a opinião expressa dos inquiridos;
- ✓ Apresenta uma solução em **conformidade com o previsto nas normas ISO/IEC**;
- ✓ Descreve uma **proposta completa e autoexplicativa** e visa proporcionar **soluções de fácil interpretação**, dispensando elevada literacia nos domínios relevantes;
- ✓ Responde à **aferição do valor de risco e potencial indemnizatório aos titulares**.

5.2 PRINCIPAIS LIMITAÇÕES

Não obstante do esforço em apresentar uma solução tecnicamente simplificada, o tema da investigação é de elevada complexidade e ausente de relevante e completa jurisprudência.

Tanto as Autoridades de Controlo europeias, como o Comité Europeu de Proteção de Dados (EDPB), têm procurado apresentar orientações relevantes, as quais são elencadas na presente tese, todavia carecem de alinhamento metodológico e de definições exatas que contribuam para uma verdadeira harmonização da gestão de risco no tratamento de dados pessoais.

De realçar igualmente, a existência de conceitos indeterminados e incerteza jurídica em temas fundamentais para o cumprimento do RGPD e demais legislação aplicável em matéria de dados pessoais, promovendo interpretação ambígua.

Procura-se desafiar um novo equilíbrio, entre o risco para a organização e o risco para o titular, que assumirá especial relevância quando se verificar uma maior literacia do mercado quanto às obrigações legais e regulatórias de dados pessoais, tornando os titulares dos dados no verdadeiro âmago da avaliação.

5.3 TRABALHO FUTURO

A presente investigação cumpre com os objetivos propostos, todavia estes assumem-se como orientadores e exemplificativos, merecendo ser mais detalhadamente explorados, pela importância que corporiza para toda a sociedade, uma vez que trata de matéria relacionada com direitos fundamentais.

Neste sentido, prevê-se a publicação de artigos que promovam a continuidade do estudo da presente tese, bem como o desenvolvimento de aplicações de software que permitam aplicar de modo simplificado a proposta desta tese, mesmo por aqueles que detenham reduzida literacia, porém sintam a necessidade de cumprir com requisitos legais e regulatórios relacionados com o tratamento de dados pessoais.

REFERÊNCIAS

[1] Warren and Brandeis, "The Right To Privacy", 4 Harvard Law Review 193 (1890), http://faculty.uml.edu/sgallagher/harvard__law_review.htm

[2] Assembleia Geral da ONU. (1948). "Declaração Universal dos Direitos Humanos" (217 [III] A). Paris. Retirado de http://www.un.org/en/universal-declaration-human-rights/

[3] Artigo publicado pelo autor desta tese, (fev. 2015). A importância das disciplinas de Compliance na Cibersegurança e Ciberdefesa Nacional. Segurança e Defesa. ISSN1646-6071. Loures: Diário de Bordo, No 31, p. 54-57.

[4] Constituição da República Portuguesa (1976)

[5] European Parliament and of the Council, Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), Official Journal of the European Union, 2016

[6] Assembleia da República Portuguesa, Lei n.º 58/2019, de 8 de Agosto, Diário da República n.º 151/2019, Série I de 2019-08-08, 2019

[7] GDPR Enforcement Tracker, https://www.enforcementtracker.com/?insights

[8] Fukuda, K. (2020). Science, technology and innovation ecosystem transformation toward society 5.0. International Journal of Production Economics, 220, 107460.

[9] WEF (Maio, 2020). COVID-19 Risks Outlook | A Preliminary Mapping and Its Implications. World Economic Forum. Cologny/Geneva, Switzerland: ISBN-13: 978-2-940631-02-5

[10] WEF (Maio, 2020). Cybersecurity Leadership PrinciplesLessons learnt during the COVID-19 pandemic to prepare for the new normal. World Economic Forum. Geneva, Switzerland

[11] OECD (2019), "Online privacy", in Measuring the Digital Transformation: A Roadmap for the Future, OECD Publishing, Paris, https://doi.org/10.1787/c49bc6a4-en.

