UNIVERSIDADE ABERTA **INSTITUTO SUPERIOR TÉCNICO**

GOVERNANÇA DA AUTOMATIZAÇÃO DE PROCESSOS EM CONFORMIDADE COM A NORMA ISO 27001:2022

António Augusto Lopes Fonseca

Mestrado em Informação e Sistemas Empresariais

Dissertação orientada pelo Professor Doutor José Henrique Pereira São Mamede

Março de 2025

Agradecimentos

Ao Professor Henrique S. Mamede, meu orientador, pela disponibilidade, apoio e motivação transmitida.

Aos colegas de trabalho que participaram nesta minha jornada.

À minha família, ao João, à Gabriela e à Ana. Ao Fernando Martinho pela paciência e pela ajuda valiosa.

A todos o meu Obrigado,

A. Augusto Fonseca

DECLARAÇÃO DE INTEGRIDADE
STATEMENT OF INTEGRITY

Declaro ter atuado com integridade na elaboração da presente dissertação. Confirmo que em todo o trabalho conducente à sua elaboração não recorri à prática de plágio ou a qualquer outra forma de falsificação de resultados.
Mais declaro que tomei conhecimento integral do Regulamento Disciplinar da Universidade Aberta, publicado no Diário da República, 2.ª série, n.º 215, de 6 de novembro de 2013.

I hereby declare having conducted my Dissertation with integrity. I confirm that I have not used plagiarism or any form of falsification of results in the process of the thesis elaboration.
I further declare that I have fully acknowledged Disciplinary Regulations of the Universidade Aberta (regulation published in the official journal Diário da República, 2.ª série, N.º 215, de 6 de novembro de 2013).

Universidade Aberta, 27 de março de 2025

Nome completo/Full name: António Augusto Lopes Fonseca
Assinatura/Signature:

Assinado por: **António Augusto Lopes Fonseca**
Num. de Identificação: 09232096
Data: 2025.04.07 19:38:47+01'00'

CHAVE MÓVEL

_____

manuscrita ou digital / handwritten or digital

Governança da Automatização de Processos em conformidade com a norma ISO 27001:2022

Resumo. No contexto da implementação iminente de tecnologias de Automação Robótica de Processos (RPA) numa organização, visando a automação de tarefas manuais repetitivas e de baixo valor nas interfaces do utilizador nos diversos processos de negócios, emergem inúmeros benefícios para alcançar a eficiência e eficácia, embora comportem alguns riscos. Estes novos processos automatizados introduzem complexidades adicionais, requerendo uma abordagem meticulosa para garantir a conformidade com os controlos estabelecidos nas políticas de segurança da informação em vigor nas organizações. Esta investigação aborda os desafios inerentes à implementação de RPA, focando a governança na segurança para a conformidade com as regras de TI e padrões internacionais de segurança da informação.

Recorrendo à metodologia de investigação *Design Science Research*, propõe-se a criação de um artefacto de TI propositadamente desenvolvido para resolver um problema organizacional importante, atuando como um "robô" de auditoria para validar a conformidade dos processos automatizados com a norma ISO 27001:2022. Este artefacto visa colmatar a lacuna entre a aplicação prática e o avanço do conhecimento científico, contribuindo tanto para a prática profissional como para a compreensão teórica da governança da segurança da informação em contexto de RPA. A pesquisa destaca ainda a relevância de alinhar as capacidades do modelo com métricas ideais, seguindo o exemplo de outros domínios, através de uma revisão Sistemática de literatura.

Este estudo teve como objetivo transmitir conhecimentos às organizações que pretendam implementar RPA em conformidade com os padrões de segurança reconhecidos e contribuir para o desenvolvimento de práticas mais eficientes e eficazes na governança da segurança da informação.

Palavras-chave: *RPA, automatização de processos, governança, conformidade, segurança da informação, ISO 27001:2022*.

Índice

1. Introdução 1
2. Metodologias de Investigação 3
   2.1. Revisão Sistemática da Literatura (SLR) 3
   2.2. Design Science Research (DSR) 4
3. Contexto Teórico 6
4. Revisão Sistemática da Literatura 9
   4.1. Planeamento 9
      4.1.1. Desenvolvimento de um Protocolo de Revisão 10
      4.1.2. As perguntas de investigação 10
      4.1.3. Execução do Protocolo de Revisão 11
   4.2. Realização da revisão 12
      4.2.1. Seleção dos Artigos 12
      4.2.2. Analise da Extração de Dados 13
   4.3. Análise 15
      4.3.1. Impacto da implementação de automação robótica de processos na segurança da informação nas organizações 16
      4.3.2. Desafios e riscos associados à integração de RPA, especificamente com vista a preservação da segurança 19
      4.3.3. Eficácia na transferência da responsabilidade dos utilizadores, em *compliance* da segurança da informação, para os robôs/*bots* 23
      4.3.4. Auditar a conformidade de segurança dos processos RPA recorrendo a robôs auditores 24
   4.4. Discussão 25
5. Problema e Proposta de Investigação 27
   5.1. Motivação da Pesquisa 28
   5.2. Objetivos 29
6. Concepção e desenvolvimento 32
   6.1. Proposta Conceptual para o desenvolvimento do artefacto Robô Auditor 32
   6.2. Levantamento do processo de auditoria interna - ISO27001 34

6.3. Seleção das atividades para automatização. 35
6.4. Analise de requisitos 36
6.5. A Arquitetura proposta 37
6.6. Implementação do artefacto 39
6.6.1. Parametrização e Configuração do Processo de Auditoria Automatizada 42
6.7. Construção do protótipo 43
7. Demonstração do artefacto robô auditor 45
7.1. Situação atual (Manual): 46
7.2. Com a Automatização (RPA): 47
7.3. Discussão 50
8. Avaliação 52
8.1. Introdução, objetivos e métodos utilizados 52
8.2. Seleção do *Focus Group* 54
8.3. Planificação e condução do Focus Group 55
8.4. Resultados da avaliação 57
9. Conclusão 59
9.1. Conclusões da pesquisa 59
9.2. Limitações da pesquisa 60
9.3. Trabalho Futuro 61
Referências 62
Anexos 65
ANEXO I - Elementos de motivação identificados e representados de acordo com a linguagem ArchiMate 65
ANEXO II - Cálculo da Redução do FTE 66
ANEXO III - Motivação (20_Equipe ISMS) 67
ANEXO IV – ViewPoint: Motivação (21_Auditor Externo) 68
ANEXO V – ViewPoint: Motivação (23_DPO) 69
ANEXO VI – ViewPoint: Motivação (24_IT & RPA team) 70
ANEXO VII – ViewPoint: Motivação (25_Business Managers) 71

Lista de Figuras

Figura 2.1- Processo DSR e seus pontos de entrada, adaptado de [5] 5
Figura 3.1-Fonte: Gartner, Quadrante mágico para RPA, Agosto de 2023 7
Figura 4.1-Protocolo de revisão realizado nesta pesquisa (adaptado de [11]) 12
Figura 4.2-Aplicação do Processo de Revisão Sistemática da Literatura 13
Figura 4.3-Distribuição dos artigos selecionados, por ano de publicação 13
Figura 5.1-Drivers motivacionais para a implementação de um robô auditor. 29
Figura 5.2-Objetivos motivacionais para a implementação de um robô auditor 30
Figura 6.1-Proposta metodológica 33
Figura 6.2-Casos de uso de uma auditoria interna na organização 35
Figura 6.3-Requisitos e restrições de alto nível (Linguagem ArchiMate) 36
Figura 6.4-Motivações organizacionais identificadas na automatização de auditorias 37
Figura 6.5-ViewPoint Motivacional para o stakeholder CISO (notação Archimate) 38
Figura 6.6-Robô Auditor - Modelação do processo principal (notação BPMN) 39
Figura 6.7-Robô Auditor - Modelação subprocesso controlos tipo 1 (notação BPMN) 40
Figura 6.8-Robô Auditor - subprocesso para pesquisa na Intranet (notação BPMN) 40
Figura 6.9-Robô Auditor - Modelação subprocesso controlos tipo 2 (notação BPMN) 41
Figura 6.10-Robô Auditor - Modelação subprocesso controlos tipo 3 (notação BPMN) ... 41
Figura 6.11-Visualização parcial do ficheiro Excel de requisitos e parâmetros 42
Figura 6.12 Workflows (UiPath Studio) 43
Figura 6.13 Store Bucket (UiPath Cloud) 43
Figura 6.14-Atividades no projeto UiPath - Robô Auditor 44
Figura 6.15-Exemplos de atividades de integração no projeto UiPath Robô Auditor 44
Figura 7.1-Plataforma Open AI, uso e custos, conta pessoal utilizada 47
Figura 7.2-Requisitos de alto nível para o artefacto robô auditor (notação archimate) 50
Figura 8.1-Strategic DSR evaluation framework [47] 53
Figura 8.2-Dimensão e métodos aplicados, baseado em [47] 54

Lista de Tabelas

Tabela 2.1 Diretrizes para Pesquisa em Ciência do Design [6] 4
Tabela 4.1-Lista de artigos selecionados 14
Tabela 5.1-Requisitos operacionais e restrições para o artefacto a desenvolver 30
Tabela 6.1-Sumário da metodologia conceptual 33
Tabela 7.1-Demonstração dos custos do uso da API OpenAI 48
Tabela 7.2-Resumo das vantagens identificadas pelo uso da RPA 51
Tabela 8.1-Caracterização do elementos do Focus Group 55
Tabela 8.2-Guia de perguntas para a condução da entrevista ao Focus Group 56

Lista de abreviaturas, siglas e acrónimos

AI	Inteligência Artificial
API	Interface de Programação de Aplicações
BC	Continuidade de Negócio
BPMN	Modelo e Notação de Processos de Negócio
CISO	Diretor de Segurança da Informação
CRD	Centro de Revisões e Divulgação, Universidade de York.
DORA	Regulamento Europeu para Resiliência Digital no setor financeiro
DPO	Encarregado de Proteção de Dados
DSR	Pesquisa em Ciência do Design
DSRP	Processo de Pesquisa em Ciência do Design / *Design Science Research Process*
ERP	Sistema integrado de gestão empresarial / *Enterprise Resource Planning*
FTE	Indicador que corresponde ao número de horas que um funcionário a tempo inteiro, ETI (afeto a 100%) trabalha para uma entidade. (*Full-Time Equivalent*)
RGPD	Regulamento Geral de Proteção de Dados
ISMS	Sistema de Gestão de Sistemas de Informação
ISO	Organização Internacional para Padronização
PDCA	Método iterativo de gestão de quatro passos, utilizado para o controle e melhoria contínua de processos e produtos
PII	Informação Pessoalmente Identificável
RPA	Automatização Robótica de Processos
SI	Sistemas de Informação
TI	Tecnologias de Informação
TISAX	Mecanismo de avaliação e troca de informação para a segurança da informação das empresas na indústria automóvel
TOGAF	*Framework* de Arquitetura empresarial do *The Open Group*
UI	Interface de utilizador

1. Introdução

Com a implementação de tecnologias de automatização de processos, denominadas por *Robotic Process Automation* (RPA), pretende-se automatizar tarefas manuais repetitivas e de baixo valor acrescentado. Isto é alcançado através da interação com as interfaces de utilizador nas aplicações que suportam os vários processos de negócio [1]. Da adoção de RPA emergem benefícios substanciais para a eficiência e eficácia desses processos, embora não isentos de desafios e de riscos [2]. A automatização desses processos introduz complexidades adicionais, exigindo uma abordagem meticulosa para garantir a conformidade com os controlos tecnológicos estabelecidos nas políticas e procedimentos de segurança da informação em vigor numa organização, enquadrados pela norma ISO 27001:2022.

Perante este cenário, entende-se como necessária uma investigação com foco no impacte e nos desafios inerentes à implementação de tecnologias de RPA nas organizações. Esta, tem ênfase na governança da segurança da informação e na conformidade com as regras de TI e padrões de segurança [3].

A ausência de uma abordagem sistematizada para governar a implementação e operação de processos RPA em conformidade com a ISO 27001:2022 representa um desafio significativo. Da mesma forma, a transferência da responsabilidade da segurança da informação dos utilizadores para os robôs deve ser acautelada. É, por isso, fundamental validar e auditar sistematicamente os controlos de segurança após a automatização, garantindo a conformidade e sem comprometer a eficiência operacional. Para isso, é importante comprovar a viabilidade da utilização de *bots* na execução dessa avaliação.

Utilizando a Metodologia *Design Science Research* (DSR), esta investigação propõe o desenvolvimento de um artefacto de TI, estrategicamente projetado para abordar um desafio organizacional crucial [4]. Este artefacto atuará como um "robô" de auditoria, validando de forma contínua a conformidade dos processos automatizados com a norma ISO 27001:2022, além de avaliar a eficácia do modelo de governança proposto.

O propósito desta investigação é contribuir para a prática profissional e para o avanço teórico, para além de preencher a lacuna entre a aplicação prática da RPA e o conhecimento científico em governança de segurança da informação. A

proposta de um artefacto de TI específico visa oferecer uma solução prática e eficiente para os desafios identificados, destacando-se especialmente a importância da governança para uma implementação bem-sucedida de RPA.

A escolha da Revisão Sistemática de Literatura, ou *Systematic Literature Review* (SLR), como parte integrante da metodologia, decorre da necessidade de um levantamento abrangente e rigoroso das evidências existentes sobre a implementação de RPA e governança de segurança da informação. A SLR permite fazer uma análise crítica da literatura, atualizando o estado da arte e a justificação para a investigação, orientando assim o desenvolvimento do artefacto de TI proposto.

Em resumo, este estudo procura não apenas oferecer perspetivas e informações valiosas para as organizações que pretendam implementar um sistema de RPA de maneira segura, alinhada com padrões de segurança reconhecidos, mas também contribuir para o desenvolvimento de práticas eficazes na governança de segurança da informação. A abordagem da SLR reforça a fundamentação teórica, fornecendo uma base sólida para o avanço do conhecimento nesta área crítica.

Este documento está estruturado da seguinte forma: no Capítulo 2 estão descritas as metodologias de pesquisa utilizadas neste estudo. No Capítulo 3 aborda-se a definição de RPA e a relevância da norma ISO 27001:2022 para a segurança da informação e introduz-se uma explicação sobre a plataforma *UiPath*. O Capítulo 4 contém a execução da SLR. O Capítulo 5 aborda o problema e a proposta desta investigação. A conceção e desenvolvimento do artefacto é apresentado no Capítulo 6 e a sua demonstração no Capítulo 7. O Capítulo 8 apresenta a avaliação da solução e no Capítulo 9 são apresentadas as conclusões desta investigação.

2. Metodologias de Investigação

Neste capítulo, abordam-se as metodologias de investigação utilizadas neste estudo: *Design Science Research* (DSR) e *Systematic Literature Review* (SLR). Explicam-se e justificam-se as escolhas dessas metodologias, destacando-se a sua importância e relevância, tanto para o desenvolvimento do artefacto proposto, como para a análise do estado da arte sobre o tema.

A metodologia escolhida para conduzir esta pesquisa é a DSR. Esta escolha é fundamentada nos objetivos específicos decorrentes do problema identificado e nas questões que deles emergiram. Três artigos do início da década de 1990 introduziram a DSR à comunidade de Sistemas de Informação (SI) [5], destacando o seu potencial para abordar problemas enfrentados pelos profissionais de SI. A DSR foi proposta como complemento na pesquisa em ciências naturais da informação, visando resultados relevantes e eficazes para a prática de SI. Na DSR, o investigador responde a perguntas relevantes e práticas, criando artefactos inovadores, contribuindo assim para o conhecimento científico. Os artefactos projetados são, para além de ancora na pesquisa, fundamentais para entender o problema identificado. Esses artefactos podem ser construtos, modelos, métodos, instâncias ou teorias de design aprimoradas.

Como estudo prévio para identificar, analisar e compreender as evidências publicadas e relacionadas com as perguntas específicas desta pesquisa recorreu-se, tal como já antes referido, a uma Revisão Sistemática de Literatura (SLR).

2.1. Revisão Sistemática da Literatura (SLR)

A SLR aplica uma metodologia bem definida que nos permite rever e avaliar as evidências existentes relacionadas ao tema desta investigação. Este método envolve a definição de critérios de inclusão e exclusão, uma estratégia de pesquisa detalhada, avaliação crítica da qualidade dos estudos selecionados e a síntese dos resultados para fornecer uma visão abrangente do estado atual do conhecimento sobre o tema em questão. Dessa revisão, também, é possível identificar lacunas nas pesquisas existentes, que permitirão propor tópicos para investigações futuras. A fim de assegurar o rigor e a condução científica desta revisão, a estratégia de

pesquisa adotada deve garantir a identificação abrangente do maior número possível de artigos relevantes para o tema.

2.2. Design Science Research (DSR)

A *Design Science Research* (DSR) é uma metodologia de pesquisa que exige a criação e avaliação de artefactos inovadores de Tecnologia da Informação projetados para resolver os problemas organizacionais identificados. A pesquisa em ciência do design é diferenciada da prática de design. O artefacto em si deve ser rigorosamente definido, formalmente representado, coerente e internamente consistente. O processo envolve uma abordagem rigorosa para desenvolver artefactos que abordem problemas observados, que contribuam para a pesquisa, avaliem os designs e comuniquem os resultados às audiências pertinentes. Esses artefactos, como anteriormente referido, podem abranger construtos, modelos, métodos, instâncias ou teorias de design aprimoradas, mas também incorporar inovações sociais ou novas propriedades em recursos técnicos, sociais ou informacionais. Na DSR o investigador responde a perguntas relevantes e práticas, criando os referidos artefactos inovadores e contribuindo assim para o conhecimento científico. Por isso, os artefactos projetados são valiosos e fundamentais para compreender o problema identificado.

Para um *framework* de pesquisa consistente em DSR, e tal como definido por Hevner *et al.* [6], devem seguir-se as sete diretrizes descritas na tabela 2.1.

Tabela 2.1 Diretrizes para Pesquisa em Ciência do Design [6]

Diretriz	Descrição
Diretriz 1: Design como um artefacto	A Pesquisa em Ciência do Design tem de produzir um artefacto viável na forma de um construto, modelo, método ou uma instância.
Diretriz 2: Relevância do problema	O objetivo da Pesquisa em Ciência do Design é desenvolver soluções baseadas em tecnologia para problemas de negócio importantes e relevantes.
Diretriz 3: Avaliação do design	A utilidade, qualidade e eficácia do artefacto de design tem de ser rigorosamente demonstrada pela execução de bons métodos de avaliação.
Diretriz 4: Contribuições de pesquisa	Uma efetiva Pesquisa em Ciência do Design tem de fornecer contributos claros e verificáveis nas áreas do design de artefactos, design dos fundamentos e/ou no design das metodologias.

Diretriz	Descrição
Diretriz 5: Rigor da pesquisa	A Pesquisa em Ciência do Design depende da aplicação de métodos rigorosos, quer na construção, quer na avaliação do artefacto de design.
Diretriz 6: Design como um processo de pesquisa	A procura por um artefacto eficaz requer a utilização dos meios disponíveis para alcançar os fins desejados e, ao mesmo tempo, satisfazer as leis no ambiente do problema.
Diretriz 7: Comunicação da pesquisa	A Pesquisa em Ciência do Design deve ser apresentado de forma eficaz tanto para públicos orientados para a tecnologia quanto para públicos orientados para a gestão.

A pesquisa deve ser suportada por um *Design Science Research Process* (DSRP), como modelo conceitual, para orientar os investigadores na realização rigorosa da pesquisa em ciência do design, especialmente no domínio dos Sistemas de Informação (SI). Assim como, modelo mental ou *template,* para que os leitores e os revisores possam reconhecer e avaliar esse tipo de pesquisa, conforme proposto e validado por Peffers *et al.* [5].

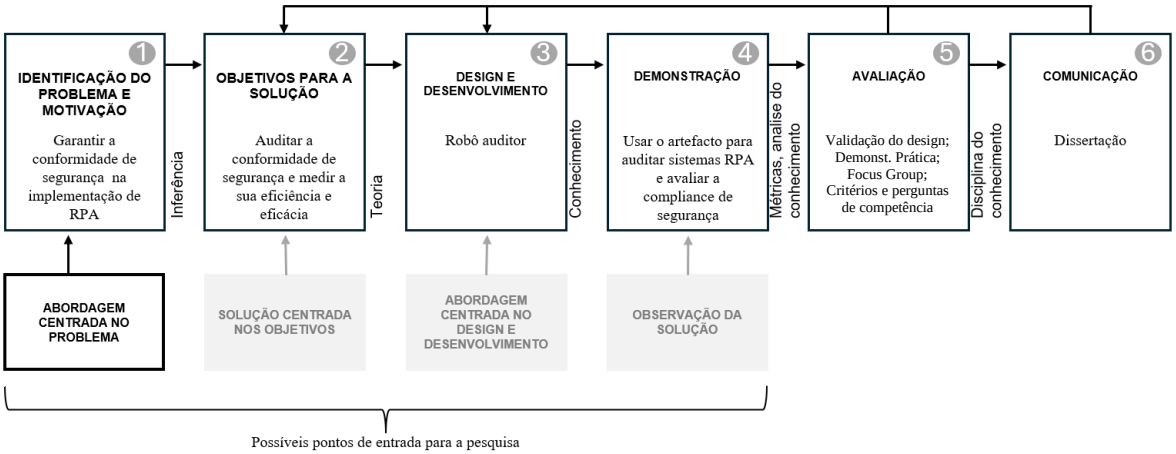


Figura 2.1- Processo DSR e seus pontos de entrada, adaptado de [5]

Sendo este processo estruturado em seis etapas numa ordem sequencial, conforme o ilustrado na figura 2.1, não existe uma obrigatoriedade de os pesquisadores respeitarem essa mesma ordem. Em vez disso, eles podem começar em diferentes etapas, tendo em conta os chamados pontos de entrada de pesquisa [5]. Uma abordagem centrada no problema, como é o caso desta pesquisa, deve iniciar-se com a atividade 1. Culminando na criação de um artefacto que, até então, ainda não tenha sido formalmente pensado como uma solução para o domínio explícito do problema no qual será usado.

3. Contexto Teórico

No seguimento da apresentação das metodologias de investigação utilizadas nesta investigação, nomeadamente a SLR e a DSR, estabelece-se neste capítulo a base teórica necessária para a compreensão do problema em análise. A definição clara dos conceitos fundamentais é essencial para enquadrar a problemática e fundamentar as decisões metodológicas tomadas nas fases subsequentes. Neste capítulo serão abordados os três pilares essenciais para a investigação: a Automação Robótica de Processos, a norma ISO 27001:2022 e a plataforma *UiPath*. Primeiramente, será explorado o conceito de RPA, abordando-se o seu funcionamento, benefícios e impacte na otimização de processos de negócio nas organizações. Posteriormente, é analisada a relevância da ISO 27001:2022, norma de referência para a gestão da segurança da informação, cujo cumprimento é fundamental para garantir a integridade, confidencialidade e disponibilidade dos dados e informação nas organizações. Por fim, será introduzida a plataforma *UiPath*, uma das soluções tecnológicas mais utilizadas para a implementação de RPA, sendo esta a ferramenta escolhida para o desenvolvimento do artefacto proposto.

Na vanguarda da transformação digital, a automatização de processos representa uma revolução na forma como as organizações gerem as suas operações. A utilização de ferramentas de RPA constitui uma abordagem inovadora que recorre a robôs de software para automatizar tarefas manuais e repetitivas, anteriormente executadas por humanos [3]. Estes robôs, programados para imitar as ações humanas, executam processos complexos de forma eficiente, reduzindo erros e libertando recursos humanos para tarefas mais estratégicas. Podemos definir RPA como uma ferramenta de software configurável, que usa regras de negócio e sequências de ações para que de forma automática complete processos em um qualquer número de aplicações diferentes, da mesma forma que os humanos, com a ajuda de pessoas para gerir as exceções. Portanto, a RPA opera no chamado *"front end"* das aplicações, de forma similar ao modo como as pessoas usam essas aplicações.

No âmbito do RPA, encontram-se robôs do tipo *"attended"* e *"unattended*" [7]. Os robôs "*attended*" operam em colaboração direta com os utilizadores, auxiliando-os em tarefas específicas e proporcionando uma abordagem mais interativa. Por outro

lado, os robôs *"unattended"* executam as suas tarefas de forma autónoma, sem a necessidade de intervenção humana direta. Esta distinção destaca a flexibilidade da RPA em se adaptar a diferentes cenários operacionais, seja aprimorando a colaboração humana ou automatizando processos de forma independente. Além disso, a evolução do RPA trouxe soluções que podem ser implementadas na nuvem, localmente (*on-premises*) ou numa abordagem híbrida. As soluções RPA na nuvem oferecem escalabilidade, flexibilidade e acessibilidade remota, enquanto as soluções *on-premises* atendem a requisitos específicos de segurança e de controlo. Essa variedade de opções destaca a adaptabilidade da RPA às diversas necessidades e contextos operacionais das organizações modernas.

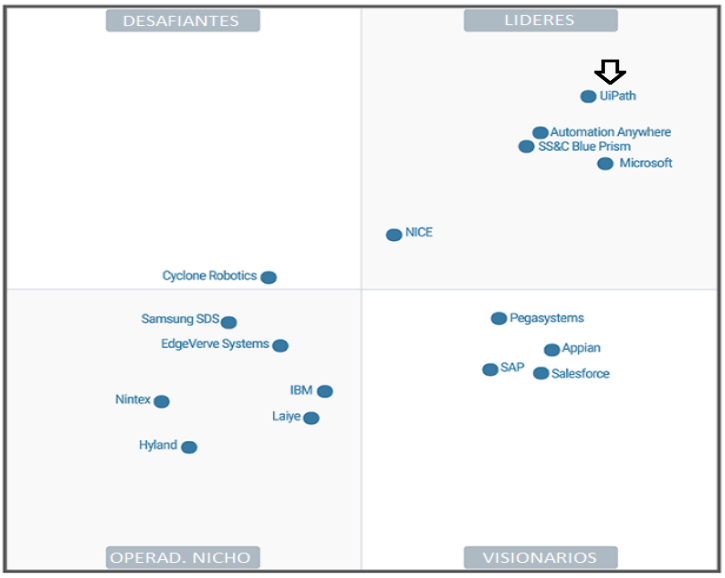


Figura 3.1-Fonte: Gartner, Quadrante mágico para RPA, Agosto de 2023

No cenário da RPA, e analisando as tendências de mercado, tais como, direção, maturidade e participantes, a plataforma *UiPath* destaca-se como uma solução líder. Essa é a conclusão plasmada no quadrante mágico da Gartner em 2023, conforme figura 3.1. O estudo da Gartner[1] envolveu 16 soluções RPA e incluiu critérios de análise como a orquestração, segurança e *compliance*, *Screen Scraping*, governança, capacidades *cloud*, automação "*unattended*", entre outros. A *UiPath* oferece uma interface intuitiva e recursos poderosos que simplificam a automatização de processos de negócio. A sua capacidade de integração, com uma ampla variedade

[1] https://www.uipath.com/blog/rpa/gartner-magic-quadrant-rpa-report-2023-archives

de sistemas, torna-a na primeira escolha em muitas organizações que procuram melhorar a eficiência operacional e reduzir os custos associados a tarefas repetitivas.

No entanto, a implementação de RPA não pode negligenciar considerações críticas de segurança da informação. É aqui que a norma ISO 27001:2022 [8] assume um papel fundamental. Esta norma é um padrão internacional para sistemas de gestão de segurança da informação, estabelecendo diretrizes e requisitos rigorosos para proteger dados sensíveis. Ao adotar os controlos da ISO 27001:2022, as organizações asseguram que os processos automatizados estão alinhados com as melhores práticas de segurança, garantindo a confidencialidade, a privacidade, a integridade e disponibilidade da informação.

Assim, neste contexto teórico destacam-se, não apenas os princípios fundamentais da RPA, mas também se enfatiza a importância do *UiPath* como uma ferramenta líder nesse domínio. Destaca-se, ainda, a essencialidade da norma ISO 27001:2022 para garantir a conformidade e uma segurança robusta na era da automatização. Este entendimento estabelece as bases para uma análise mais aprofundada nos capítulos subsequentes.

4. Revisão Sistemática da Literatura

No capítulo anterior fez-se o enquadramento teórico da investigação, abordando conceitos fundamentais como a RPA, a norma ISO 27001:2022 e a plataforma *UiPath*. Esta base conceptual permitiu compreender os principais elementos envolvidos na problemática estudada nesta investigação, assim como a sua relevância no contexto da segurança da informação. Neste capítulo apresenta-se a Revisão Sistemática da Literatura, uma etapa essencial da metodologia de pesquisa utilizada para garantir um levantamento rigoroso e estruturado do estado da arte atual sobre o tema. A SLR foi conduzida de acordo com um protocolo definido, incluindo a formulação das perguntas de investigação, a definição dos critérios de seleção de estudos e a execução do processo de extração e análise dos dados.

A revisão da literatura tem como objetivo identificar, organizar e sintetizar as principais contribuições científicas relacionadas ao impacte da RPA na segurança da informação, os desafios e riscos da sua integração, a transferência da responsabilidade (pela verificação da conformidade da segurança) para os robôs e a viabilidade da auditoria automatizada dos processos RPA. As evidências obtidas nesta fase constituem um alicerce fundamental para a definição do problema de investigação e a subsequente conceção do artefacto, garantindo que a proposta esteja alinhada com as lacunas identificadas na revisão da literatura científica. A aplicação de uma LSR, conforme recomendado por Kitchenham *et al.* [9], permite uma abordagem rigorosa e replicável na seleção e análise de estudos relevantes, assegurando a fundamentação teórica necessária para o desenvolvimento da solução proposta e que serão explorados nos capítulos seguintes.

4.1. Planeamento

A necessidade de uma revisão sistemática surge da exigência dos investigadores resumirem todas as informações existentes sobre algum fenómeno de maneira abrangente e imparcial. Acima de tudo, antes de realizar uma revisão sistemática, os investigadores devem garantir que ela seja necessária [9]. Neste contexto, o *Centre for Reviews and Dissemination* (CRD), do Reino Unido, sugere a seguinte lista de verificações [10]:

- Quais são os objetivos da revisão?

- Que fontes foram pesquisadas para identificar estudos primários? Houve alguma restrição?
- Quais foram os critérios de inclusão/exclusão e como foram aplicados?
- Que critérios foram utilizados para avaliar a qualidade dos estudos primários e como foram aplicados?
- Como foram extraídos os dados dos estudos primários?
- Como foram sintetizados os dados? Como foram investigadas as diferenças entre os estudos? Como foram combinados os dados? Foi razoável combinar os estudos? As conclusões decorrem das evidências?

4.1.1. Desenvolvimento de um Protocolo de Revisão

Um protocolo de revisão identifica os métodos que serão utilizados numa revisão sistemática específica. Um protocolo predefinido é necessário para reduzir a possibilidade de viés do investigador. Por exemplo, sem um protocolo, é possível que a seleção de estudos individuais ou a análise sejam orientadas pelas expectativas do investigador. Os componentes de um protocolo devem incluir todos os elementos da revisão, além de algumas informações adicionais de planeamento. O contexto, as perguntas da pesquisa, estratégias de pesquisa, critérios de seleção, procedimentos de avaliação da qualidade dos artigos e estratégia para a extração e síntese dos dados devem fazer parte desses componentes [9].

4.1.2. As perguntas de investigação

A atividade mais importante durante a elaboração do protocolo é formular a pergunta, ou as perguntas de investigação. Existem algumas diretrizes, nomeadamente as definidas pelo *National Health and Medical Research Council* (NHMRC) australiano [9] que poderão ser adaptadas para questões de engenharia de software.

Para orientar a pesquisa de maneira científica, e partindo das diretrizes referidas, foram formuladas as seguintes questões:

- RQ1. Que evidências existem sobre o impacte da implementação de automação robótica de processos na segurança da informação nas organizações.

- RQ2. Quais os desafios e riscos associados a essa integração, especificamente com vista a preservação da segurança.
- RQ3. Como medir a eficácia da transferência da responsabilidade dos utilizadores, em *compliance* da segurança da informação, para os robôs/*bots*?
- RQ4. Qual a necessidade e como auditar a *compliance* de segurança dos processos com automação robótica, recorrendo a robôs “auditores”?

4.1.3. Execução do Protocolo de Revisão

O protocolo iniciou-se com uma pesquisa na literatura científica, tendo como ponto de partida a definição da chamada *string* de pesquisa. Essa *string* é constituída por um conjunto de palavras-chave com vista a encontrar estudos científicos que possam fornecer dados e informação que respondam às perguntas desta investigação – RQ1 a RQ4.

A *string* final, descrita em seguida, foi aplicada durante o mês de janeiro de 2024 sobre o *Dataset* EBSCO[2].

***String* de pesquisa:** "*robotic process automation*" AND (*ontology OR "information security" OR challenge* OR integrat* OR efficienc* OR compliance OR audit* OR robot*).

O protocolo completo de revisão é ilustrado na Figura 4.1. Após a obtenção do conjunto de artigos com base na *string* de pesquisa conclui-se a primeira fase do processo. Numa segunda fase são aplicados os critérios de inclusão e exclusão para aprimorar os resultados da pesquisa. Passa-se depois a uma terceira fase onde a totalidade dos resumos são analisados para avaliar a relevância que cada um deles tem para a pesquisa. Os mais relevantes transitam para a fase seguinte onde são lidos e analisados na integra para definir a sua legibilidade. Na quinta e última fase é definido o conjunto final de documentos para a realização da revisão.

[2] https://search.ebscohost.com/

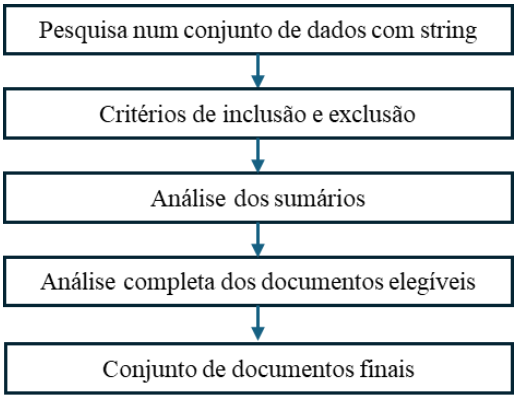


Figura 4.1-Protocolo de revisão realizado nesta pesquisa (adaptado de [11])

4.2. Realização da revisão

Nesta seção aborda-se a condução da revisão, que constitui a segunda fase da Metodologia de Revisão Sistemática da Literatura. Nesta fase realiza-se o processo de execução da pesquisa, utilizando a consulta específica nas bases de dados, previamente selecionadas, conforme delineado pelo protocolo de revisão. Os dados extraídos são depois sujeitos a uma análise profunda.

4.2.1. Seleção dos Artigos

Da execução da *string* de pesquisa realizada de acordo com o preconizado no protocolo de revisão, seção 4.1.3, foram encontrados 618 estudos. Após a aplicação dos vários filtros, desde os critérios de exclusão e inclusão, passando pela remoção dos duplicados, análise dos resumos e analise integral dos artigos, respetivamente, selecionaram-se 24 artigos relevantes para a nossa pesquisa. No entanto, ao longo do desenvolvimento desta investigação, identificaram-se outros artigos que, também, foram incluídos. A sua relevância e contribuição adicional para o tema, permitiram enriquecer a análise e garantir uma abordagem mais abrangente e atualizada dos temas. Na figura 4.2 estão representados os cinco níveis e tipos de filtros aplicados, sendo utilizados os seguintes critérios de inclusão e exclusão no filtro 2: Artigos científicos e revistos pelos pares; Escritos em inglês; Artigos disponíveis na integra.

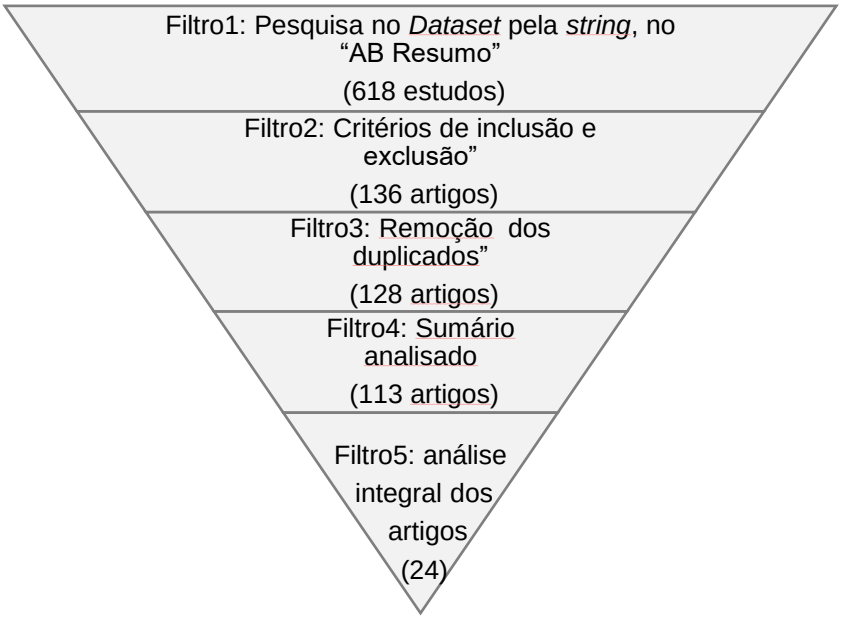


Figura 4.2-Aplicação do Processo de Revisão Sistemática da Literatura

4.2.2. Analise da Extração de Dados

Nesta subsecção apresenta-se a análise de diferentes dimensões sobre os resultados obtidos, ou seja, dos 24 artigos selecionados. Na figura 4.3 observa-se uma tendência de crescimento nos artigos publicados após 2018, apresentando o ano mais recente um número que é superior ao dobro de qualquer outro.

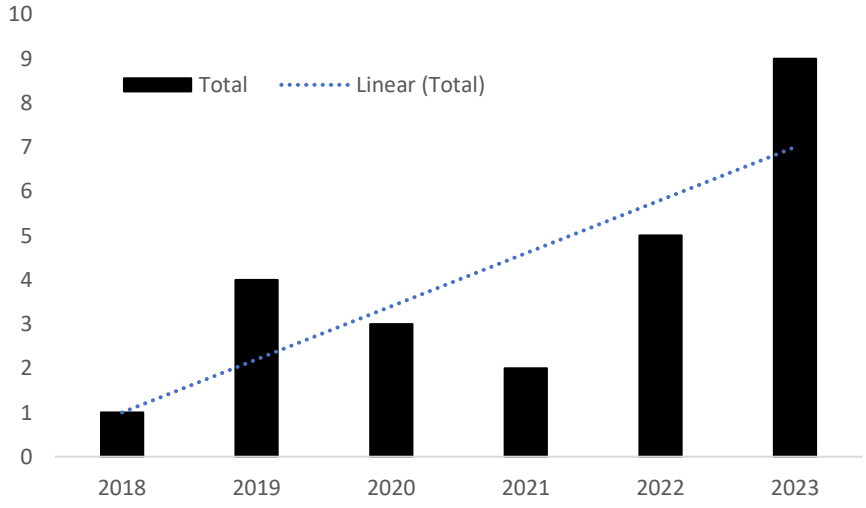


Figura 4.3-Distribuição dos artigos selecionados, por ano de publicação

Apesar de a tecnologia RPA estar já num nível de maturidade alta[3], esta analise permitiu verificar que as publicações científicas disponíveis e relevantes para o problema em analise, com ênfase em segurança da informação, são relativamente escassas e recentes.

A origem dos artigos selecionados é bastante dispersa, sendo que os 24 foram publicados em 22 revistas cientificas e apenas se repetiram as revistas "*Engineering Management in Production*" (2 artigos) e "*Journal of Emerging Technologies in Accounting*"(3 artigos). A tabela 4.1 mostra a totalidade dos 24 artigos e a sua respetiva origem.

Tabela 4.1-Lista de artigos selecionados

Revista	#
Accounting Horizons	1
Robotic Process Automation (RPA) Implementation Case Studies in Accounting: A Beginning to End Perspective.	
Annals of 'Constantin Brancusi' University of Targu-Jiu. Economy Series / Analele Universita-Jiu Seria Economie	1
Good business processes candidates for automation future of work: robotic process automation.	
Business Horizons	1
Deciding on the robotic process automation operating model: A checklist for RPA managers.	
Business Process Management Journal	1
Toward robotic process automation implementation: an end-to-end perspective.	
Contemporary Accounting Research	1
A Framework for Using Robotic Process Automation for Audit Tasks*.	
CPA Journal	1
Exploring the Use of Robotic Process Automation (RPA) in Substantive Audit Procedures.	
Dyna	1
Roadmap for the implementation of robotic process automation in enterprises	
Engineering Management in Production and Services	2
Robotic process automation - a driver of digital transformation?	
Robotic process automation (RPA) adoption: a systematic literature review.	
Enterprise Information Systems	1
Robotic process automation - a systematic mapping study and classification framework.	
European Journal of Information Systems	1
Security by envelopment-a novel approach to data-security-oriented configuration of lightweight-automation systems.	