[12] Parecer N.º 20/2018 da CNPD em https://cutt.ly/p20-2018-cnpd-parlamento

[13] Chatterjee, S., Tulu, B., Abhichandani, T., and Li, H. SIP-based Enterprise Converged Network for Voice/Video over IP: Implementation and Evaluation of Components. IEEE Journal on Selected Areas in Communications - Recent Advances in Managing Enterprise Network Services, 23, 10 (2005)

[14] Cole, R., Purao, S., Rossi, M., and Sein, M.K. Being Proactive: Where Action Research Meets Design Research. Twenty-Sixth International Conference on Information Systems, Las Vegas, USA: AIS, 2005, 325-336

[15] Järvinen, P. Action Research is Similar to Design Science. Quality & Quantity, 41, 1 (2007), 37-54

[16] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," Journal of Management Information Systems, vol. 24, no. 3, pp. 45–78, Dec. 2007

[17] Lei n.º 10/91; Lei n.º 67/98 de 26 de outubro; Lei n.º 58/2019 de 8 de agosto.

[18] Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995; Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016.

[19] WP218 14/EN, Statement on the role of a risk-based approach in data protection legal frameworks, adopted on 30 May 2014.

[20] Center for Information Policy Leadership, Risk, High Risk, Risk Assessments and Data Protection Impact Assessments under the GDPR. CIPL Hunton & Williams LLP (2016)

[21] Center for Information Policy Leadership, The Role of Risk Management in Data Protection. CIPL Hunton & Williams LLP (2014)

[22] Center for Information Policy Leadership, A Risk-based Approach to Privacy: Improving Effectiveness in Practice. CIPL Hunton & Williams LLP (2014)

[23] Resultado obtido por meio da pesquisa: https://trends.google.com/trends/explore?date=all&q=CIPL,WP29

[24] Commission Nationale de L'Informatique et des Libertés (CNIL), Methodology for Privacy Risk Management, 2012

[25] Commission Nationale de L'Informatique et des Libertés (CNIL), Security of Personal data, 2018

[26] 2019, https://www.cnil.fr/en/open-source-pia-software-helps-carry-out-data-protection-impact-assesment

[27] WP248 17/EN Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, revised and adopted on 4 October 2017

[28] 2016, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V1.0.pdf

[29] 2014, https://www.aepd.es/sites/default/files/2019-09/guia-evaluaciones-de-impacto-rgpd.pdf

[30] 2014, https://www.pdpjournals.com/docs/88317.pdf

[31] International Organization for Standardization [ISO], ISO/IEC 27005:2018 Information technology — Security techniques — Information security risk management, 2018

[32] AXELOS. (2011). Management of Risk (M_o_R®) - Guidance for Practitioners. TSO (The Stationery Office).

[33] ENISA (2013), Data breach severity methodology

[34] https://www.elmundo.es/madrid/2019/05/29/5ced874421efa046348b4591.html

[35] https://apnews.com/article/technology-hacking-europe-cf8f8eee1adcec69bcc864f2c4308c94

[36] European Data Protection Board (EDPB), Guidelines 01/2021 on Examples regarding Data Breach Notification Version 1.0, adopted on 14 January 2021

[37] Governo de Portugal, Portaria n.º 679/2009 de 25 de junho, Diário da República n.º 121/2009, Série I de 2009-06-25, 2009

[38] Acórdão do Tribunal da Relação de Coimbra – Processo n.201/10.3TBTBU.C1

[39] Laborda Calvo E. Quantum Doloris. Aspectos práticos da avaliação do dano Corporal em Direito Civil 2008

[40] European Parliament and of the Council, Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 concerning the processing of personal data and the protection of privacy in the electronic communications sector (Directive on privacy and electronic communications), Official Journal of the European Union, 2002

[41] European Parliament and of the Council, Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009, amending Directive 2002/22/EC on universal ser-vice and users' rights relating to electronic communications networks and services, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, Official Journal of the European Union, 2009

[42] Article 29 Data Protection Working Party, Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679, 2017

[43] European Data Protection Board (EDPB) Homepage, https://edpb.europa.eu/, last accessed 2020/08/18

[44] CNPD Homepage, https://www.cnpd.pt/, last accessed 2020/08/18

[45] Common Criteria Portal Homepage, https://www.commoncriteriaportal.org, last accessed 2020/08/18

[46] International Organization for Standardization [ISO], ISO/IEC 27000:2018 Information technology — Security techniques — Information security management systems — Overview and vocabulary, 2018

[47] International Organization for Standardization [ISO], ISO/IEC 27001:2013 Information technology – Security techniques -- Information Security Management System -- Requirements, 2013

[48] International Organization for Standardization [ISO], ISO/IEC 27701:2019 Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines, 2019

[49] International Organization for Standardization [ISO], ISO/IEC 29100:2012, Information technology —Security techniques — Privacy framework, 2012

[50] International Organization for Standardization [ISO], ISO/IEC 31000:2018 Risk management – Principles and guidelines, 2018

[51] International Organization for Standardization [ISO], ISO/IEC 31010:2019 Risk assessment – Risk assessment techniques, 2019

[52] Nicolas Mayer, Éric Dubois, Raimundas Matulevicius and Patrick Heymans., Towards a Measurement Framework for Security Risk Management, CEUR Workshop Proceedings (2009)

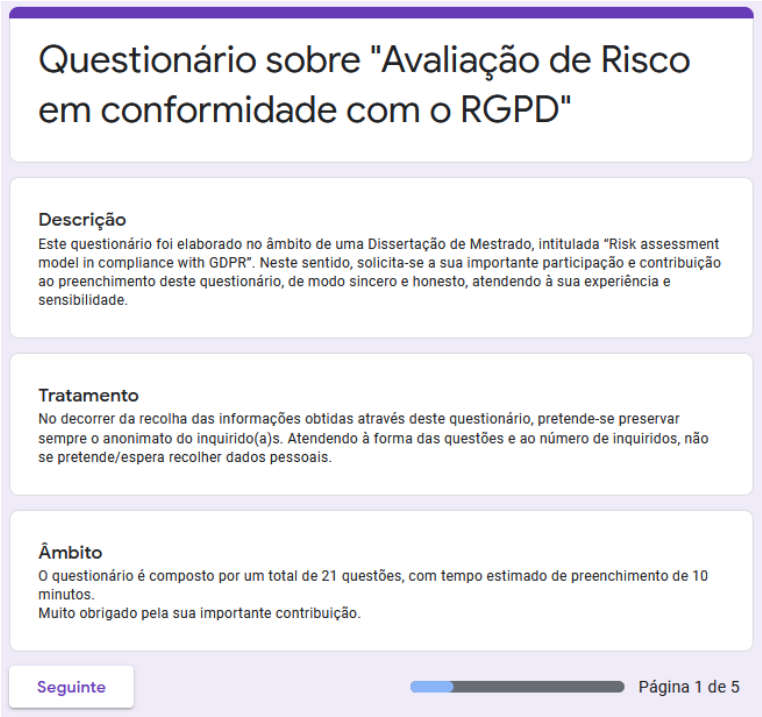
[53] Ionita, D., Hartel, Pieter, Pieters, Wolter, Wieringa, Roel., Current Established Risk Assessment Methodologies and Tools, 10.13140/RG.2.2.22914.68806 (2019)

[54] National Institute of Standards and Technology (NIST), NIST Special Publication (SP) 800-30, Revision 1, Guide for Conducting Risk Assessments, (2020)

[55] National Institute of Standards and Technology (NIST), Managing Information Security Risk Organization, Mission, and Information System View, (2011)

ANEXO

Inquérito online, disponibilizado a profissionais e especialistas, por meio do seguinte endereço: https://cutt.ly/MISE_RM_RGPD



Questionário sobre "Avaliação de Risco em conformidade com o RGPD"

Descrição

Este questionário foi elaborado no âmbito de uma Dissertação de Mestrado, intitulada "Risk assessment model in compliance with GDPR". Neste sentido, solicita-se a sua importante participação e contribuição ao preenchimento deste questionário, de modo sincero e honesto, atendendo à sua experiência e sensibilidade.