[3] https://www.uipath.com/blog/rpa/gartner-magic-quadrant-rpa-report-2023-archives

Revista	#
Information (2078-2489)	1
Intelligent Process Automation and Business Continuity: Areas for Future Research.	
International Journal of Accounting Information Systems	1
Prototyping and implementing Robotic Process Automation in accounting firms: Benefits, challenges and opportunities to audit automation.	
International Journal of Business	1
The challenges of implementing robotic process automation in global business services.	
Journal of Emerging Technologies in Accounting	3
Intelligent Process Automation in Audit.	
Robotic Process Automation for Auditing.	
Robotic Process Automation Risk Management: Points to Consider.	
Journal of Information Systems	1
Attended Process Automation in Audit: A Framework and A Demonstration.	
Journal of Purchasing	1
Robotic Process Automation in purchasing and supply management: A multiple case study on potentials, barriers, and implementation.	
LogForum	1
Using robotic process automation (rpa) to enhance item master data maintenance process.	
Management Issues / Problemy Zarzádzania	1
Building a Robotic Capability Map of the Enterprise	
Organizacija	1
How Robot/human Orchestration Can Help in an HR Department: A Case Study From a Pilot Implementation.	
Proceedings of the International Conference on Business Excellence	1
Revamping Business Services: RPA Solutions Landscape.	
TEM Journal	1
Multi-Criteria Decision Making Analysis of Optimal Service Delivery Technique Using AHP.	
Total de artigos	**24**

4.3. Análise

Nesta última fase da Revisão Sistemática da Literatura são apresentados os resultados sobre as quatro questões de pesquisa, com base na análise efetuada às publicações obtidas e usando o protocolo de pesquisa. Estes resultados estão individualizados em quatro tópicos: Impacte na implementação de automação robótica de processos na segurança da informação nas organizações; Desafios e riscos associados à integração de RPA, especificamente com vista à preservação da

segurança; Métricas de eficácia da transferência da responsabilidade dos utilizadores, em *compliance* da segurança da informação, para os robôs/*bots*; Como auditar a *compliance* de segurança dos processos RPA recorrendo a robôs auditores.

4.3.1. Impacto da implementação de automação robótica de processos na segurança da informação nas organizações

A COVID-19 provou que os primeiros adeptos que investiram em RPA já experimentaram retornos importantes em 2020, devido aos recursos fundamentais que a RPA proporcionou às organizações, já que a diminuiu o trabalho humano, ajudou a gerir a organização e garantiu a continuidade do negócio. Embora essa transformação tenha permitido ganhos, criou um ecossistema mais complexo no qual vários *Business Processes* (BP) foram atualizados para incorporar tecnologias emergentes associadas ao RPA, exigindo que todos os riscos e benefícios tenham de ser reavaliados de modo a serem controlados em termos de *Business Continuity* (BC) [3]. Um total de 71 resultados de pesquisa [3] relatam que, pelo facto de algumas novas tecnologias disruptivas não serem bem conhecidas ou compreendidas, podem apresentar uma série de riscos desconhecidos, se não houver uma mitigação de resposta preparada com antecedência. Por um lado, Brás *et al.* [3] aponta para um risco acrescido decorrente da adoção e utilização de novas tecnologias e da falta de conhecimento do seu impacto real nas organizações, enquanto outros autores apontam evidências de que essas mesmas tecnologias ajudam a mitigar muitos tipos de risco.

Embora a RPA possa reduzir os erros humanos não intencionais, ou até intencionais [3], a sua adoção introduz novos riscos, que as empresas precisam compreender e abordar. Um dos muitos riscos analisados está relacionado com a segurança cibernética, pela falha da organização em considerar os efeitos das mudanças operacionais nos seus controlos internos, especialmente os tecnológicos, ou até do próprio esquecimento em atualizar os seus planos de BC. É imperativo que as empresas reavaliem os planos de BC existentes [3], realizem avaliações de risco completas e identifiquem novas vulnerabilidades impostas pelas tecnologias emergentes, bem como, pelas mudanças na forma como passaram a trabalhar.

A RPA é considerada por muitas organizações uma ferramenta ou solução acessível, que reduz o risco de conformidade e ao mesmo tempo economiza tempo [12]. Por definição, RPA envolve o emprego de ferramentas de software para automatizar processos de negócios; isto resulta na eliminação de atividades laboriosas, previsíveis e repetitivas que antes eram realizadas por humanos [13]. A automação de processos tem inúmeras vantagens, incluindo maior eficácia, redução de custos de processo e baixas taxas de erro. A RPA opera separadamente de outros programas de software incorporados no negócio, opera em ambientes próprios, normalmente virtuais – em servidores locais ou na nuvem. A escalabilidade é um dos principais benefícios [12], pois simplifica a replicação de *bots* quando o volume aumenta, assim como a sua desativação [14], ou seja, tem um contributo importante na dimensão de segurança - disponibilidade.

Wewerka *et al.* [15], sugerem que os efeitos positivos do RPA em qualquer organização sejam agrupados em quatro categorias (excluindo os aspetos humanos): Maior velocidade com que as tarefas de processos automatizados são executadas e, consequentemente, a redução da duração das tarefas; a Disponibilidade, onde a maioria dos *bots* estão disponíveis 24 horas por dia, 7 dias por semana e acesso instantâneo. Além disso, a RPA é altamente escalável para atender a uma intensidade variável de pedidos; a Conformidade, onde as tarefas do processo executadas por um *bot* são altamente transparentes e documentadas em detalhe. Como consequência, a conformidade e qualidade aumentam, o RPA elimina erros humanos, melhora a precisão e a qualidade dos dados e por isso leva a uma maior Satisfação do cliente.

Outro impacte passa pela falha em especificar a integridade da RPA como um objetivo [2], podendo criar várias ameaças aos ativos, à segurança da informação e à privacidade de uma organização. Por exemplo, o armazenamento de credenciais em *bots*, se deixadas desprotegidas, podem permitir acesso não autorizado a informações confidenciais.

Outra questão crítica da RPA abordada [16] é a da segurança da informação ao lidar com dados sensíveis, destacando-se que, apesar da automatização, muitas violações de segurança ainda ocorrem devido à falta de sistemas adequados e à incapacidade dos sistemas RPA avaliarem e protegerem dados sensíveis.

Observou-se, também, [17] que os processos mais críticos, embora muitas vezes adequados à automatização, podem apresentar desvantagens: as políticas da organização podem restringir a gama de escolhas de um decisor de RPA.

Por outro lado, quanto maior o número de diferentes formatos de dados, interfaces e sistemas de TI envolvidos, maior será a complexidade, a suscetibilidade a erros e o esforço de integração de *bots* [18], ou seja, especificações, programação e manutenção. Assim, alterações e atualizações nos sistemas acedidos têm um impacte significativo na RPA. Além disso, a redefinição de *bots* é frequentemente subestimada, mas necessária, pois um *bot* configurado com defeitos é menos eficiente e pode causar consequências graves.

Há um problema comum a todas as soluções RPA que as organizações enfrentam aquando da implementação, em larga escala, pela primeira vez [19]. Como a RPA pode ser executada maioritariamente em qualquer hardware, tenta-se escalar com base em algo chamado “use-se o que temos”, o que causa um desempenho diferente do servidor nestas novas circunstâncias e, consequentemente numa degradação do desempenho e na disponibilidade do robô.

À medida que os robôs interagem com a interface de utilizador do aplicativo (UI), estes acabam por integrar-se com qualquer software da organização, sem a preocupação da abertura à integração de terceiros [20]. Como o robô interage com UI, as aplicações não são modificadas, mantendo-se os seus níveis de segurança [21]. Isso significa que se podem implementar novas funcionalidades mais rapidamente do que outras soluções de TI que usam APIs para integração com sistemas, sendo implementado em 2 a 4 semanas, em vez de meses ou anos [22], ou seja, têm um impacte positivo na eficiência operacional e na dimensão da disponibilidade da informação.

Como resultado do projeto piloto concluído na investigação de Zhang [23], com vista à verificação do mapa de capacidades proposto, foram feitas as seguintes modificações: Uma nova capacidade de "Gestão de Normas de Segurança" foi adicionada na área de capacidade "Gestão de Normas de Automação de Processos Robóticos". Essa mudança foi motivada pela necessidade de destacar o papel da segurança no contexto da automação de processos robóticos.

Em contexto de realização de auditorias a implementação adequada da RPA pode libertar tempo para os auditores abordarem as questões mais importantes nos seus clientes [24]. No entanto, a RPA pode apresentar uma infinidade de desafios e oportunidades no futuro. Essas implicações práticas complementam os cinco temas principais relacionados: força de trabalho, governança de TI, privacidade e segurança, sustentabilidade do sistema e medição do sucesso da RPA, que Zhang *et al.* [25] identificaram anteriormente como importantes e que devem ser considerados pelas organizações ao adotarem RPA.

Refira-se, ainda, que o benefício mais evidente da aplicação da RPA em auditoria é a redução do tempo gasto em processos altamente repetitivos [26]. Retirar tarefas de "robô" aos humanos devolve mais trabalho de criação de valor aos auditores. Ainda como outros benefícios, inclui-se uma maior confiabilidade, uma execução perfeita dos planos de auditoria, uma qualidade de serviço aprimorada e melhor segurança da informação [26].

4.3.2. Desafios e riscos associados à integração de RPA, especificamente com vista a preservação da segurança

A preocupação com a segurança dos dados está entre os principais obstáculos à adoção da RPA [27]. A RPA pode operar com diferentes aplicações numa organização [28]. Esse recurso de interoperabilidade da RPA pode permitir a automação em larga escala em diferentes aplicações, mas estimula, também, preocupações sobre a manutenção da privacidade e segurança dos dados, uma vez que a RPA facilita a movimentação de dados entre aplicações em comparação com o processo manual. Além disso, os *bots* podendo agir como trabalhadores humanos, geralmente, têm as mesmas credenciais. Se a RPA for adotada para automatizar tarefas envolvidas com dados confidenciais, o risco de os *bots* os manipularem incorretamente (seja devido a fraude intencional ou erros não intencionais) deve ser levado em consideração. O uso de credenciais da organização nos processos de login dos *bots* são também um desafio à segurança, se essas credenciais não forem devidamente protegidas, o acesso não autorizado a um sistema RPA pode resultar em sérias consequências [7] [19] .

O binómio acesso-segurança, também, está entre as questões-chave nas implementações de RPA [29]. Os acessos aos recursos foram sempre geridos por humanos. No entanto, com os robôs de software, novas medidas devem ser consideradas no acesso desses robôs à informação [30]. Da mesma forma, as práticas de segurança atuais não consideram a existência de trabalhadores digitais, e implementar um novo quadro de segurança com sucesso constitui um desafio significativo para as organizações. A novidade do software e a resultante falta de documentação torna isso um desafio para as entidades adotarem RPA, pois atualmente não existem padrões e metodologias em vigor [31].

Como não há verificação humana antes de se executar uma tarefa, com maior enfase em robôs "*unattended",* o robô pode cometer erros mais rapidamente [20], pois não espera pelas respostas das aplicações como um humano o faria e, por isso, não sendo, eventualmente, capaz de verificar problemas de conexão, pode executar apenas parcialmente as tarefas. Além disso, um robô pode ter amplos direitos de acesso para interagir com outros sistemas, tanto quanto um superutilizador ou administrador, o que pode gerar problemas de segurança [20].

É também enfatizado por Asatiani *et al.* [16] que a implementação de RPA sobre uma arquitetura de TI existente torna a tecnologia suscetível a invasões deliberadas e fugas não intencionais de dados, por um possível aproveitamento de vulnerabilidades técnicas, representando um desafio significativo para a segurança da informação. O estudo releva que, por padrão, as soluções RPA muitas vezes não são projetadas para a segurança dos dados, tornando essencial um especial cuidado durante a configuração para garantir a preservação da segurança. Tratando-se de sistemas ligeiros de automação, que podem ser relativamente fáceis, a frequente negligência em relação aos aspetos de segurança desses sistemas pode tornar a organização mais vulnerável a diversos riscos. Destaca, ainda, a falta de orientação sobre como configurar sistemas RPA e redesenhar os processos subjacentes para abordar crescentes preocupações com segurança [16]. Sobre o compromisso entre a eficiência e a segurança, o artigo destaca o desafio de equilibrar a necessidade de eficiência ao conceder acesso total a sistemas sensíveis para agentes de automatização *mindless* e a prática de manter a segurança desses dados, reconhecendo a importância de escolhas cuidadosas de design de arquitetura empresarial.

Todas as arquiteturas devem garantir que os novos sistemas se integram perfeitamente com as plataformas da organização como um todo [32]. A área de TI deve estabelecer um mecanismo de monitorização do desempenho para gerir e monitorizar os projetos de RPA, assim como, realizar a manutenção e o suporte aos protocolos.

Para aproveitar plenamente a automatização e enfrentar os riscos, falhas ou ameaças potenciais, as organizações precisam de adotar uma abordagem holística para gerir a mudança, incluindo o alinhamento entre negócios e as TI, rever o plano de *Business Continuity* e criar novos controlos projetados para enfrentar os riscos específicos emergentes da RPA. O estudo de Brás *et al.* [3] revela que um total de 27 artigos analisados mostram que as organizações subestimam por vezes os desafios associados à integração de RPA nas suas operações, o que pode deixá-las vulneráveis a riscos e sujeitá-las a desafios adicionais na implementação de controlos, resultando, assim, em problemas de governança. A solução para mitigar riscos em RPA deve seguir um programa rigoroso, onde as regras e controlos de auditoria devem ser definidas corretamente. Deste ponto de vista, Wilkin e Chenhall [24] defendem que a implementação de RPA deve ser apoiada por um mecanismo eficaz de governação. Organizar e implementar a governança de RPA garante que o IT se alinha, metodicamente, com os processos de negócio. A seleção e a implementação de ferramentas, bem como processos apropriados, melhoram o desempenho e a segurança de projetos individuais de RPA, que, por sua vez, também se estendem ao cenário abrangente de automação em toda a organização. O objetivo é, assim, orquestrar com eficiência a colaboração de processos, pessoas e *bots*, para que todos possam estar alinhados com a estratégia de automação.

O conhecimento e competências são outro desafio na adoção de RPA. Faz prova disso o estudo apresentado por Wewerka *et al.* [15], que revela, com base num conjunto de artigos analisados, o quão patente é a critica de que faltam conhecimentos e competências e que as soluções de RPA não são robustas, no que diz respeito às interfaces de utilizador em constante evolução. Por outro lado, o estudo acrescenta que as implementações de RPA exigem maior envolvimento do departamento de TI do que se pensava inicialmente. A sensibilização e o conhecimento devem ser disponibilizados às partes interessadas para que possam compreender

plenamente o conceito de RPA e como ele capacitará cada processo [33]. Regista-se, também, que muitas publicações enfatizam as diferenças entre RPA e BPM e que compreender essas diferenças é fundamental para aplicar adequadamente os métodos RPA e BPM num contexto empresarial. Desta análise comparativa identificam-se como problemas na RPA a privacidade e os incidentes de segurança da informação. Portanto, é de suma importância que uma organização adquira as capacidades apropriadas na área de RPA [34]. Os detalhes dessas capacidades dependem dos objetivos de automação robótica adotados por uma organização específica. A organização pode adquiri-los a um fornecedor externo ou desenvolvê-los internamente, implementando um portfólio específico de projetos. Por isso, Zhang [23] defende que o mapa de capacidade robótica que propõe é uma boa ferramenta para coordenar trabalhos nessa área.

Assim, tal como a implantação de qualquer outro software empresarial, a implementação de RPA envolve um conjunto de decisões que requerem considerações cuidadosas. Embora existam muitos modelos de operação de RPA para escolher, nem sempre é claro qual deles é mais adequado ao contexto e aos objetivos de negócios de uma determinada organização. Esta falta de clareza, também, afeta os fornecedores de RPA [17]. Eles podem enfrentar uma série de dificuldades para compreender o contexto e as necessidades específicas dos seus clientes. Trazer clareza quanto às capacidades das novas tecnologias, às aplicações apropriadas no negócio e aos riscos associados, é especialmente importante para as tecnologias emergentes e rodeadas de *hype*. Tendo os robôs de software as opções de implementação disponíveis para uma organização que implementa RPA semelhantes às de qualquer outro software (por exemplo, um sistema ERP), os *managers* têm de decidir se implementarão RPA *on-premises*, na *cloud* ou de forma híbrida.

O foco na modelação e na descrição dos processos, também, é uma fase inicial chave [35], já que a RPA é construída com base em regras precisas. A seleção do processo necessita de se concentrar naqueles que estão especificados com precisão. Um dos desafios mais importantes reside na identificação dos processos adequados para a automação RPA [36]. É crucial selecionar um processo apropriado para automatização, de modo a evitar o aumento da ineficiência e as falhas [37]. Com o objetivo de determinar processos adequados para a automatização, é

necessário estabelecer critérios que auxiliem a reconhecer a elegibilidade de um processo para RPA.

4.3.3. Eficácia na transferência da responsabilidade dos utilizadores, em *compliance* da segurança da informação, para os robôs/*bots*

A incorporação da RPA torna necessária a adaptação ou criação de novas políticas a serem integradas na política do *Business Continuity* [4]. As organizações devem documentar todas as políticas e processos, assim como, disponibilizar essas informações, centralmente, para que possam ser usadas na autoaprendizagem e na formação dos colaboradores.

Segundo o estudo publicado por Perdana *et al.* [24], 92% dos entrevistados sentiram que a conformidade melhorou após a implementação da RPA nas suas tarefas de negócio. Os funcionários entrevistados no estudo de Zhang *et al.* [25], também, afirmaram estar cientes de que a RPA é uma tecnologia baseada em dados que têm implicações na privacidade e segurança dos mesmos. Numa das entrevistas foi expressamente referido que o desenvolvimento e produção de robôs RPA tinham de cumprir os padrões do Regulamento Geral de Proteção de Dados (RGPD). Foi, também, relatado que, em algumas implementações, embora houvesse consciência da importância de manter a privacidade e a segurança dos dados, ocorreram violações de dados e foram implementados procedimentos de conformidade de forma reativa após os incidentes. Isto destaca a necessidade de considerar cuidadosamente os efeitos da RPA nos dados sensíveis e revela falhas na transferência da responsabilidade dos utilizadores em *compliance* da segurança da informação para os robôs [25]. Além disso, alguns entrevistados das implementações estudadas indicaram que a má comunicação durante a fase de desenvolvimento do *bot* causou a violação de segurança de dados mencionada anteriormente.

Uma das conclusões do estudo "*Security by envelopment – a novel approach to data-security-oriented configuration of lightweight-automation systems*" [16] revelou que os softwares robôs RPA operam de maneira *"mindless"* e são incapazes de avaliar e salvaguardar dados sensíveis durante as suas interações com sistemas organizacionais, aumentando os riscos de exposição de dados.

Outra evidencia da eficácia da transferência da responsabilidade ficou patente nos resultados das implementações RPA apresentados no estudo "*Roadmap for*

the implementation of robotic process automation in enterprises" [32]. Verificou-se, por exemplo, no caso da Agência Colombiana de Hidrocarbonetos (CARL), que o robô responsável por ajustar os preços do petróleo para *royalties*, durante o processo de compra pela CARL, para além dos benefícios apresentados (em disponibilizar informação em tempo real), garante precisão no cálculo dos preços do petróleo. Isto significa maior integridade com impacte financeiro na organização, proporcionando, assim, maior precisão no pagamento dos *royalties* à Agência.

4.3.4. Auditar a conformidade de segurança dos processos RPA recorrendo a robôs auditores

A solução para mitigar riscos em RPA deve seguir um programa de governança rigoroso [2] e as regras e controlos de auditoria devem ser definidas corretamente [3]. A implementação de programas de automatização de processos utilizando RPA leva à exposição a riscos elevados em comparação com processos típicos de automação de TI. Ao analisar alguns casos numa perspetiva de auditoria, descobriu-se que há mudanças claras no risco do processo após a automatização das diferentes funções de trabalho impactando na segurança de acesso, por considerações relacionadas com a mudança de aplicações e na estratégia de governança do ambiente RPA. Em ambientes mais complexos, auditar estas tecnologias emergentes torna-se mais exigente que numa auditoria tecnológica regular [3]. Ou seja, para reduzir as ameaças, a supervisão regular e a manutenção dos registos de auditoria relativos à atividade dos *bots* devem ser realizadas [24], para verificar se esses mesmos *bots* estão a operar dentro de um qualquer conjunto de regras pretendido e pré-definido.

A *Digital Operational Resilience Act* (DORA) é um exemplo da realidade concreta sobre preocupações legais aplicadas às instituições financeiras [3]. Esta aponta a necessidade de encontrar e implementar controlos automatizados e mecanismos rápidos e flexíveis para auditar, relatar e partilhar informação. Assim como, monitorizar as organizações para que os seus fluxos de trabalho, de dados e de informação possam ser compreendidos.

Perdana *et al.* [24], também, estudaram os benefícios, desafios e oportunidades para automatização das auditorias. Do resultado da interação com o pessoal e com as equipas de auditoria sénior, durante o curso das várias implementações RPA,

todas as empresas envolvidas sentiram que o tempo investido na aprendizagem de RPA valeu a pena, com os benefícios (especialmente poupanças a longo prazo) a excederem claramente os custos. Portanto, como descobertas deste estudo refere-se, principalmente, um primeiro passo bem-sucedido na direção da defesa da implementação de RPA em maior escala para cenários de auditoria mais abrangentes.

Ao implementar a RPA, os auditores também podem poupar tempo no seu trabalho, uma vez que elimina a necessidade meticulosa de ter de reconciliar fisicamente documentos [38]. Como resultado, pode ser gasto mais tempo na concentração em tarefas de auditoria de maior risco. Isto pode, igualmente, aumentar a produtividade e a eficiência dos auditores nas suas tarefas, reduzindo assim a probabilidade de terem de trabalhar horas extras e o problema de rotatividade associado. Além disso, os erros humanos podem ser minimizados [39], o que impactará positivamente na produtividade e eficiência [40]. No final, melhora a eficiência quando o trabalho necessário para executar uma análise pode ser feito por uma aplicação de teste automatizada num período muito menor, economizando assim valiosas horas de trabalho.

Para reduzir tal ameaça, a supervisão regular e a manutenção de registos de auditoria relativos à atividade do *bot* devem ser realizadas para verificar se os *bots* estão a operar dentro de qualquer conjunto de regras pretendido.

Finalmente, a utilização da RPA pode permitir aos auditores aprender novas competências de valor acrescentado. Com o advento de tecnologias disruptivas, muitos dos empregos existentes serão transformados à medida que a automatização se consolidar [41].

4.4. Discussão

Da revisão da literatura publicada identificou-se informação muito relevante que respondeu às questões de pesquisa. O estudo revelou que os impactes negativos, riscos e desafios na implementação de RPA estão muito ligados à manutenção da *compliance* da segurança da informação. Estes riscos emergem sobretudo das ameaças ligadas a ataques cibernéticos. O estudo confirmou que estas ameaças

podem aproveitar sobretudo as novas vulnerabilidades técnicas decorrentes das novas tecnologias e das arquiteturas RPA. Outra fonte de risco passa pelo uso e registo de credenciais dos utilizadores para a realização das tarefas na RPA, assim como, o uso de acessos privilegiados, a configuração do acesso a recursos de informação, a movimentação de dados sensíveis entre aplicações e a salvaguarda de informação e código fonte em novos repositórios.

Por outro lado, as preocupações por alguma falta de cumprimento dos requisitos legais, em implementações de RPA, foi outra das evidências encontradas na LSR.

A necessidade de melhorar o foco na governança de soluções RPA, como a gestão de alterações, planos de BC, gestão de capacidade e disponibilidade e gestão de configurações, é outra das conclusões do deste estudo. Importa referir que essas melhorias não devem comprometer a eficácia e eficiência das soluções RPA nem, consequentemente, das próprias organizações.

Por fim, ficou patente a necessidade de auditar regularmente as soluções RPA de forma automatizada, sendo a própria RPA uma solução possível e vantajosa. Isto porque, revelou o estudo, a RPA aumenta a eficiência e reduz o erro. O benefício em usar arquiteturas *cloud* para a implementação de RPA, sobretudo para a escalabilidade da solução, foi outra das evidências, assim como os riscos daí provenientes para a segurança da informação.

5. Problema e Proposta de Investigação

Este capítulo enquadra-se nas fases de Identificação do Problema e Motivação e na Definição dos Objetivos da metodologia DSR, onde se define a questão central da investigação e se justifica a necessidade do desenvolvimento do artefacto “Robô Auditor”. No capítulo anterior, foi realizada uma revisão sistemática da literatura. Esta incluiu a análise do impacte da RPA na segurança da informação, os desafios e riscos da sua integração, a redistribuição das responsabilidades de conformidade para os robôs e a viabilidade da auditoria automatizada da conformidade de segurança dos processos RPA. A discussão desses temas permitiu identificar lacunas e oportunidades de investigação, evidenciando a necessidade de uma solução automatizada que suporte a auditoria de conformidade da segurança da informação em ambientes com RPA. Neste capítulo, é formulado o problema de investigação com base nessas lacunas, demonstrando as limitações do processo manual de auditoria e a necessidade de uma abordagem automatizada. São definidos os objetivos da pesquisa e é apresentada uma proposta inovadora para o desenvolvimento de um Robô Auditor, capaz de melhorar a eficiência, precisão e segurança da auditoria de conformidade com a norma ISO 27001:2022.

No cenário atual de crescente adoção de RPA pelas organizações, impulsionada pela procura de eficiência operacional, surge a necessidade crítica de estabelecer governança para garantir a conformidade com padrões específicos, nomeadamente, na área da segurança da informação. Em concreto, é essencial garantir o cumprimento dos controlos para mitigar os problemas identificados na SLR realizada, em conformidade com a norma ISO 27001:2022. Esta norma define requisitos essenciais para a implementação de um sistema de gestão da segurança da informação (ISMS) e pode ser de cumprimento obrigatório para organizações certificadas neste referencial.

A ausência de uma abordagem sistematizada para governar a implementação e operação de processos RPA em conformidade com a ISO 27001:2022 representa um desafio significativo. A transferência de responsabilidade da segurança da informação, dos utilizadores para os robôs, durante a execução dos processos automatizados, cria novos desafios e maior complexidade, exigindo-se uma abordagem estruturada que equilibre segurança e eficiência operacional. À semelhança de

outros domínios, onde a falta de métodos e métricas específicas impactou na eficiência e eficácia, a governança em RPA, também, enfrenta desafios semelhantes.

Em suma, esta investigação aborda a ausência de um *framework* específico para garantir a segurança no desenvolvimento e implementação de robôs/bots, com ênfase nos controlos referidos no Anexo A da norma ISO 27001:2022. Neste conceito de *framework* inclui-se a capacidade de auditar, de maneira eficiente, a conformidade de segurança e a transferência de responsabilidade dos utilizadores para os robôs de RPA.

5.1. Motivação da Pesquisa

A motivação desta pesquisa reside na necessidade urgente de desenvolver uma abordagem sólida para governar a RPA, assegurando a conformidade com a ISO 27001:2022 e gerindo de forma eficaz os custos associados à validação e manutenção dessa conformidade. Ou seja, a principal motivação desta pesquisa é projetar e implementar um artefacto inovador de TI que permita auditar e avaliar a eficácia e eficiência da transferência da responsabilidade de segurança dos utilizadores para os robôs implementados numa organização e desta forma contribuir para a redução do risco do negócio. Esse artefacto, denominado Robô Auditor, é concebido para garantir a conformidade contínua com os requisitos de segurança estabelecidos pela norma ISO 27001:2022 e pelas políticas de segurança em vigor na organização e no total cumprimento da privacidade dos dados.

Esta motivação surge também da necessidade de fornecer conhecimentos valiosos para as organizações que procuram uma integração segura e eficiente da automatização robótica nos seus processos operacionais. Além disso, o facto de ser essencial assegurar que a transferência da responsabilidade dos utilizadores para os robôs ocorra de forma eficaz, mantendo continuamente a conformidade com os padrões de segurança estabelecidos, reforça, também, a relevância desta investigação. Paralelamente, os custos associados à validação e manutenção da conformidade em ambientes de RPA evidenciam a urgência de soluções mais eficientes.

Perante estes desafios, identificaram-se diversos *drivers* motivacionais que impulsionam esta pesquisa e justificam a necessidade do Robô Auditor. Mas também

porque há uma série de outros fatores possíveis a serem considerados, para além da eficiência e da eficácia, porque a RPA afeta a motivação, criatividade e inovação dos colaboradores [42].

Estes *drivers* representam os principais fatores que motivam a adoção de uma solução automatizada para auditoria de segurança em RPA, garantindo conformidade contínua, otimização de processos e redução de riscos. Na figura 5.1 apresenta-se uma visão estruturada destes *drivers*.

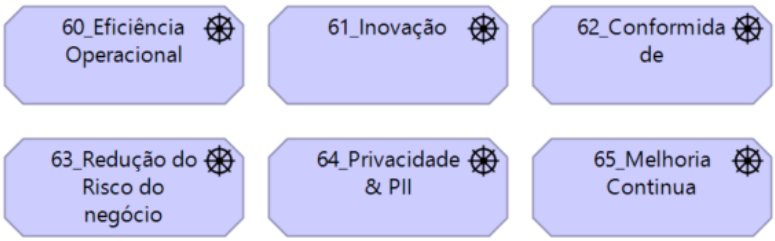


Figura 5.1-Drivers motivacionais para a implementação de um robô auditor.

5.2. Objetivos

Face aos desafios para garantir a conformidade contínua com os padrões de segurança estabelecidos em ambientes de RPA, surgiu a necessidade de desenvolver uma solução automatizada com capacidades de inteligência artificial para auditar de forma eficiente esses processos. O objetivo central desta pesquisa é projetar e implementar o Robô Auditor, um artefacto de TI inovador que assegure a conformidade com os requisitos de segurança da norma ISO 27001:2022.

O desenvolvimento do artefacto passa pela definição de objetivos claros, que envolvem tanto a análise do processo atual de auditoria de segurança, quanto a identificação de novos requisitos funcionais e operacionais necessários para a sua implementação. Tendo sido identificados os seis objetivos que se apresentam na figura 5.2.

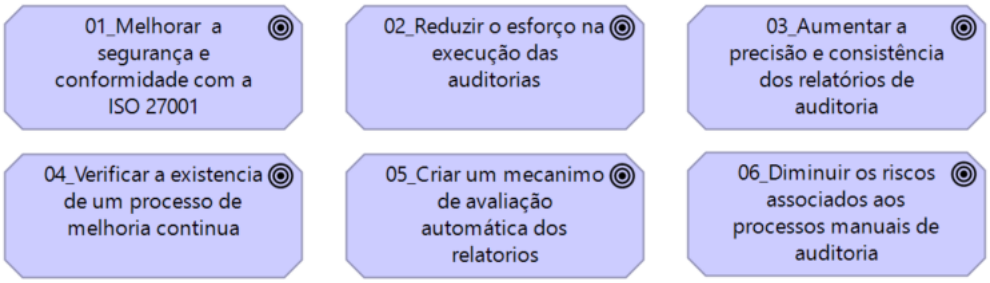


Figura 5.2-Objetivos motivacionais para a implementação de um robô auditor

A partir dos objetivos estabelecidos, é possível compor a lista de requisitos essenciais que sustentam o desenvolvimento do Robô Auditor, os quais visam não apenas otimizar o processo de auditoria, mas também garantir que o sistema atenda de forma eficaz às exigências e restrições necessárias para a sua operação. Para garantir o sucesso e a viabilidade do artefacto, é fundamental que o seu desenvolvimento siga parâmetros bem definidos, alinhando tanto aos objetivos da pesquisa quanto as necessidades operacionais e normativas. Na tabela 5.1 apresenta-se uma visão detalhada destes requisitos e restrições, abordando os objetivos normativos e de desempenho, assim como, as limitações técnicas e operacionais que devem ser atendidas para garantir a sua eficácia e integridade no contexto organizacional.

Tabela 5.1-Requisitos operacionais e restrições para o artefacto a desenvolver

Categoria	Requisito	Descrição	Tipo
Controlos do Anexo A da Norma ISO 27001:2022	Verificar a conformidade com os Controlos de Segurança	O Robô Auditor deve garantir a verificação da conformidade contínua com todos os controlos do Anexo A da ISO 27001, realizando auditorias regulares.	Quant.
	Avaliar o Risco de incumprimento da Conformidade	O Robô Auditor deve ter capacidades de inteligência artificial para avaliar o grau de conformidade de cada controlo.	Qual.
Orientações ISO 27002:2022 [43]	Validar a correta implementação dos Controlo de Segurança	O Robô Auditor deve validar a implementação eficaz das medidas de controlo recomendadas pela ISO 27002:2022	Qual.
	Avaliar a eficácia dos Controlo de Segurança	O sistema deve avaliar a eficácia das medidas de controlo implementadas, identificando se estão a cumprir os objetivos de segurança	Qual.
Políticas ISMS	Verificar a inclusão da RPA nas Políticas do ISMS	O Robô deve validar se as políticas do ISMS da organização contemplam a RPA	Qual.
	Verificação da Conformidade com as Políticas ISMS	O Robô tem de validar a conformidade das políticas e procedimentos da organização com os controlos da ISSO 27001:2022	Qual.

Categoria	Requisito	Descrição	Tipo
RGPD	As auditorias devem contemplar a validação da Conformidade com o RGPD	O Robô Auditor deve realizar auditorias automáticas para garantir a conformidade com o RGPD dos processos automatizados.	Qual.
	O Robô tem de cumprir com os requisitos RGPD	O sistema deve cumprir com os requisitos RGPD, protegendo os dados pessoais durante a execução das auditorias.	Qual.
Facilitador da Melhoria Contínua (PDCA)	Integração com o Ciclo PDCA	O Robô Auditor deve ser integrado no ciclo PDCA, promovendo a melhoria contínua do processo de auditoria e subsequente melhoria da segurança da organização	Qual.
	Aumentar as capacidades técnicas de Auditoria	O Robô Auditor deve incorporar novas funcionalidades visando à melhoria contínua do processo de auditoria	Quant.
Medição de Desempenho do Artefacto	Aumento da eficiência na realização das auditorias	O Robô Auditor deve reduzir em, pelo menos, 50% o tempo de execução das auditorias	Quant.
	Redução de FTE	O Robô Auditor deve reduzir em pelo menos 50% as horas de trabalho humano necessárias para a execução das auditorias.	Quant.
(Restrição)	compatibilidade tecnológica com *Uipath* & *intranet*	Utilização de *UiPath* para auditar em ambientes *windows* e na intranet da organização	
(Restrição)	Garantir Integridade dos dados de Auditoria	A solução de RPA deve ser limitada a capturar dados sem modificações, podendo ser necessário a implementação de mecanismos como *hashes* ou *checksums* para verificar a integridade dos dados durante o processo de auditoria	
(Restrição)	Restrição à Frequência e âmbito da auditoria	Frequência configurável e de âmbito ajustável para evitar sobrecarga dos sistemas e risco da criação de dados desnecessários.	

Os requisitos e restrições apresentados refletem os principais desafios e diretrizes para o desenvolvimento do Robô Auditor que serão explorados no capítulo seguinte.

6. Conceção e desenvolvimento

Este capítulo descreve a fase de Design e Desenvolvimento da DSR, que envolve a criação do artefacto Robô Auditor para automatizar o processo de auditoria interna ISO 27001:2022. No capítulo anterior, foram apresentadas as motivações, objetivos e requisitos da pesquisa, que delinearam o problema a ser resolvido com o desenvolvimento de uma solução automatizada. Neste capítulo, é apresentada a proposta conceptual para o desenvolvimento, seguida do levantamento detalhado do processo de auditoria interna ISO 27001:2022 e da seleção das atividades mais adequadas para a automatização. Serão, ainda, explorados os requisitos necessários para o funcionamento do artefacto, a arquitetura proposta para o sistema e os detalhes da sua implementação. Finalmente, o capítulo aborda a construção do protótipo, detalhando as etapas do desenvolvimento do artefacto que resultaram na solução final.

6.1. Proposta Conceptual para o desenvolvimento do artefacto Robô Auditor

A proposta conceptual aqui apresentada inicia-se com a explanação do processo identificado para a implementação do artefacto Robô Auditor. Esta, seguindo a metodologia da DSR e baseando-se, também, em estudos prévios, como por exemplo os de Hevner [44] e Peffers *et al.* [5], pretende garantir um processo que é consistente com os resultados da revisão de literatura e, por esta razão, será suficientemente robusto para servir como um modelo eficaz para futuras pesquisas na área do RPA aplicado a auditorias em SI. Guiada, também, por modelos mentais experimentados de como deve ser feita a investigação em ciência do design em SI, reflete na sua essência, o novo papel do auditor. Este será redirecionado e alterado, retirando-lhe as tarefas repetitivas de recolha e processamento de dados, para enfatizar principalmente a componente de avaliação dos procedimentos de auditoria. Para isso, foram consideradas, também nesta conceptualização, as fases principais recomendadas por Moffitt *et al.* [45] para a implementação de RPA a processos de auditoria:

- Que atividades de auditoria devem ser alvo de automatização?

- De que forma os procedimentos de auditoria podem ser repartidos em pequenas etapas adequadas para a automatização?
- Quais os procedimentos de auditoria que podem resultar em automatização?
- Estão os dados num formato legível para os sistemas RPA/máquinas?

Em resumo, a figura 6.1 apresenta um *framework* metodológico que integra as fases da DSR, com etapas preparatórias e complementares, estruturando a abordagem para o desenvolvimento e implementação do artefacto.

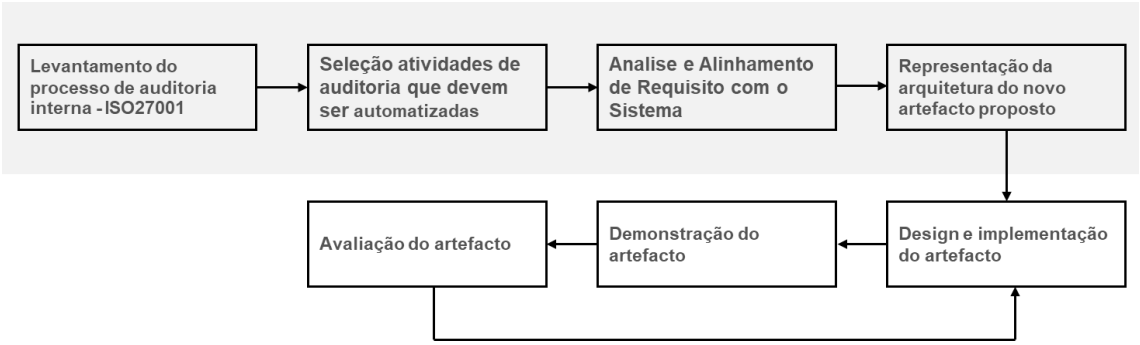


Figura 6.1-Proposta metodológica

Segue-se a descrição de cada uma das etapas apresentadas no *framework*, assim como os resultados esperados para cada uma delas.

Tabela 6.1-Sumário da metodologia conceptual

Etapa	Descrição	Resultados esperados
Levantamento do processo de auditoria interna – ISO 27001	Documentação do processo representando todas as tarefas e a sua descrição	Diagrama de casos de uso
Seleção das atividades de auditoria que devem ser automatizadas.	Organização por ordem decrescente de prioridade as tarefas identificadas na etapa anterior tendo em conta a facilidade de automatização e esforço manual necessário (repetibilidade) à sua execução	Lista das tarefas a automatizar.
Analise e Alinhamento de Requisito com o Sistema	Identificação dos requisitos funcionais e de domínio – controlos da Norma e políticas. Identificação dos requisitos de desempenho	*Viewpoint Archimate* de requisitos e lista de requisitos da norma ISO27001_AnexoA.xlsx
Representação da arquitetura proposta	Representação da arquitetura de alto nível e com enfase na motivação organizacional subjacente à criação do projeto.	*Viewpoints Archimate*
Design e implementação do artefacto	Modelação do processo a executar pelo robô e desenvolvimento do projeto de	Modelação BPMN do Robô auditor e projeto “Robô_auditor”

Etapa	Descrição	Resultados esperados
	automatização parcial das tarefas identificadas com recurso ao sistema *Uipath*	
Demonstração do artefacto	Execução e apresentação do artefacto aos vários *stakeholders*	Relatorio_auditoria.docx e vídeo demonstrativo. Tabela comparativa entre processo manual e processo automatizado.
Avaliação do artefacto	Realização de entrevista com *stakeholders* e recolha dos diversos inputs	Resultado da análise das entrevistas / *focus group* e conclusões

6.2. Levantamento do processo de auditoria interna - ISO27001

Para identificar quais as atividades passiveis de automatização fez-se o levantamento dos casos de uso no processo de auditoria interna da organização, com maior detalhe na fase de execução da auditoria e na respetiva verificação da implementação dos controlos do anexo A da norma ISO27001:2022. É nesta fase que se concentra o maior esforço manual na execução das atividades repetitivas e sem grande valor acrescentado.

Para melhorar este processo devem automatizar-se todas as tarefas manuais e repetitivas de baixo valor acrescentado, ou seja, eliminar a necessidade da intervenção humana nesta fase da auditoria. Simultaneamente, é necessário reduzir o tempo de execução das auditorias em, pelo menos, 50%, tornando o processo mais eficiente, com menor consumo de recursos humanos e maior fiabilidade nos resultados. Poder-se-á, ainda, recorrer a mecanismos de inteligência artificial para analisar os dados e auxiliar na avaliação automatizada da conformidade.