Tratamento

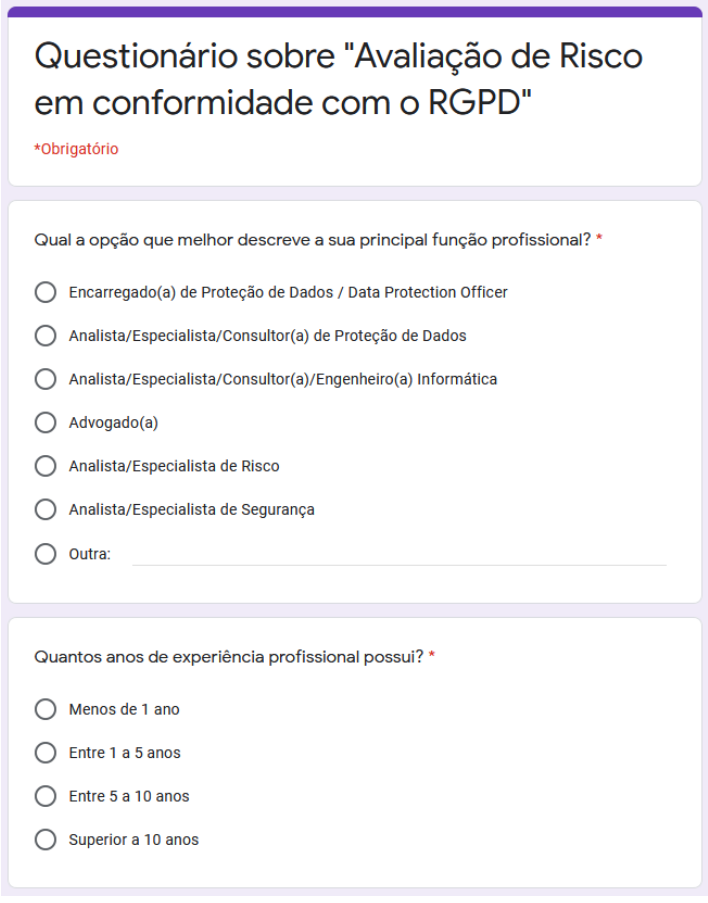
No decorrer da recolha das informações obtidas através deste questionário, pretende-se preservar sempre o anonimato do inquirido(a)s. Atendendo à forma das questões e ao número de inquiridos, não se pretende/espera recolher dados pessoais.

Âmbito

O questionário é composto por um total de 21 questões, com tempo estimado de preenchimento de 10 minutos.
Muito obrigado pela sua importante contribuição.

Seguinte

Página 1 de 5



Questionário sobre "Avaliação de Risco em conformidade com o RGPD"

*Obrigatório

Qual a opção que melhor descreve a sua principal função profissional? *

- ◯ Encarregado(a) de Proteção de Dados / Data Protection Officer
- ◯ Analista/Especialista/Consultor(a) de Proteção de Dados
- ◯ Analista/Especialista/Consultor(a)/Engenheiro(a) Informática
- ◯ Advogado(a)
- ◯ Analista/Especialista de Risco
- ◯ Analista/Especialista de Segurança
- ◯ Outra: _____

Quantos anos de experiência profissional possui? *

- ◯ Menos de 1 ano
- ◯ Entre 1 a 5 anos
- ◯ Entre 5 a 10 anos
- ◯ Superior a 10 anos

O exercício da sua atividade profissional é realizado apenas num sector específico, ou atua/interage com diferentes sectores? *

- ◯ Num sector específico
- ◯ Em diferentes sectores

Atendendo à sua experiência, considera que o mercado sabe a diferença entre "Risco para o Negócio" e "Risco para a Privacidade/Proteção de Dados Pessoais"? *

- ◯ Sim
- ◯ Não

Qual a importância da avaliação de risco, na conformidade com o RGPD? *

- ◯ Fundamental
- ◯ Recomendável
- ◯ Dispensável

Anterior Seguinte Página 2 de 5

Questionário sobre "Avaliação de Risco em conformidade com o RGPD"

*Obrigatório

Por favor descreva quais as dimensões e critérios que, na sua opinião e experiência, devem ser tidos em conta na avaliação do "Risco para a Privacidade/Proteção de Dados Pessoais" em conformidade com o RGPD? *

- ☐ Tipo de dados pessoais (ex.: dados de identificação, financeiros, sensíveis, etc.)
- ☐ Facilidade de correlação dos dados com pessoas singulares
- ☐ Confidencialidade
- ☐ Integridade
- ☐ Disponibilidade
- ☐ Motivação (ex: maliciosa ou ato acidental)
- ☐ Fundamento de licitude do tratamento
- ☐ Superfície de exposição (ex.: publicado na Internet ou restrito a um reduzido número de titulares)
- ☐ Impacto financeiro/solvência e/ou reputacional do Responsável pelo Tratamento
- ☐ Danos para os titulares, nomeadamente dano material ou não-material
- ☐ Benefícios para os titulares, nomeadamente as vantagens e benefícios ao seu dispor (ex: proteção, facilidade de uso do serviço)
- ☐ Outra: _____

Considera que os danos materiais devem ter a mesma importância dos não-materiais (ex.: perda de liberdade/movimento versus prejuízo para a reputação; etc....) *

- ◯ Sim
- ◯ Não

Já implementou alguma metodologia de avaliação de risco para a privacidade, na sua organização ou clientes? *

- ◯ Sim
- ◯ Não

Se respondeu sim à questão anterior, por favor indique em que se fundamentou?