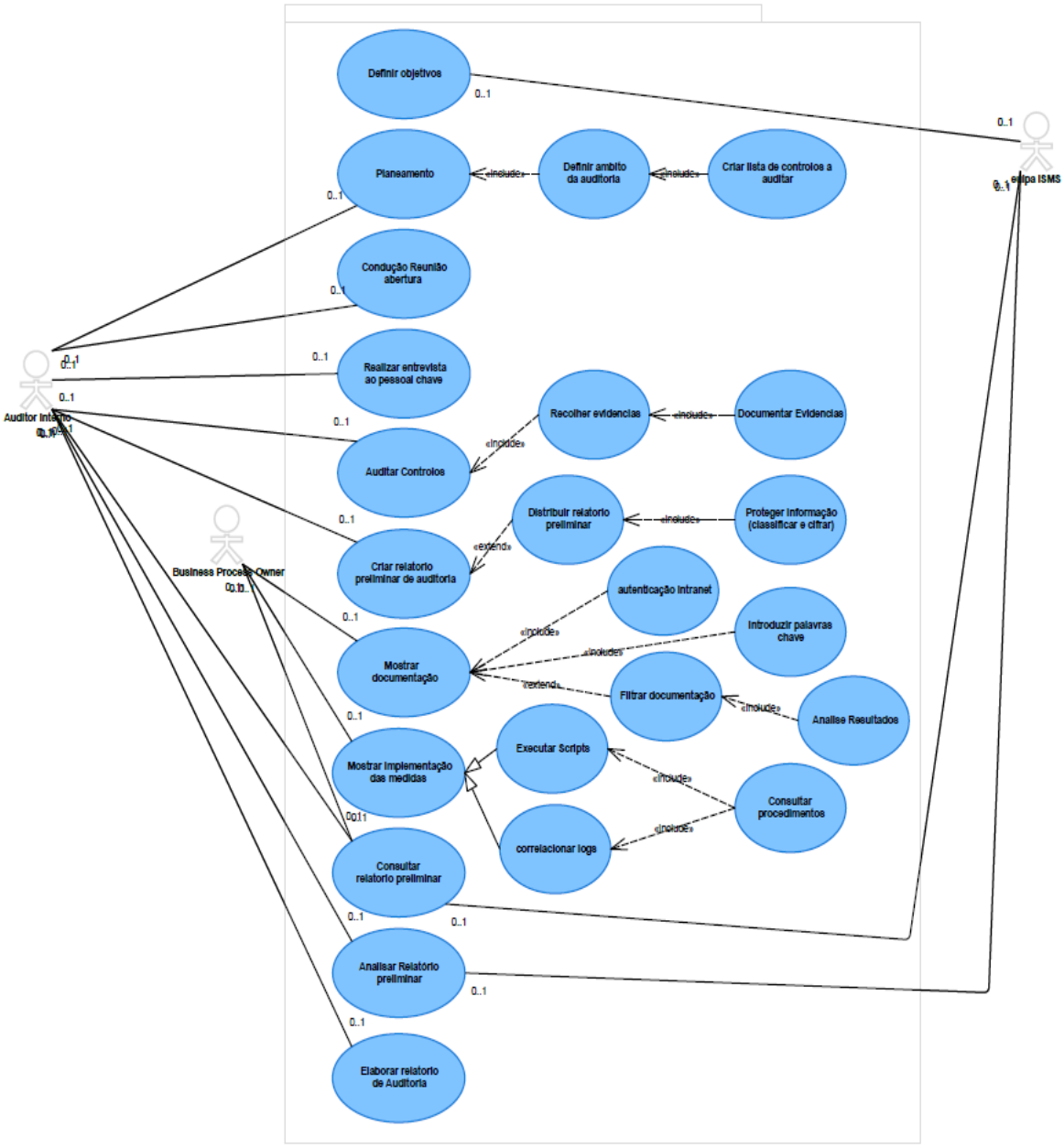


Figura 6.2-Casos de uso de uma auditoria interna na organização

6.3. Seleção das atividades para automatização.

Com base no impacte, em termos de ganhos de eficiência, que a automatização dos diferentes casos de uso teria no funcionamento da organização e na adequação das tarefas que compõem o processo de auditoria interna para serem automatizadas com RPA, elaborou-se a lista a seguir apresentada com os casos de uso prioritários, e respetivas tarefas, para o processo de automatização.

1. Auditar controlos;
2. Mostrar documentação;
3. Demonstrar implementação das medidas de controlo;
4. Criar relatório preliminar de auditoria interna.

6.4. Analise de requisitos

Os requisitos descritos nesta seção derivam das necessidades identificadas na seção 5.2, assegurando que a conceção da solução cumpre e responde aos objetivos estabelecidos no contexto do problema e da motivação da pesquisa.

O artefacto deve aceder à gestão documental na intranet e comparar os controlos da ISO 27001 e as orientações de implementação da ISO 27002 [43], com as políticas do ISMS em prática na organização. Deverá, ainda, criar um relatório preliminar que suporte a analise do grau de *compliance* na implementação dos controlos do anexo A da norma ISO27001:2022, complementando-o com as evidências da correta implementação das medidas de controlo. O artefacto terá de aumentar a eficiência na realização das tarefas manuais e, durante a execução destas, cumprir as regras de privacidade dos dados, de acordo com o regulamento RGPD. Deve permitir a sua instanciação, de acordo com as necessidades da organização, permitindo o aumento do número de auditorias e alguma agilidade na definição do seu âmbito, que deverá estar alinhado com as práticas organizacionais da melhoria contínua. Terá, ainda, de ser implementado em tecnologia *UiPath*. Na figura 6.3 estão compilados os requisitos, e restrições, de forma macro, que compõem a arquitetura do sistema.

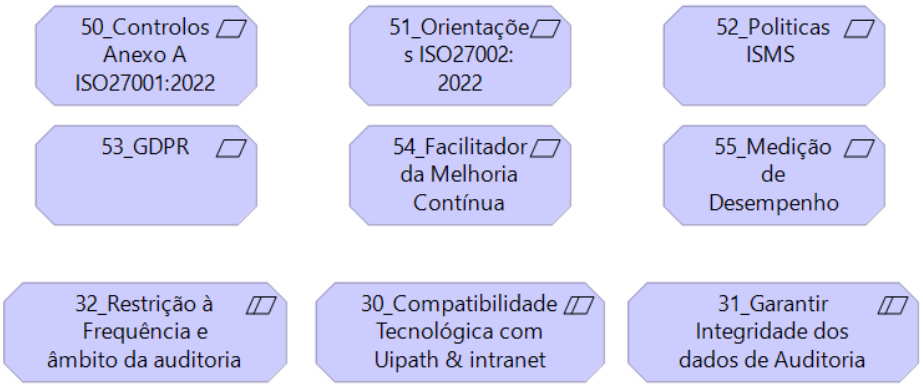


Figura 6.3-Requisitos e restrições de alto nível (Linguagem ArchiMate)

6.5. A Arquitetura proposta

Para estruturar e organizar a arquitetura de TI proposta, utilizamos o *The Open Group Architecture Framework* (TOGAF). Desta forma, fez-se uma abordagem sistemática para desenvolvimento da arquitetura alinhada com as metas gerais de negócios e garantindo a governança e o cumprimento dos objetivos organizacionais. A arquitetura apresentada situa-se ao nível estratégico e motivacional e está refletida no *viewpoint* motivacional de resumo (figura 6.4). Este, engloba as várias motivações organizacionais identificadas: **eficiência operacional**, maximizando o uso de recursos automáticos e reduzindo esforços manuais; **inovação**, com a adoção de tecnologias como RPA e inteligência artificial (AI) para impulsionar novos níveis de desempenho, promover a automatização inteligente com geração de *insights* e alavancar novos processos**; conformidade**, garantindo a aderência à norma ISO27001:2020 e politicas de segurança em prática nas organizações; **redução do risco do negócio**, protegendo ativos críticos contra ameaças e vulnerabilidades; **privacidade e proteção de PII**, assegurando a gestão ética e responsável de dados sensíveis; e **melhoria contínua**, que orienta a evolução sistemática das práticas e processos.

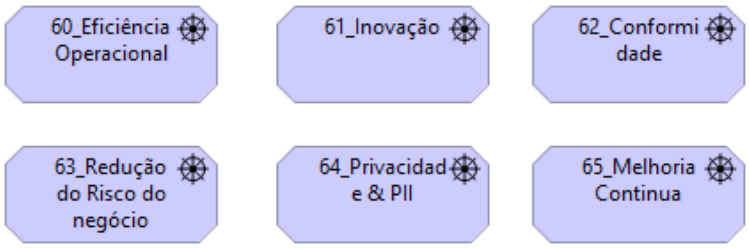


Figura 6.4-Motivações organizacionais identificadas na automatização de auditorias

Evoluiu-se, depois, para o detalhe representando-se os *viewpoints* motivacionais completos, elaborados em conformidade com o *framework* TOGAF *e* linguagem *ArchiMate* e com foco nos seus vários elementos e respetivas ligações. Estes, foram separados pelos diversos *stakeholders* identificados, apenas para simplificar a sua leitura e interpretação. Na conceptualização de exemplo apresentada na figura 6.5, onde é representado o *stakeholder Chief Information Security Officer* (CISO), percorrem-se os vários elementos chegando-se ao nível mais baixo (os requisitos) e explicitando-se a forma como estes elementos arquiteturais necessários se

devem ligar, que na prática representam a arquitetura desejável ao desenvolvimento do artefacto proposto. Os restantes diagramas que se aplicam aos demais *stakeholders* estão disponibilizados na sessão de anexos deste documento.

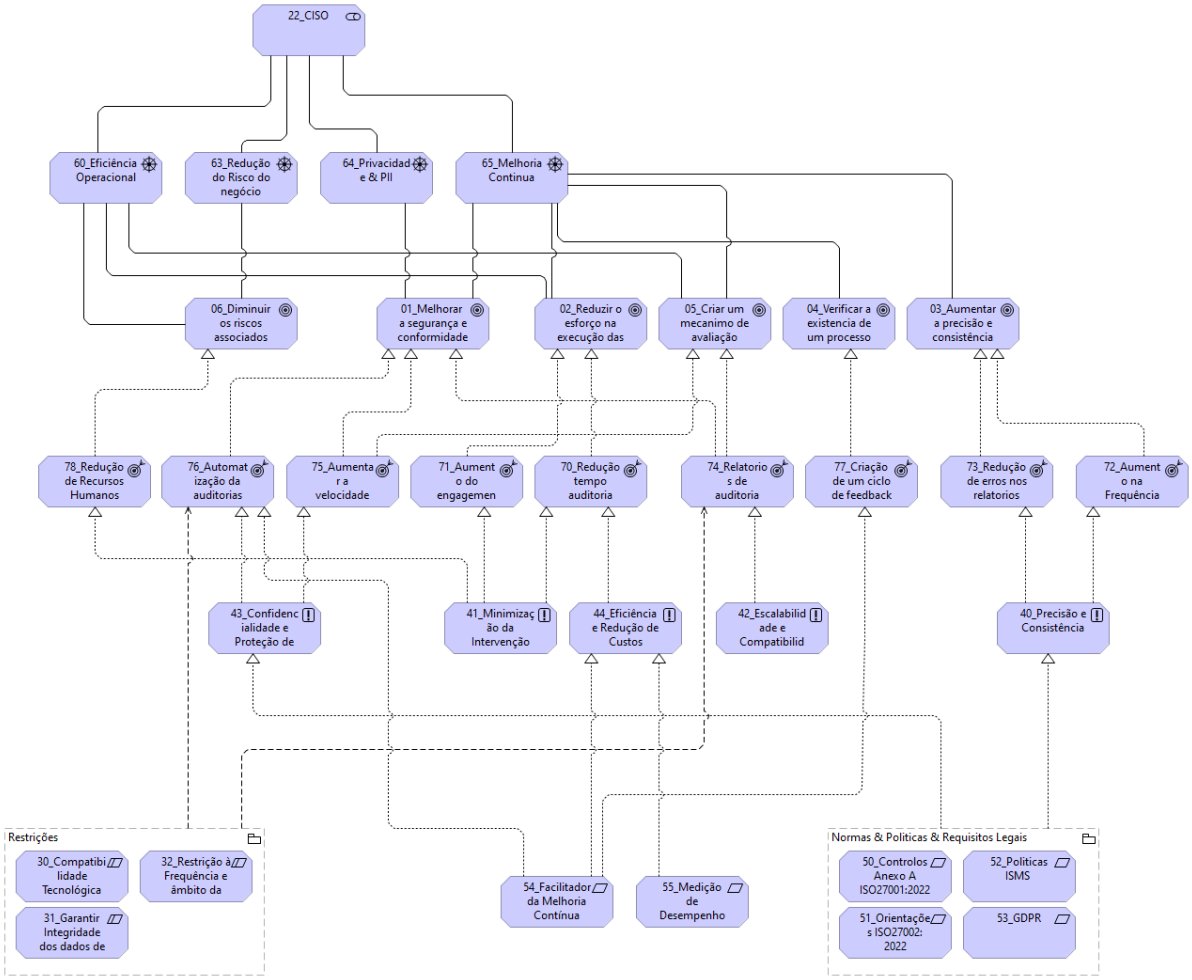


Figura 6.5-ViewPoint Motivacional para o stakeholder CISO (notação Archimate)

Para além dos requisitos, também as restrições foram tidas em conta, nomeadamente o facto de a solução proposta partir duma escolha prévia da tecnologia de RPA, o *Uipath*, pelo facto de esta ser líder de mercado e ser a que estava em implementação na organização onde se fez este estudo. Além disso, inclui os princípios e entregáveis, ou *outcomes*, que realizam os respetivos objetivos. Para garantir uma visão abrangente, os *viewpoints* motivacionais, correspondentes a outros *stakeholders* identificados, oferecendo uma análise completa das diversas perspetivas e expectativas que fundamentam o desenvolvimento da solução proposta**.**

6.6. Implementação do artefacto

Neste ponto é descrito o processo implementado de acordo com a proposta conceptual e suportado na tecnologia RPA para automatizar as tarefas repetitivas e de baixo valor acrescentado nas auditorias internas de segurança da informação, para a verificação da implementação dos controlos do anexo A da norma ISO27001:2022, assegurando maior eficiência e precisão. Na figura 6.6 mostra-se a modelação do processo principal que será instanciado em cada auditoria realizada pelo robô auditor e iniciado por agendamento.

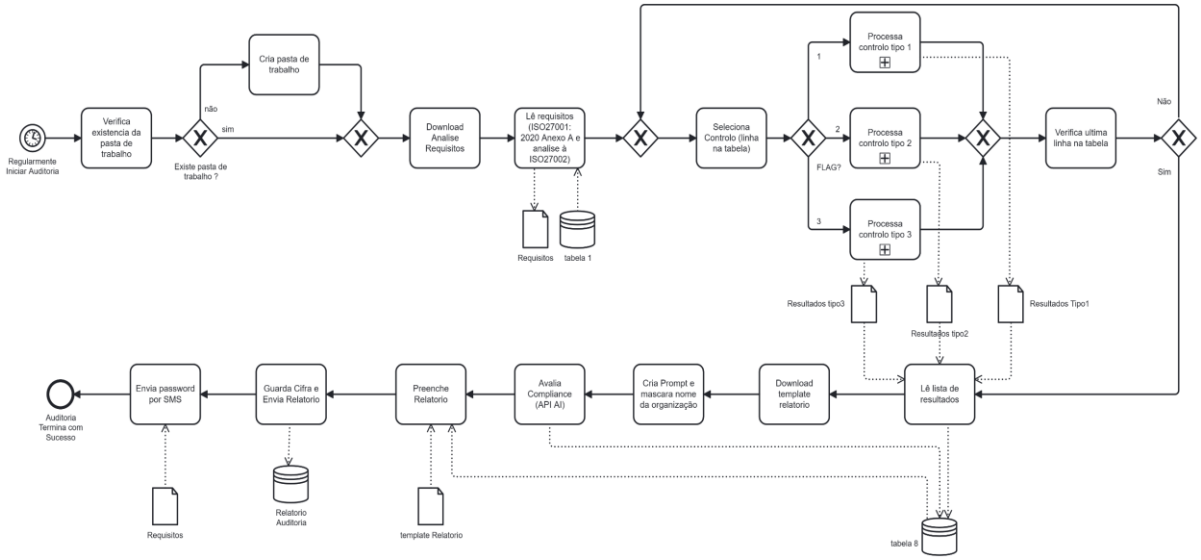


Figura 6.6-Robô Auditor - Modelação do processo principal (notação BPMN)

Esta implementação divide-se em três subprocessos, identificados com base na especificidade e tipo de tarefas a realizar e com o objetivo de aumentar não só a eficiência da tecnologia, mas também a rapidez de implementação da mesma, ou seja, procurar um melhor desempenho do sistema de informação (SI).

O subprocesso identificado como “Processa controlo tipo 1” e identificado na figura 6.7, realiza, com base nos requisitos normativos, as tarefas necessárias e repetitivas à recolha das evidências documentais existentes na organização, permitindo ainda a inclusão de uma lista de exclusões de documentos, que foi previamente elaborada com base na análise dos resultados de auditorias anteriores ou por indicação dos respetivos *stakeholders.*

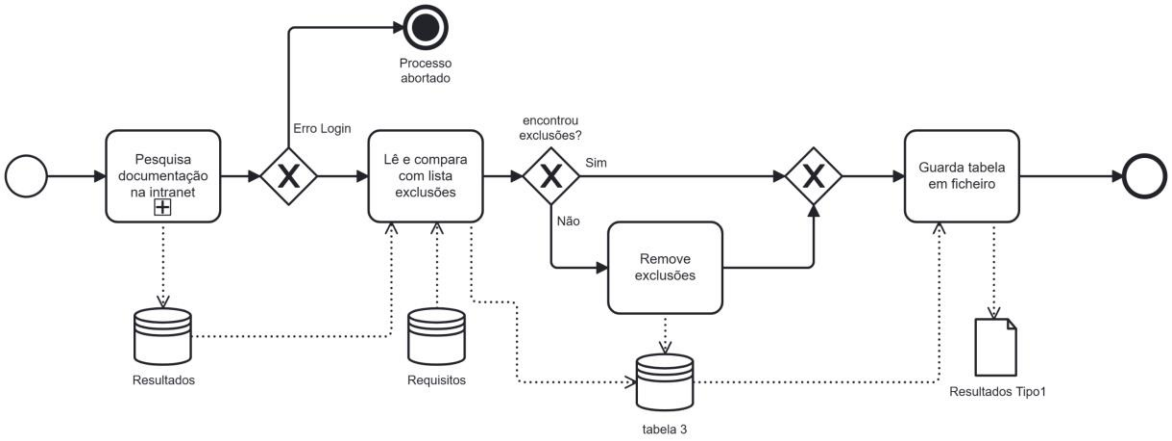


Figura 6.7-Robô Auditor - Modelação subprocesso controlos tipo 1 (notação BPMN)

Deste subprocesso fazem parte as atividades de pesquisa de documentação, comparação dessa pesquisa com os requisitos, exclusão de documentos do resultado da pesquisa, se aplicável, e salvaguarda dessa informação para construção do relatório preliminar de auditoria (tarefa essa pertencente ao processo principal). Por razões de eficiência operacional e agilidade na construção do artefacto, transformou-se a atividade de pesquisa (“Pesquisa documentação na intranet”), conforme modelo na figura 6.8, num subprocesso instanciado pelos 3 tipos de controlos como uma primeira fase que contempla o acesso e navegação na intranet.

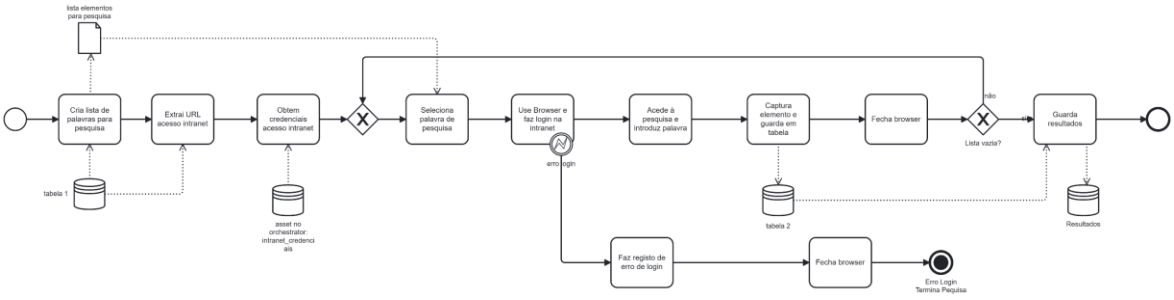


Figura 6.8-Robô Auditor - subprocesso para pesquisa na Intranet (notação BPMN)

O subprocesso “Processa controlo tipo 2”, desenhado na figura 6.9, difere do primeiro porque introduz tarefas que permitem complementar a recolha de evidências, validando a adequada implementação das medidas de controlo. Este subprocesso, aplicável a controlos mais técnicos, que para além de incluir as atividades de pesquisa de documentação comuns a todos os controlos, executa comandos *powershell* na infraestrutura tecnologia e de sistemas de informação para recolher *outputs* que complementam as evidências no relatório da auditoria.

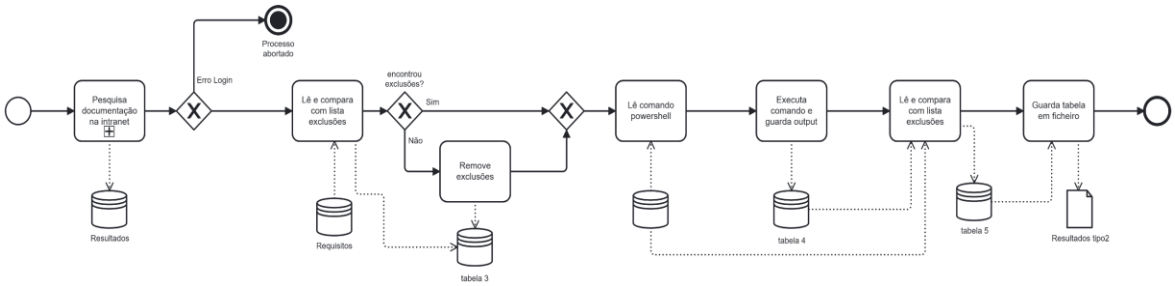


Figura 6.9-Robô Auditor - Modelação subprocesso controlos tipo 2 (notação BPMN)

A recolha e análise dos *logs*, referentes à execução dos processos automatizados na organização, foi incluída no subprocesso “Processa controlo tipo 3” e representado na figura 6.10. Esta é uma atividade relevante para validar a conformidade das medidas de controlo implementadas e associadas a alguns controlos do Anexo A da norma ISO27001:2022. Este subprocesso pode, por isso, ser instanciado quando se está perante a validação da conformidade dos controlos diretamente relacionados aos registos, ou *logs*, gerados pelos sistemas TI durante a execução dos vários processos automatizados. Estes *logs* são selecionados numa base temporal flexível, dependendo da periodicidade das auditorias ou outros requisitos do negócio.

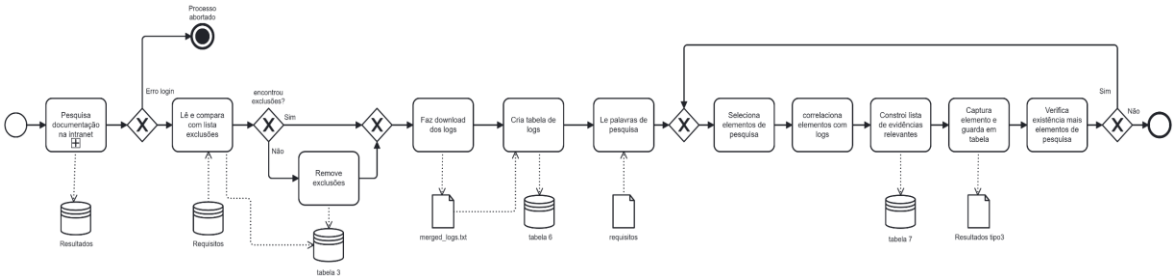


Figura 6.10-Robô Auditor - Modelação subprocesso controlos tipo 3 (notação BPMN)

A instanciação do processo principal ocorre periodicamente, de acordo com as necessidades, garantindo uma auditoria contínua e adaptável aos requisitos da organização. O fluxo BPMN ilustra todas as etapas principais, desde a ativação do robô auditor até o término do processo, que ocorre com a criação, cifragem e envio do relatório preliminar de auditoria às partes interessadas.

6.6.1. Parametrização e Configuração do Processo de Auditoria Automatizada

Antes da execução do processo de auditoria automatizado, é essencial dispor de uma peça de informação estruturada que enumere todos os controlos do anexo A da norma ISO27001:2020, assim como os critérios e parâmetros necessários para o funcionamento do robô de RPA. Para este fim, foi elaborado um arquivo Excel que serve como base de configuração dinâmica e ajustável, tipificando os controlos e permitindo gerir o âmbito de cada instanciação ou auditoria interna. Este documento, representado pela figura 6.11, contém os requisitos específicos de auditoria, como descrições detalhadas dos controlos a serem avaliados e palavras-chave para buscas automatizadas. Possui ainda, identificação das aplicações que servirão de fonte dos dados, critérios de validação e parâmetros para a execução de comandos ou *scripts* de suporte à realização das tarefas automatizadas, para além de critérios para a exclusão de documentos não pertinentes ao processo, que serão incluídos ao longo do tempo pelos auditores internos que utilizam o artefacto. Esta abordagem, e a sua flexibilidade, permitem que as regras sejam facilmente ajustadas, promovendo a escalabilidade e a adaptabilidade do artefacto a diferentes organizações ou cenários. Este documento, para além de suportar as atividades do robô, também, facilita a rastreabilidade e auditabilidade dos próprios critérios de auditoria, servindo como um ponto de referência para ajustes futuros e validações durante a execução do processo descrito no modelo BPMN. Tem, ainda, a lista de *stakeholders* para a distribuição automática do relatório.

A	B	F	G	H	I	J
#	ISO 27001:2022	FLAG	Sistemas	Palavras Chave	Medida	Comando Powershell
5.1	Policies for information security	1	https://tosrvvir2970.ad.huf/softexpert/login;https://hufglobal.sharepoint.com/:f:/r/sites/SGSIISMS/Freigegebene%20Dokumente/General/DOC?csf=1&web=1&e=hFN3hY	"Política de segurança da informação";"Política de Controlo";"Risk evaluation matrix";"Data Protection Policy";"user account privilege";"Tools and Scripts"		
8.17	Clock synchronization	2	https://tosrvvir2970.ad.huf/softexpert/login;https://hufglobal.sharepoint.com/:f:/r/sites/SGSIISMS/Freigegebene%20Dokumente/General/DOC?csf=1&web=1&e=hFN3hY	Stratum;"sincronização do tempo";"time protocol";NTP	Validação da configuração do serviço: NTP	w32tm

Figura 6.11-Visualização parcial do ficheiro Excel de requisitos e parâmetros

6.7. Construção do protótipo

A construção do protótipo foi concretizada na ferramenta *UiPath Studio* pelos motivos já apresentados no capítulo 3 e pelo facto da organização ter adotado recentemente esta tecnologia. A figura 6.12 mostra a lista de objetos criados no projeto *UiPath* que materializam o artefacto. Foram usados, também, recursos *Cloud*[4], nomeadamente, serviços disponibilizados na área da orquestração: *Assets; Store Buckets*, tornando a solução mais escalável, disponível e segura, conforme representados na figura 6.13.

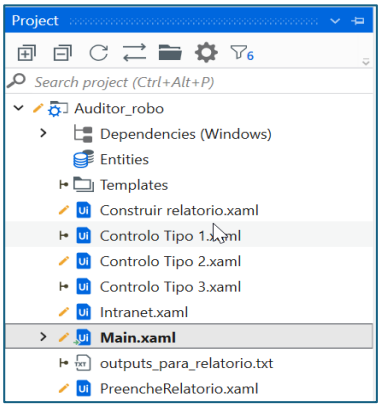


Figura 6.12 Workflows (UiPath Studio)

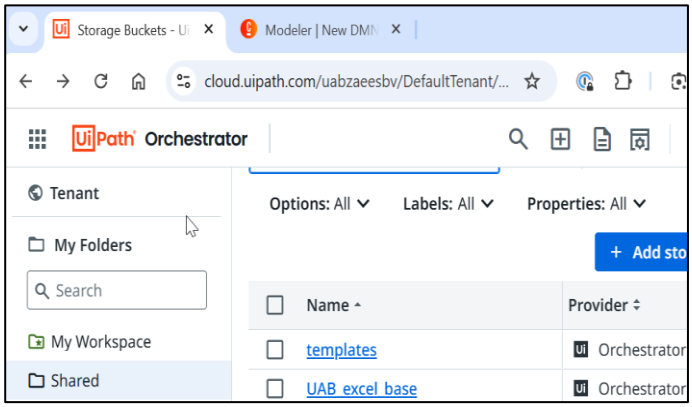


Figura 6.13 Store Bucket (UiPath Cloud)

No projeto foram utilizadas diversas atividades disponibilizadas pelo *UiPath*, desde a leitura e escrita em ficheiros Word e Excel, passando pela atividade de automatização do acesso e navegação na intranet com recurso ao *browser*. As atividades de registo de *logs* e de invocação de código permitiram, por um lado, adicionar metadados ao processo e por outro executar *scripts* para tarefas mais especificas como, por exemplo, a execução de comandos *PowerShell.*

Na Figura 6.14, é apresentada a atividade de “Autenticação integradaUI”, que faz parte do processo automatizado de login na intranet. Neste exemplo de fluxo, o *UiPath* utiliza atividades como “*Type Into*” para inserir as credenciais nos campos de Utilizador e Senha.

[4] https://cloud.uipath.com

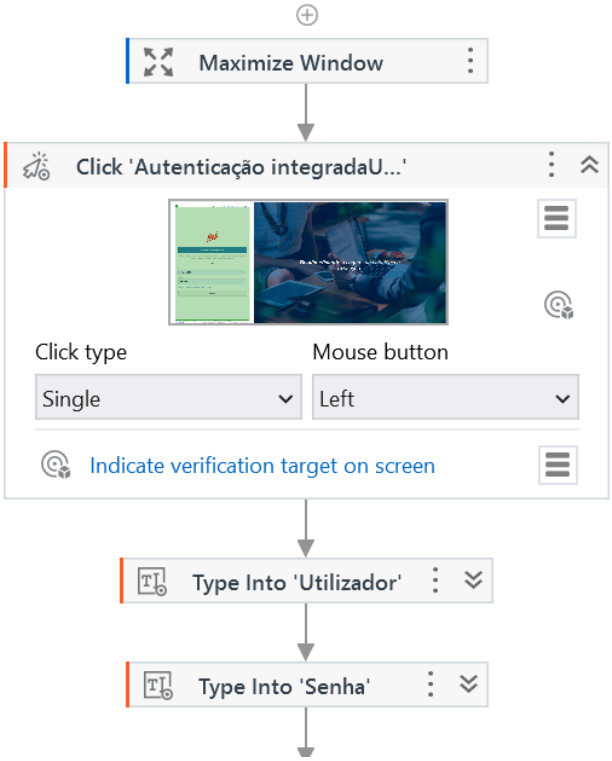


Figura 6.14-Atividades no projeto UiPath - Robô Auditor

Realizou-se, ainda, uma integração com a API da OpenAI para aprimorar [46] a avaliação de *compliance* dos controlos. Através de inteligência artificial criou-se um *score* de conformidade com base nas diretrizes da norma, partindo-se da lista de evidências de documentos recolhidos por cada controlo auditado. Para assegurar a anonimização dos dados, o processo de preparação do *prompt* passou por uma etapa de ofuscação do nome da organização. Finalmente, para o envio do relatório recorreu-se a algumas atividades de integração com sistemas externos *cloud*, por exemplo o "*Twilio*" para o envio de SMS, conforme se mostra na figura 6.15.

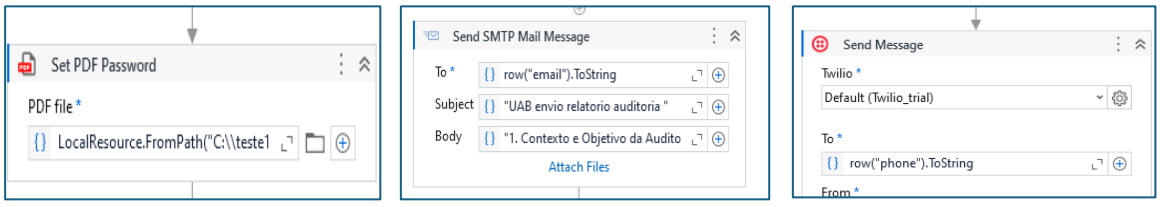


Figura 6.15-Exemplos de atividades de integração no projeto UiPath Robô Auditor

7. Demonstração do artefacto robô auditor

Este capítulo descreve a fase de Demonstração da metodologia DSR, na qual se apresenta a aplicação prática do artefacto desenvolvido, o Robô Auditor, no contexto de auditoria interna ISO27001:2022. No capítulo anterior, foi abordado o processo de Design e Desenvolvimento, que envolveu o desenvolvimento conceptual, o mapeamento do processo de auditoria e seleção das atividades a automatizar. Foram, ainda, detalhados os requisitos, a arquitetura e a implementação e construção do artefacto.

Desta fase faz parte a demonstração da aplicação do artefacto Robô Auditor no contexto de auditoria interna ISO27001:2022, e com ênfase na conformidade das soluções de RPA, na execução dos quatro casos de uso implementados: auditar controlos, mostrar documentação por parte do auditado, demonstrar a eficácia da implementação das medidas de controlo, e criar relatório preliminar de auditoria. A demonstração foi realizada utilizando o protótipo do Robô Auditor integrado nos sistemas IT em produção na organização.

Através desta demonstração prática, foi possível evidenciar as vantagens da automatização, não só em termos de eficiência, mas também em termos de precisão e segurança. Além disso, a demonstração incluiu a instanciação dos três tipos de abordagem à auditoria dos controlos de segurança definidos conceptualmente nesta investigação: controlo do tipo 1, que consistiu na recolha de evidências documentais, controlo do tipo 2, que requer tanto a recolha das evidências documentais quanto a validação da implementação técnica e controlo tipo 3, que envolve a recolha de evidências documentais juntamente com a análise dos *logs* da execução dos processos em RPA. Esta classificação foi um ponto crucial para otimizar, tanto a eficiência da implementação e desenvolvimento do artefacto, quanto a eficiência e eficácia do processo de auditoria.

Outro aspeto importante da demonstração está relacionado com a exposição dos mecanismos intrínsecos da solução *Uipath* para a verificação da segurança da informação.

Portanto, a demonstração da aplicação do Robô Auditor não expôs apenas os benefícios em termos de eficiência operacional e precisão, mas evidenciou também como a automatização pode melhorar a segurança e a qualidade dos processos de

auditoria de segurança. A seguir, são detalhados os resultados observados durante a demonstração dos quatro casos de uso implementados, em comparação com o processo manual existente.

7.1. Situação atual (Manual):

Na recolha das evidências o auditor, com a ajuda dos especialistas de TI ou responsáveis pelos processos (*process owners*), obtém manualmente os indícios de conformidade com os controlos de segurança. Isso envolve questionar o auditado e procurar, na aplicação de gestão documental, os vários documentos. Realizam-se, ainda, entrevistas e análises aos *logs* dos sistemas IT, recorrendo ao suporte de especialistas da área de IT.

Após a recolha das evidências, o auditor tem de as registar e compilar em documento preliminar de relatório da auditoria. Isso envolve o uso de vários ficheiros eletrónicos e a gestão dos mesmos. A recolha e documentação das evidências são demoradas e sujeitas a erros humanos, com baixa eficiência e alto risco de falhas na segurança dos dados. A avaliação da conformidade é feita no final de cada sessão e é incluída no relatório final.

Atores Envolvidos: esta atividade obriga à presença em sala de todos os elementos envolvidos na auditoria, com forte impacte na gestão dos recursos humanos da organização. Existe uma interação constante entre auditores, especialistas de TI e donos dos processos de negócio.

Tempo de Execução: Com base no histórico de relatórios de auditorias na organização verificou-se que o processo manual exige várias horas de execução. Cada controlo auditado consome em média mais de 20 minutos. Isto influência também, negativamente, a quantidade de controlos auditados, sendo estes repartidos por várias auditorias (âmbito da auditoria interna). Este processo manual de auditoria apresenta, também, alguma subjetividade e depende da proficiência e da disponibilidade da equipa envolvida. Está sujeito a erros na construção da documentação e cria algumas dificuldades de gestão da informação produzida. É, por isso, um processo ineficiente, levando a um uso intensivo de recursos e com limitação de escala.

7.2. Com a Automatização (RPA):

A recolha das evidências faz-se com acesso automático aos sistemas, assim como o seu registo e documentação. O processo é feito em tempo real e pode ser instanciado sempre que necessário. O robô executa a pesquisa nos documentos existentes na intranet e procura e analisa os *logs* do sistema RPA, com base no ficheiro de requisitos e parâmetros. Faz, ainda, a execução de *scripts* para comparar configurações de sistemas com os padrões de segurança estabelecidos pelos controlos e politicas de segurança. Não há necessidade de interação manual constante entre auditores e especialistas de TI ou os *process owners.*

O robô foi capaz de gerar automaticamente o relatório preliminar de auditoria com as evidências recolhidas. Inclui, ainda, neste um score construído por AI e faz a sua distribuição automática e de forma segura. Todo o processo é feito numa duração média de um minuto por controlo, reduzindo-se significativamente o tempo de execução da auditoria.

O Robô demonstrou ser capaz de realizar todas as tarefas que o processo manual executa nesta fase e ofereceu, ainda, funcionalidades adicionais como foi o caso da capacidade de distribuir o relatório preliminar de forma automática e segura.

Na criação do Score de conformidade recorrendo a AI, verificou-se, conforme demonstra a figura 7.1, que a média de *tokens* por controlo é inferior a mil. O que nos permite demonstrar, aplicando os valores da tabela 7.1, que o uso desta tecnologia tem um custo aproximado de 0,20 € por auditoria, quando aplicável ao total dos 93 controlos do anexo A da ISO27001:2022, usando o modelo GPT-3.5.

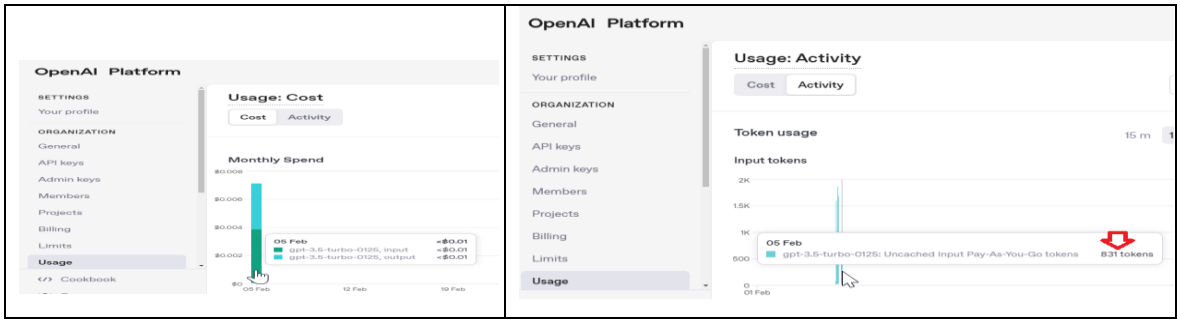


Figura 7.1-Plataforma Open AI, uso e custos, conta pessoal utilizada

Tabela 7.1-Demonstração dos custos do uso da API OpenAI

Modelo da OpenAI	Custo max. 1.000x93 tokens	Diferenças entre os Modelos
GPT-3.5	€0,188	Modelo mais barato, adequado para tarefas gerais de processamento de linguagem natural. Suporta até 4.096 tokens.
GPT-4 (8K)	€2,82	Modelo mais avançado que suporta até 8.000 tokens, ideal para tarefas mais complexas.
GPT-4 (32K)	€5,64	Modelo mais poderoso, suportando até 32.000 tokens. Ideal para grandes volumes de dados ou diálogos longos.

Da demonstração, podemos concluir que, na dimensão da funcionalidade, o protótipo apresentou um elevado nível de adequação, pois adaptou-se facilmente às atividades requeridas e mostrou um alto grau de flexibilidade, especialmente na definição do âmbito e na recursividade das auditorias. Eliminou a possibilidade de erros humanos na recolha e documentação das evidências, assegurando que os dados fossem transcritos e registados de maneira correta e consistente. Durante a demonstração, o processo foi repetido diversas vezes e, em todas as execuções, obteve-se o mesmo resultado, reforçando a confiabilidade do sistema. Além disso, a integração com a API do *ChatGPT* permitiu a criação totalmente automatizada de um *score* de conformidade de cada controlo, utilizando a análise precisa e eficiente dos dados recolhidos. Essa automatização não só acelerou a avaliação, mas também eliminou falhas de interpretação que poderiam ocorrer em processos manuais, garantindo uma análise mais consistente e objetiva.