- ☐ ISO/IEC
- ☐ M_o_R
- ☐ NIST
- ☐ Outra: _____

A definição da metodologia de avaliação de risco para a privacidade, teve o envolvimento de profissionais e/ou especialistas de risco? *

- ◯ Sim
- ◯ Não

Anterior Seguinte Página 3 de 5

Questionário sobre "Avaliação de Risco em conformidade com o RGPD"

*Obrigatório

Ao nível do risco para a organização, considera que o mercado dispõe de informações profícuas para avaliar o risco de conformidade com o RGPD? *

- ◯ Sim
- ◯ Não

Quão consciente considera que o mercado está, relativamente ao RGPD prever para além das coimas, a possibilidade de indeminização aos titulares de dados pessoais? *

- ◯ Totalmente
- ◯ Parcialmente
- ◯ Vagamente
- ◯ Não está minimamente consciente

Quão relevante considera que, a avaliação de risco permita aferir sempre que possível, um valor indemnizatório indicativo/referencia ao(s) titular(es) de dados pessoais visado(s)? *

- ◯ Fundamental
- ◯ Recomendável
- ◯ Dispensável

Considera exequível que no momento da celebração de um contrato (ex.: aquisição/subscrição de produto ou serviços), fossem solicitados elementos ao titular de dados que, permitam identificar o apetite e a tolerância ao risco, que este se encontra disposto a experienciar? *

- ◯ Sim, considero exequível e obrigatório, de outro modo será sempre uma avaliação totalmente subjetiva.
- ◯ Sim, considero possível, mas não obrigatória, podendo a tolerância ao risco ser aferida de outra(s) forma(s).
- ◯ Não, considero possível, mas não recomendável, por diversos motivos técnicos e/ou jurídicos.
- ◯ Não, pois além de impossível é também não recomendável, por diversas razões.

Por favor justifique a sua afirmação à questão anterior, caso não tenha respondido à opção a) na pergunta anterior.

A sua resposta

Anterior Seguinte Página 4 de 5

Questionário sobre "Avaliação de Risco em conformidade com o RGPD"

*Obrigatório

De acordo com a sua experiência e sensibilidade, como prevê que seja o impacto dos eventos de privacidade nos próximos 5 anos? *

- ◯ Elevado
- ◯ Moderado
- ◯ Reduzido

Considerando as tendências tecnológicas e as transformações a que o mercado tem sido forçado nos últimos 3 anos (ex.: aumento das obrigações regulatórias e pandemia covid19), como define a evolução do risco para os titulares de dados pessoais? *

- ◯ Aumentou radicalmente
- ◯ Aumentou marginalmente
- ◯ Estabilizou
- ◯ Decresceu

Num exercício de avaliação de proporcionalidade, entre os benefícios e os danos para o(s) titular(es) num mesmo TRATAMENTO de dados pessoais, como considera cada um? *

- ◯ Os benefícios para o(s) titular(es) devem ter um MAIOR peso que os danos, valorizando especialmente os benefícios e as funcionalidades ao dispor do(s) titulares, ainda que esse tratamento promova danos para o(s) mesmo(s).
- ◯ Os benefícios e os danos devem ser considerados com o MESMO peso (contributo igualitário), devendo ser realizada uma avaliação de impacto que afira ambos, todavia cada um terá a mesma importância na ponderação da avaliação de risco.
- ◯ Os benefícios devem ter um peso INFERIOR aos danos, pois os benefícios e funcionalidades a favor dos titulares, devem ser menos relevantes na análise do que os danos intrinsecamente causados.

Utiliza algum software para avaliar o risco de proteção de dados, que já proporcione uma avaliação de risco por defeito (ex.: PIA da CNIL, etc.)? *

- ◯ Sim
- ◯ Não

Se respondeu "Sim" à questão anterior, por favor indique o nome do(s) software(s) utilizado(s).

A sua resposta

No contexto do presente questionário, pode colocar qualquer comentário que considere relevante:

A sua resposta

Anterior | Submeter | Página 5 de 5