A segurança dos dados acedidos e tratados neste processo, também, foi garantida através do uso de recursos na *cloud*, com armazenamento e processamento seguro das informações. Os relatórios gerados são criptografados antes de serem enviados, assegurando a sua confidencialidade. Além disso, são gerados *logs* detalhados durante a execução dos processos em RPA, permitindo uma monitorização transparente e rastreável de todas as atividades realizadas.

O processo automatizado mostrou uma alta confiabilidade na execução das tarefas, garantindo consistência e precisão nos resultados. A usabilidade foi comprovada pela simplicidade do processo: o utilizador precisou apenas de criar um arquivo Excel com os parâmetros necessários e carregá-lo na *cloud* (orquestrador *Uipath*), tornando a operação acessível e direta. Além disso, a execução do Robô

é feita de modo não assistida (*unattended*), o que significa que o processo ocorre automaticamente, sem necessidade de monitorização ou intervenção humana.

Sobre a eficiência do processo, evidenciou-se um aumento significativo com a adoção do RPA. Enquanto o processo manual de auditoria exige várias horas de execução, demorando cada controlo mais de 20 minutos, o robô automatizou todas as tarefas, reduzindo o tempo (em 90%) e permitindo que se possa auditar mais controlos por auditoria. Além disso, o processo manual depende da interação constante entre auditores, especialistas de TI e *process owners*, tornando-o moroso e sujeito a atrasos. Com a automatização, essa necessidade diminui, permitindo que as equipas se concentrem em tarefas estratégicas. O robô também automatizou a distribuição segura do relatório preliminar. Verificou-se, portanto, que a solução é eficiente em tempo e custos.

Da demonstração do Robô Auditor concluiu-se que foi provada a eficácia da automatização no contexto da auditoria interna da ISO 27001:2022, evidenciando ganhos significativos em eficiência, precisão e segurança. Comparado com o processo manual, o RPA reduziu drasticamente o tempo de execução (em 90%), eliminou a necessidade de interação contínua entre auditores e especialistas de TI e garantiu maior consistência nos resultados. Além disso, a integração com a API do *ChatGPT* permitiu a avaliação automatizada da conformidade, assegurando objetividade e escalabilidade no processo.

A demonstração validou ainda a capacidade do Robô Auditor em cumprir os requisitos funcionais e normativos definidos e de acordo com o descrito na figura 7.2. O artefacto foi capaz de auditar a aplicabilidade dos controlos do Anexo A da ISO27001:2022, verificar a sua implementação e garantir conformidade com as políticas do ISMS. Além disso, respondeu ao requisito de proteção da privacidade dos dados, em conformidade com o RGPD, e demonstrou ser um facilitador da melhoria contínua (PDCA), garantindo desempenho superior ao processo manual.

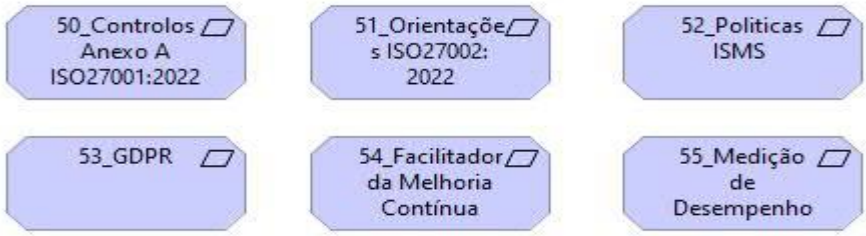


Figura 7.2-Requisitos de alto nível para o artefacto robô auditor (notação archimate)

A segurança da informação foi reforçada com criptografia de relatórios e monitorização detalhada através de *logs*. A abordagem não assistida (*unattended*) provou ser eficaz, tornando o processo mais ágil e reduzindo a dependência de recursos humanos. Assim, a demonstração validou a viabilidade do Robô Auditor como uma solução robusta para otimizar auditorias de segurança, assegurando maior confiabilidade, rastreabilidade e redução de custos.

7.3. Discussão

A implementação do Robô Auditor trouxe ganhos significativos em eficiência e abrangência, permitindo a verificação integral dos 93 controlos referidos no Anexo A da ISO 27001:2022 (sempre que pretendido) e reduzindo em 90% o tempo de execução. Além disso, a menor necessidade do envolvimento de recursos humanos tornou o processo mais ágil e flexível. A Tabela 7.2 resume as vantagens identificadas no uso da RPA no contexto da auditoria interna.

No entanto, a transição para a RPA exigiu a criação do ficheiro Excel com a lista de requisitos e parâmetros, conforme o previsto, mas obrigou a vários ajustes para resolver alguns dos problemas encontrados. Exemplo disso, foi a necessidade de ajustar a lista prévia de palavras-chave para pesquisa, associadas a cada controlo, para evitar demasiadas repetições e, desse modo, penalizar o desempenho da solução.

Outro desafio surgiu do uso recorrente da atividade *"Invoke Code"* no *UiPath*, que aumentou a complexidade da solução. Esta situação revelou-se um entrave à demonstração do artefacto, principalmente quando foram necessários ajustes na formatação do relatório, o que obrigou a alterações nos *scripts e,* consequentemente,

a um maior tempo gasto quando comparado com outros ajustes em atividades padronizadas (low code).

A adoção do modo incógnito do browser foi outra adaptação necessária, que solucionou problemas de interação do robô com a intranet devido ao armazenamento de sessões e cookies.

Tabela 7.2-Resumo das vantagens identificadas pelo uso da RPA

Processo atual de Auditoria	Auditoria com Robô Auditor	Vantagens
É criado um plano de auditoria, selecionando-se um conjunto reduzido de controlos a auditar, por motivos de agenda e tempo necessário à sua execução. Cada controlo necessita em média de vinte minutos (fonte: relatórios auditorias).	O âmbito é definido pela parametrização dos controlos a auditar na ferramenta, permitindo a inclusão ou exclusão de controlos conforme necessário. Cada controlo demora apenas dois minutos em média.	Não existe limitação à quantidade de controlos a auditar, podendo a auditoria interna incluir a totalidade dos 93 controlos do Anexo A da ISO 27001:2022. Redução em 90% o tempo de execução
Realiza-se a auditoria aos controlos do anexo A, em sala, com toda a equipa de auditoria (auditores; auditados; técnicos IT)	Execução automática e agendada da auditoria aos controlos do anexo A, sem necessidade de qualquer intervenção humana.	Redução de FTEs, libertando os recursos para tarefas de maior valor. Validação do grau de *compliance* por mecanismos de AI.
A presença e disponibilidade de especialistas de TI na auditoria é obrigatória	Os especialistas IT são apenas envolvidos no desenvolvimento e parametrização do robô	Redução da equipa de auditoria, com aumento da flexibilidade e capacidade para realizar auditorias na organização
O relatório de auditoria é construído e distribuído pelo auditor	Relatório automático, cifrado, e enviado por email para os interessados, sendo a chave de encriptação distribuída por SMS e guardada num cofre digital seguro	Maior rapidez, garantindo-se que os interessados recebem de imediato e, de forma segura, o relatório da auditoria
O processo de auditoria interna ocorre anualmente	Pode instanciar-se o processo de auditoria sempre que necessário e de forma periódica.	Passagem de uma visão da conformidade no momento da verificação para uma conformidade em tempo real, reduzindo riscos de não conformidade ao longo do tempo.

8. Avaliação

Este capítulo descreve a fase de Avaliação da metodologia *Design Science Research*, na qual se realiza a análise crítica do artefacto desenvolvido, o Robô Auditor, com base nos resultados obtidos durante a sua demonstração. No capítulo anterior, foi apresentada a Demonstração do artefacto, incluindo a sua execução prática e a análise do seu desempenho em comparação com o processo manual de auditoria. Neste capítulo, será realizada a Avaliação do Robô Auditor, focando-se na análise de sua eficácia, eficiência, confiabilidade e segurança.

8.1. Introdução, objetivos e métodos utilizados

Nesta seção descreve-se a forma como a proposta de investigação foi avaliada. Sendo o processo de avaliação fundamental para assegurar a eficácia do sistema proposto, ou seja, de que forma o artefacto suporta uma solução para o problema [47]. Este processo corresponde à fase de avaliação da metodologia DSR sendo delineado com base em princípios metodológicos previamente discutidos e adaptados ao contexto específico do desenvolvimento de um artefacto, o robô auditor, para garantir a conformidade de segurança da informação em ambientes RPA.

A avaliação surge como uma temática crucial tanto na investigação geral em SI como na DSR e está sujeita à dicotomia entre positivismo e interpretativismo. Enquanto o paradigma da ciência do comportamento procura descobrir "o que é verdadeiro", o paradigma da ciência do design procura criar "o que é eficaz". Por isso, vários autores defendem a necessidade de ambos os paradigmas garantirem a relevância e efetividade da pesquisa em SI, especialmente devido à natureza artificial das organizações e sistemas de informação [6].

Na literatura geral de SI, a avaliação é, geralmente, considerada a partir de uma de duas perspetivas. Na perspetiva “*ex ante*”, os sistemas, ou tecnologias candidatas, são avaliados antes de serem escolhidos e adquiridos ou implementados. Na perspetiva “*ex post*”, um sistema ou tecnologia escolhida é avaliada após ser adquirida ou implementada [47].

Esta avaliação, na pesquisa em DSR, também abrange duas abordagens fundamentais: a naturalista ou a artificial, conforme representado na figura 8.1. Sendo útil a sua distinção, pois existem vantagens, tanto na avaliação artificial, como maior

controlo e menor custo, quanto na avaliação naturalística, esta com mais realismo [47]. A abordagem naturalista implica avaliar o artefacto em cenários do mundo real, utilizando métodos empíricos, interpretativos e críticos. Neste contexto, Hevner *et al.* [6] destacam a importância da rigorosa avaliação de artefactos de design, apresentando cinco métodos distintos (observacional, analítico, experimental, testes e descritivo). Por outro lado, a abordagem artificial envolve cenários construídos, experiências e simulações, muitas vezes seguindo uma perspetiva positivista e reducionista. A escolha entre essas abordagens influencia diretamente na aplicabilidade dos resultados ao uso real do artefacto, e o *framework* proposto na DSR oferece uma visão estratégica para orientar tais escolhas, considerando os objetivos de pesquisa e as limitações específicas de cada estudo.

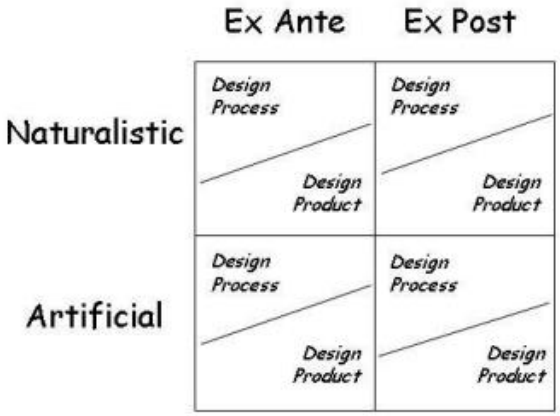


Figura 8.1-Strategic DSR evaluation framework [47]

Reconhece-se a importância de adotar uma abordagem abrangente na avaliação do artefacto desenvolvido neste estudo e, de acordo com exposto na figura 8.2, combinaram-se tanto elementos "*ex ante*" quanto "*ex post*". Na fase "*ex ante*", fez-se uma análise prévia do design do artefacto, considerando as necessidades operacionais, requisitos da ISO 27001:2022 e políticas de segurança da empresa. Isto permitiu estabelecer os fundamentos e requisitos antes da implementação e, dessa forma, avaliar antes de enfrentar os riscos e esforços de construir uma instância do artefacto.

Posteriormente, na fase "*ex post*", direcionou-se a avaliação para o artefacto em operação, utilizando métodos como a demonstração prática para avaliar a eficácia e a aceitação do Robô Auditor. A avaliação do Robô Auditor foi realizada por meio de entrevistas coletivas utilizando a técnica de *Focus Group*. Sendo o *Focus Group*

uma abordagem qualitativa, em que um grupo de especialistas discute de forma dirigida um tema específico, a mesma permitiu que cada participante expusesse a sua opinião e comentasse as opiniões dos restantes. Esta técnica favoreceu a exploração da compreensão subjetiva dos participantes num curto período de tempo, permitindo uma análise tanto individual quanto social sobre os desafios e impactos do artefacto. O objetivo foi obter uma visão mais ampla e detalhada sobre a eficácia do Robô Auditor na auditoria interna ISO 27001:2022, identificando pontos fortes, limitações e oportunidades de melhoria. A análise dos dados foi realizada com base no contexto da discussão, procurando interpretar as perceções e feedbacks dos especialistas.

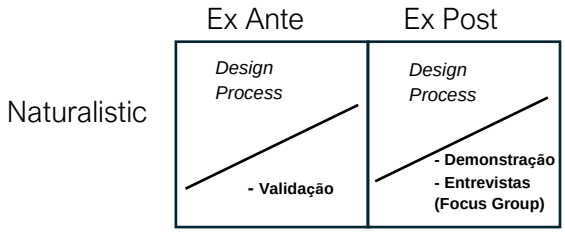


Figura 8.2-Dimensão e métodos aplicados, baseado em [47]

8.2. Seleção do *Focus Group*

A seleção do *Focus Group* para avaliar qualitativamente o artefacto Robô Auditor foi pensada para garantir uma análise holística e adequada à sua eficácia e efetividade [6]. O representante local do *Data Protection Officer* foi incluído devido à sua responsabilidade pela conformidade com as normas de proteção de dados, particularmente considerando os aspetos relacionados à segurança e privacidade de possíveis dados pessoais que o artefacto gera e utiliza. O *IT Manager* foi selecionado dado a sua visão estratégica e de supervisão sobre os recursos tecnológicos da organização, o que lhe confere uma perspetiva crucial para avaliar a escalabilidade, a integração do artefacto com a infraestrutura existente e a sua viabilidade operacional. Os auditores de segurança da informação, além de sua *expertise* na análise e mitigação de riscos e na conformidade com normas de segurança, onde se inclui a ISO 27001:2022 e o mecanismo TISAX, têm um papel fundamental na avaliação, visto que, na prática, serão os utilizadores diretos do artefacto. Estes auditores são também os principais beneficiários da implementação do artefacto,

pois ele facilitará as suas atividades de auditoria, tornando o processo mais eficiente e eficaz. Finalmente, os técnicos de TI que participaram da implementação foram incluídos devido ao seu conhecimento prático e profundo do processo de implementação, fornecendo uma visão realista sobre os desafios, dificuldades e resultados esperados na operação diária do artefacto. Esta seleção de *stakeholders* reflete também uma dimensão de avaliação naturalista, uma vez que a avaliação ocorreu num contexto real e prático de uso do artefacto.

Tabela 8.1-Caracterização dos elementos do Focus Group

Função	Experiência (anos)	Grau académico
Gestor IT	>20	Licenciatura
Gestor Eng. Operações	>15	Doutoramento
Auditor Interno	>20	Licenciatura
Auditor & Gestor Qualidade	>10	Licenciatura
Representante local. DPO	>10	Ensino Secundário
Auditor interno	>1	Licenciatura
Gestor operações e auditor IATF	>20	Licenciatura
Auditor	>10	Licenciatura

8.3. Planificação e condução do Focus Group

A constituição do *Focus Group* foi cuidadosamente planeada e é uma amostra representativa dos interessados na implementação e uso do artefacto, para garantir que a avaliação fosse ampla e eficaz. Os entrevistados incluíram o Encarregado de Proteção de Dados (DPO), o *IT Manager*, auditores de segurança da informação e técnicos de TI que participaram na implementação do artefacto. Cada grupo de participantes contribuiu com uma perspetiva específica sobre o artefacto, baseada na sua experiência direta ou no seu envolvimento nas operações da organização. Foi para isso criado um guião de perguntas direcionadas que abordassem questões de interesse no contexto da pesquisa:

Pertinência: Para entender a relevância do artefacto no contexto atual de segurança da informação e conformidade normativa. Questões relacionadas à pertinência ajudaram a avaliar a importância do artefacto de acordo com o conhecimento dos participantes sobre os desafios enfrentados na organização.

Utilidade: Pretendia-se avaliar se os *stakeholders* consideravam o artefacto útil nas suas atividades diárias, além de refletir sobre como ele atendia às suas necessidades específicas, como gestão da segurança e análise de conformidade;

Completude: A pergunta sobre completude foi usada para obter a opinião dos *stakeholders* sobre se o artefacto oferecia uma solução integral, que cobria todos os requisitos necessários para a execução de auditorias automatizadas e, desta forma, lidar com a segurança e a governança no contexto da organização;

Uso: As questões sobre a simplicidade de uso do artefacto procuraram identificar o quanto este é fácil de ser integrado e utilizado nas operações;

Melhorias: Cada entrevistado foi incentivado a fornecer sugestões e recomendações para melhorar o artefacto, numa ótica de identificar áreas em que o sistema poderia ser mais eficaz ou onde mais funcionalidades poderiam ser acrescentadas.

No guião, para além da apresentação dos objetivos do estudo, onde se incluiu uma execução do artefacto, foram incluídas as seguintes questões:

Tabela 8.2-Guia de questões para a condução da entrevista ao Focus Group

#	Area	Questão
Q1	Pertinência	Em que medida considera pertinente e/ou importante a existência do artefacto Robô Auditor agora proposto?
Q2	Pertinência	Que desafios atuais ou lacunas no processo de auditoria dos controlos do anexo A da ISO 27001:2022 acredita que o Robô pode ajudar a resolver ??
Q3	Pertinência	De que forma a adoção deste artefacto pode impactar positivamente na eficiência ou na qualidade dos processos na organização?
Q4	Utilidade	Na sua opinião o artefacto proposto será útil para a sua função? Porquê?
Q5	Utilidade	Que funcionalidades ou características do 'Robô Auditor' considera mais importantes para facilitar o trabalho dos auditores internos?
Q6	Completude	Em termos de completude, como classifica o Robô? Cobre os requisitos para a realização de auditorias internas aos controlos do anexo A da norma ISSO 27001: 2022?
Q7	Completude	Quais funcionalidades ou aspetos que considera ainda ausentes no 'Robô Auditor' para atender completamente às exigências das auditorias internas de segurança da informação?

#	Area	Questão
Q8	Uso	Considera simples utilizar o “Robô Auditor”? Consegue identificar as tarefas como potencialmente a mais complexa e a mais simples?
Q9	Melhorias	Que recomendações/sugestões indicaria de forma a ser possível melhorar o processo automatizado de auditorias de segurança da informação a sistemas IT (RPA)?
Q10	Melhorias	Na sua opinião, quais os aspetos do 'Robô Auditor' (ex.: interface, desempenho, integração com sistemas existentes) poderiam ser otimizados para melhorar a experiência dos utilizadores?
Q11	(Genérico)	Acha que o 'Robô Auditor' pode assegurar a privacidade dos dados gerados, acedidos ou manipulados, em conformidade com os regulamentos aplicáveis, como o RGPD? Identifica algum risco nesse sentido?
Q12	(Genérico)	Considera que o 'Robô Auditor' facilita o processo de auditoria, promovendo a melhoria contínua (ciclo PDCA) e oferecendo resultados significativamente melhores que os obtidos por processos manuais?

8.4. Resultados da avaliação

A adoção do Robô Auditor foi considerada altamente pertinente, especialmente com o crescente uso de soluções de RPA, permitindo que as empresas assegurem a conformidade das aplicações e direcionem os seus recursos para outras atividades estratégicas. O artefacto pode ajudar a colmatar lacunas no processo de auditoria dos controlos do Anexo A da ISO 27001:2022, automatizando a extração e comparação dos requisitos da norma, o que reduz a dependência do conhecimento técnico dos auditores humanos e possibilita auditorias contínuas, em vez de limitadas a períodos curtos. Considerou-se que a implementação do Robô Auditor contribui diretamente para a melhoria da qualidade dos processos organizacionais, garantindo um cumprimento mais rigoroso e eficiente dos requisitos de segurança. O artefacto será extremamente útil, pois oferece uma recolha contínua de evidências, ao contrário do modelo tradicional, proporcionando maior fiabilidade e consistência na monitorização da conformidade.

Entre as funcionalidades mais importantes já mencionadas, para os auditores internos, estão a automatização da extração e validação dos requisitos, a capacidade de realizar auditorias contínuas e a análise exaustiva de grandes volumes de dados. O Robô Auditor cobre os requisitos necessários para auditorias internas de segurança da informação, aos controlos do Anexo A da ISO 27001:2022. No entanto, seria útil que o artefacto fornecesse recomendações sobre políticas para

melhorar a conformidade, além de integrar KPIs, em vez de apenas um indicador geral. É essencial que, para além da automatização de muitos processos, algumas tarefas continuem a ser feitas ou monitorizadas por auditores humanos para evitar falhas que comprometam a auditoria.

A interação com o Robô Auditor é simples, mas o uso do Excel para parametrização pode limitar a sua aplicabilidade em diferentes ambientes. Este aspeto é uma área para aperfeiçoamento, a fim de aumentar a flexibilidade e a escalabilidade da solução. Além disso, ampliar o âmbito das atividades de auditoria automatizadas, como a seleção dos controlos a partir da leitura do plano de auditoria, seria uma melhoria importante para tornar o processo ainda mais eficiente. O robô evidenciou que para além de cumprir os requisitos RGPD, garante que os processos automatizados podem ser auditados nessa dimensão de forma mais eficaz.

Essas respostas demonstram que o Robô Auditor tem um grande potencial para transformar a auditoria interna de segurança da informação, tornando-a mais contínua, eficiente e eficaz.

9. Conclusão

Neste capítulo, são apresentadas as conclusões gerais da investigação, bem como as suas limitações e possíveis direções para trabalhos futuros.

9.1. Conclusões da pesquisa

Tendo em vista o desafio identificado – a necessidade de garantir a governança eficaz da RPA para assegurar a conformidade com os padrões normativos sobre segurança da informação – este estudo trouxe contribuições significativas para as organizações ao demonstrar como a automatização pode ser utilizada para validar, de forma eficiente e precisa, o cumprimento dos requisitos da norma ISO 27001:2022. Demonstrou, também, que a transferência da responsabilidade pela segurança dos utilizadores na execução dos processos pode ser delegada com eficácia à RPA, graças a esta nova capacidade de auditoria automatizada.

A partir da revisão da literatura sobre governança de RPA, conformidade e gestão da segurança da informação, foi possível propor uma nova abordagem que, para além de otimizar a verificação dos controlos referidos no anexo A da norma ISO 27001:2022, contribuirá para a redução do risco operacional associado ao não cumprimento da *compliance*. De facto, as evidências resultantes desta LSR forneceram uma base sólida para compreender o impacte da RPA na segurança da informação, revelando não só os benefícios da conformidade e da mitigação de riscos (RQ1), mas também os desafios inerentes à sua implementação (RQ2). Além disso, explorou-se a eficácia da transferência de responsabilidade dos utilizadores para os robôs (RQ3) e as metodologias para auditoria da segurança nos processos automatizados, incluindo o uso de robôs auditores (RQ4).

Esta investigação permitiu também compreender a importância de incluir os princípios de segurança da informação em todas as fases do processo de adoção da RPA, desde a análise e seleção dos processos a automatizar, até ao design, desenvolvimento e implementação dos robôs. Outra conclusão retirada está relacionada com o reconhecimento da falta de *frameworks* e métricas que garantam uma transição adequada da responsabilidade de segurança dos utilizadores para os robôs. Portanto, concluiu-se que nenhum trabalho científico previamente publicado abordou de forma objetiva a temática de estudo sugerida por esta investigação.

Com base nesses resultados, avançou-se para o desenvolvimento do artefacto protótipo – o Robô Auditor – que visou automatizar a verificação da conformidade em termos de segurança da informação em ambientes RPA, através da aplicação da metodologia *Design Science Research*. A arquitetura desenvolvida adotou uma abordagem estratégica e motivacional, visando o alinhamento com os objetivos estratégicos da organização e garantindo uma integração eficaz nos seus processos.

O protótipo do robô auditor foi desenvolvido na ferramenta *Studio X* da *UiPath*. Durante a sua fase de testes, o protótipo foi submetido a diversas execuções e ajustes, tendo sido posteriormente realizada a sua demonstração e avaliação. Esta, permitiu verificar se o artefacto atendia aos requisitos previamente estabelecidos, que estavam alinhados com os objetivos do estudo. A avaliação, realizada por *Focus Group*, destacou a pertinência da automatização na auditoria de segurança da informação, especialmente para os controlos do Anexo A da ISO 27001:2022, assim como, o grande potencial demonstrado ao permitir auditorias contínuas, reduzindo a dependência de conhecimento técnico dos auditores e melhorando a eficiência e consistência na monitorização da conformidade. As funcionalidades mais notadas foram a automatização da extração e validação dos requisitos, bem como, a possibilidade de análise de grandes volumes de dados. Outra das conclusões do estudo passou pela validação dos ganhos significativos de eficiência, com uma redução de 90% no tempo de execução da validação dos controlos (ver tabela 7.2) e uma diminuição de cerca de 92% no esforço humano (FTE), conforme anexo II.

9.2. Limitações da pesquisa

A conceção e execução deste estudo apresentam algumas limitações que, embora não comprometam a validade dos resultados obtidos, devem ser tidas em consideração em investigações futuras. Metodologicamente, a validação do artefacto Robô Auditor baseou-se exclusivamente num grupo de discussão (*Focus Group*) com especialistas de uma única organização, o que pode ter restringido a diversidade de perspetivas. Quanto ao âmbito, embora o protótipo seja aplicável aos 93 controlos do Anexo A da ISO 27001:2022, a sua demonstração e validação foi realizada com apenas 15% desses controlos, selecionados aleatoriamente. Esta limitação pode

restringir a avaliação da sua eficácia em relação aos restantes controlos e ao processo de auditoria como um todo.

Do ponto de vista tecnológico e prático, o artefacto foi testado com dados reais da organização, demonstrando um bom desempenho em termos de escalabilidade e integração com sistemas existentes. No entanto, a sua aplicação ficou limitada à auditoria do próprio Robô Auditor, sem avaliar outros robôs que executam diferentes funções dentro da organização.

9.3. Trabalho Futuro

Os resultados deste estudo abrem caminho para novas investigações, permitindo que pesquisas futuras avaliem a eficácia do Robô Auditor em diferentes contextos e explorem formas de melhorar as suas funcionalidades e aplicabilidade.

Uma possível evolução do artefacto poderá consistir no aperfeiçoamento da matriz de relacionamento, de modo a aumentar a sua capacidade de correlacionar os controlos auditados com diferentes métricas organizacionais, como por exemplo, o impacte financeiro, o nível de criticidade dos processos e o grau de conformidade regulatória. Este aprimoramento possibilitará a criação de um mapa integrado de riscos e conformidade, oferecendo uma visão mais estratégica e orientada para a tomada de decisão pela gestão de topo, facilitando a priorização de ações corretivas e a alocação eficiente de recursos.

Referências

[1] W. M. P. v. d. Aalst, M. Bichler e A. Heinzl, “Robotic Process Automation,” *Springer Fachmedien Wiesbaden GmbH,* 2018.

[2] B. Hong, M. Ly e H. Lin, “Robotic Process Automation Risk Management: Points to Consider,” *JOURNAL OF EMERGING TECHNOLOGIES IN ACCOUNTING,* 2023.

[3] J. Brás, R. Pereira e S. Moro, “Intelligent Process Automa-tion and Business Continuity: Areas for Future Research,” *Information (2078-2489),* 2023.

[4] B. Akash, A. H. Saad e M. El-Saadawi, “Multi-Criteria Decision Making Analysis of Optimal Service Delivery Technique Using AHP,” *TEM Journal,* 2023.

[5] K. Peffers, T. Tuunanen, C. E. Gengler, M. Rossi, W. Hui, V. Virtanen e J. Bragge, “ SCIENCE RESEARCH PROCESS: A MODEL FOR PRODUCING AND PRESENTING INFORMATION SYSTEMS RESEARCH,” *1st International Conference on Design Science in Information Systems,* 2006.

[6] A. R. Hevner, S. T. March, J. Park e S. Ram, “DESIGN SCIENCE IN INFORMATION SYSTEMS RESEARCH,” *MIS Quarterly,* 2004.

[7] C. Zhang, C. Thomas e M. A. Vasarhelyi, “Attended Process Automation in Audit: A Framework and A Demonstration,” *Journal of Information Systems,* 2022.

[8] “ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection - Information security management systems – Requirements,” 2022.

[9] B. Kitchenham, “Procedures for Performing Systematic Reviews,,” *NICTA Report,* 2004.

[10] K. Khan, G. T. Riet, J. Glanville, A. Sowden e J. Kleijnen, “Undertaking Systematic Review of Research on Effectiveness. CRD’s Guidance for those Carrying Out or Commissioning Reviews,” *NHS Centre for Reviews and Dissemination,* 2001.

[11] J. Krüger, C. Lausberger, I. v. Nostitz-Wallwitz, G. Saake e T. Leich, “Search. Review. Repeat? An empirical study of threats to replicating SLR searches,” *Empirical Software Engineering,* 2020.

[12] L.-E. ANICA-POPA, I.-M. PETRICĂ e M. G. SAVA, “Revamping Business Services: RPA Solutions Landscape,” *Proceedings of the 17th International Conference on Business Excellence ,* 2023.

[13] R. Chugh, S. Macht e R. Hossain, “Robotic Process Automation: a review of organizational,” *International Journal of Information Systems and Project Management,* 2022.

[14] P. Lin, “Adapting to the New Business Environment,” *CPA Journal ,* 2018.

[15] J. Wewerka e M. Reichert, “Robotic process automation - a systematic mapping study and classification framework,” *Enterprise Information Systems,* 2023.

[16] A. Asatiani, T. Hakkarainen, K. Paaso e E. Penttinen, “Security by envelopment - a novel approach to data-security-oriented configuration of lightweight-automation systems,” *European Journal of Information Systems,* 2023.

[17] A. Asatiani, O. Copeland e E. Penttinen, “Deciding on the robotic process automation operating model: A checklist for RPA managers,” *Business Horizons,* 2023.

[18] C. Flechsig, F. Anslinger e R. Lasch, “Robotic Process Automation in purchasing and supply management: A multiple case study on potentials, barriers, and implementation,” *Journal of Purchasing,* 2022.

[19] D. Fernandez e A. Aman, “,THECHALLENGES OF IMPLEMENTING ROBOTIC PROCESS AUTOMATION IN GLOBAL BUSINESS SERVICES,” *International Journal of Business,* 2021.

[20] A.-M. Crijman, “GOOD BUSINESS PROCESSES CANDIDATES FOR AUTOMATION FUTURE OF WORK: ROBOTIC PROCESS AUTOMATION,” *Annals of the 'Constantin Brancusi' University of Targu Jiu, Economy Series,* 2021.

[21] V. K. Suri, M. Elia e J. v. Hillegersberg, “Software Bots - The Next Frontier for Shared Services,” *Springer International Publishing AG,* 2017.

[22] A. Asatiani und E. Penttinen, „Turning robotic process automation into commercial success–Case OpusCapita,“ *Journal of Information Technology Teaching Cases,* 2016.

[23] C. Zhang, “Intelligent Process Automation in Audit,” *Journal of Emerging Technologies in Accounting,* 2019.

[24] A. Perdana, W. Lee e C. M. Kim, “Prototyping and implementing Robotic Process Automation in accounting firms: Benefits, challenges and opportunities to audit automation,” *International Journal of Accounting Information Systems,* 2023.

[25] C. Zhang, H. Issa, A. Rozario e J. S. Soegaard, “Robotic Process Automation (RPA) Implementation Case Studies in Accounting: A Beginning to End Perspective,” *Accounting Horizons,* 2023.

[26] D. ŠIMEK e R. ŠPERKA, “How Robot/human Orchestration Can Help in an HR Department: A Case Study From a Pilot Implementation,” *Organizacija,* 2019.

[27] protiviti, 2019. [Online]. Available: https://www.protiviti.com/sites/default/files/2022-10/2019-global-rpa-survey-protiviti_global.pdf. [Acedido em 10 March 2025].

[28] L. Willcocks, M. Lacity e A. Craig, “The IT function and robotic process automation,” *Journal of Information Technology,* 2015.

[29] D. A. d. S. Costa, H. S. Mamede e M. M. d. Silva, “ROBOTIC PROCESS AUTOMATION (RPA) ADOPTION: A SYSTEMATIC LITERATURE REVIEW,” *Engineering Management in Production,* 2022.

[30] M. Schuett, “Robotic Process Automation Meets Identity and Access Management,” *ISSA Journal,* 2019.

[31] M. Zelenka e M. Vokoun, “Information and communication technology capabilities and business performancThe case of differences in the Czech financial sector and lessons from robotic process automation between 2015 and 2020,” *Review of Innovation and Competitiveness: A Journal of Economic and Social Research,* 2021.

[32] F. A. Liévano-Martínez e J. D. Fernández-Ledesma, “Roadmap for the implementation of robotic process automation in enterprises,” *Dyna,* 2022.

[33] F. Santos, R. Pereira e J. B. Vasconcelos, “Toward robotic process automation implementation: An end-to-end perspective,” *Business Process Management Journal,* 2020.

[34] A. Sobczak, “Building a Robotic Capability Map of the Enterprise,” *Management Issues,* 2019.

[35] M. Cohen, A. Rozario e C. Zhang, “Exploring the Use of Robotic Process Automation (RPA) in Substantive Audit Procedures,” *CPA Journal,* 2019.

[36] H. Leopold, H. v. D. Aa e H. Reijers, “Identifying candidate tasks for robotic process automation in textual process descriptions,” *Springer International Publishing,* 2018.

[37] J. Siderska, “ROBOTIC PROCESS AUTOMATION - A DRIVER OF DIGITAL TRANSFORMATION?,” *Engineering Management in Production and Services,* 2020.

[38] F. Huang e M. A. Vasarhelyi, “Applying robotic process automation (RPA) in auditing: A framework,” *International Journal of Accounting Information Systems,* 2019.

[39] A. M. Radke, M. T. Dang e A. Tan, “USING ROBOTIC PROCESS AUTOMATION (RPA) TO ENHANCE ITEM MASTER DATA MAINTENANCE PROCESS,” *LogForum,* 2020.

[40] R. Syed, S. Suriadi, M. Adams, W. Bandara, S. J. Leemans, C. Ouyang, A. H. t. Hofstede, I. v. d. Weerd, M. T. Wynn und H. A. Reijers, „Robotic Process Automation: Contemporary themes and challenges,“ *Computers in Industry,* 2020.

[41] C. B. Frey e M. A. Osborne, “The future of employment: How susceptible are jobs to computerisation?,” *Technological forecasting and social change,* 2017.

[42] M. Eulerich, J. Pawlowski, N. J. Waddoups e D. A. Wood, “A Framework for Using Robotic Process Automation for Audit Tasks,” *Contemporary Accounting Research,* 2021.

[43] “ISO/IEC 27002:2022 Information security, cybersecurity and privacy protection - Information security controls,” 2022.

[44] A. R. Hevner, “A Three Cycle View of Design Science Research,” *Scandinavian Journal of Information Systems,* 2007.

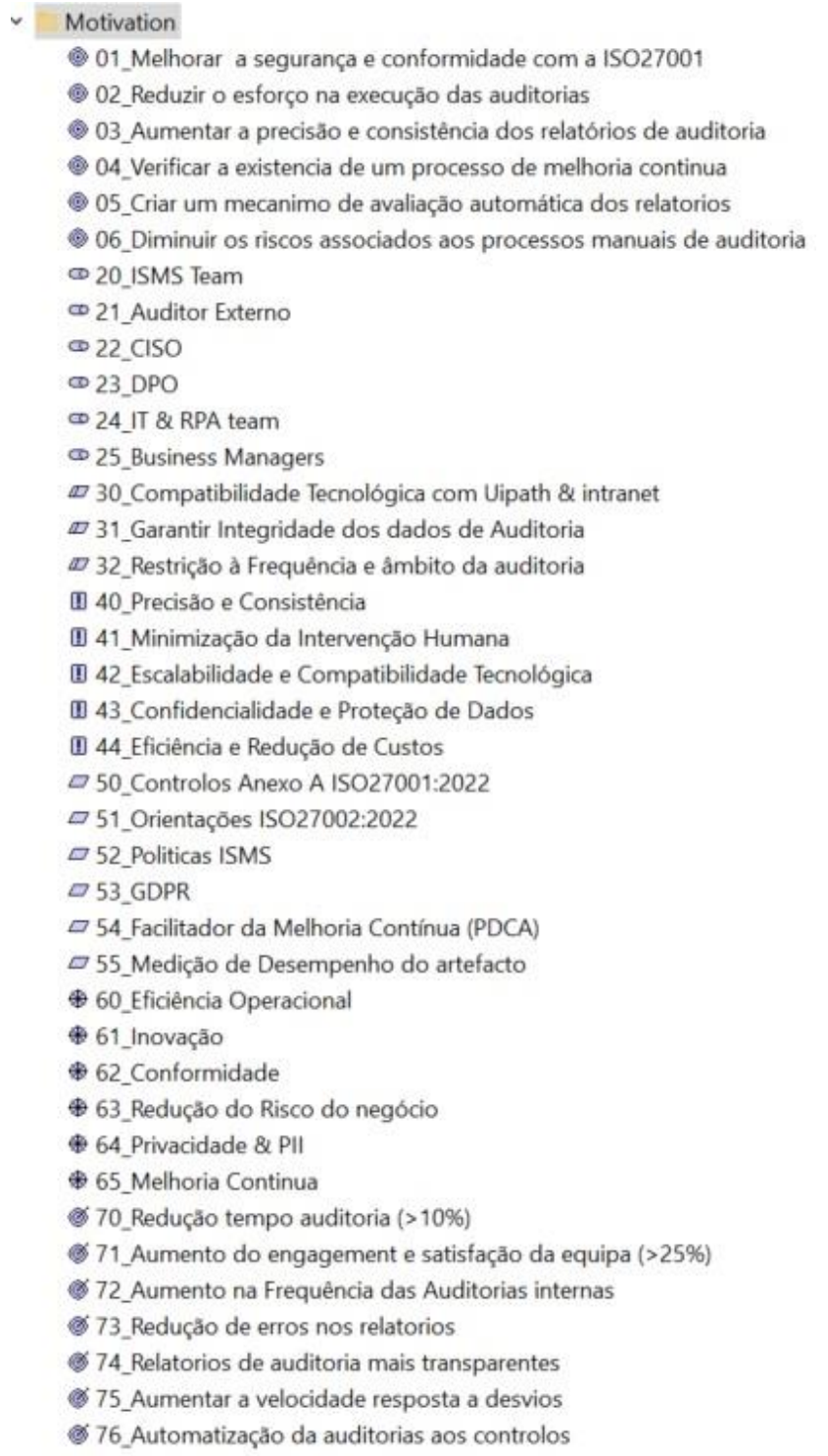
[45] K. C. Moffitt, A. M. Rozario e M. A. Vasarhelyi, “Robotic Process Automation for Auditing,” *Journal of Emerging Technologies in Accounting,* 2018.

[46] M. Gotthardt, D. Koivulaakso, O. Paksoy, C. Saramo, M. Martikainen e O. Lehner, “Current State and Challenges in the Implementation of Smart Robotic Process Automation in Accounting and Auditing,” *ACRN Journal of Finance and Risk Perspectives,* 2020.

[47] J. R. Venable, J. Pries-Heje e R. Baskerville, “Strategies for design science research evaluation,” *European Conference on Information Systems, ECIS,* 2008.

Anexos

ANEXO I - Elementos de motivação identificados e representados de acordo com a linguagem *ArchiMate*



Legenda:

	Stakeholder
	Driver
	Objetivo
	Resultado
	Principio
	Requisito
	Restrição

ANEXO II - Cálculo da Redução do FTE

Definição do Conceito de FTE (*Full-Time Equivalent*)
O FTE (*Full-Time Equivalent*) é uma métrica utilizada para quantificar a carga de trabalho com base no tempo total de um colaborador a tempo inteiro. Normalmente, o cálculo do FTE é baseado num período padrão de trabalho, que pode variar conforme a organização (dia; semana; mês; ano) e o objetivo da validação da métrica. Para este estudo, considerou-se uma jornada padrão de 8 horas diárias.
A fórmula utilizada para calcular o FTE é:

$$FTE = \frac{Total\ Horas\ Trabalhadas}{Carga\ Horária\ Padrão}$$

Cálculo do FTE Antes e Depois da Implementação do Robô Auditor:

Antes da implementação do Robô Auditor, o processo de auditoria exigia:
3 pessoas, onde cada uma trabalha 4 horas por dia;
O tempo total de trabalho humano era de:

$$3x4 = 12\ horas$$

Cálculo do FTE inicial:

$$FTE_{inicial} = \frac{12}{8} = 1{,}5$$

Ou seja, antes da automatização, o esforço requerido era equivalente a 1,5 colaboradores a tempo inteiro.

Com a implementação do Robô Auditor, o processo de auditoria passou a exigir:

1 pessoa durante 1 hora, ou seja:

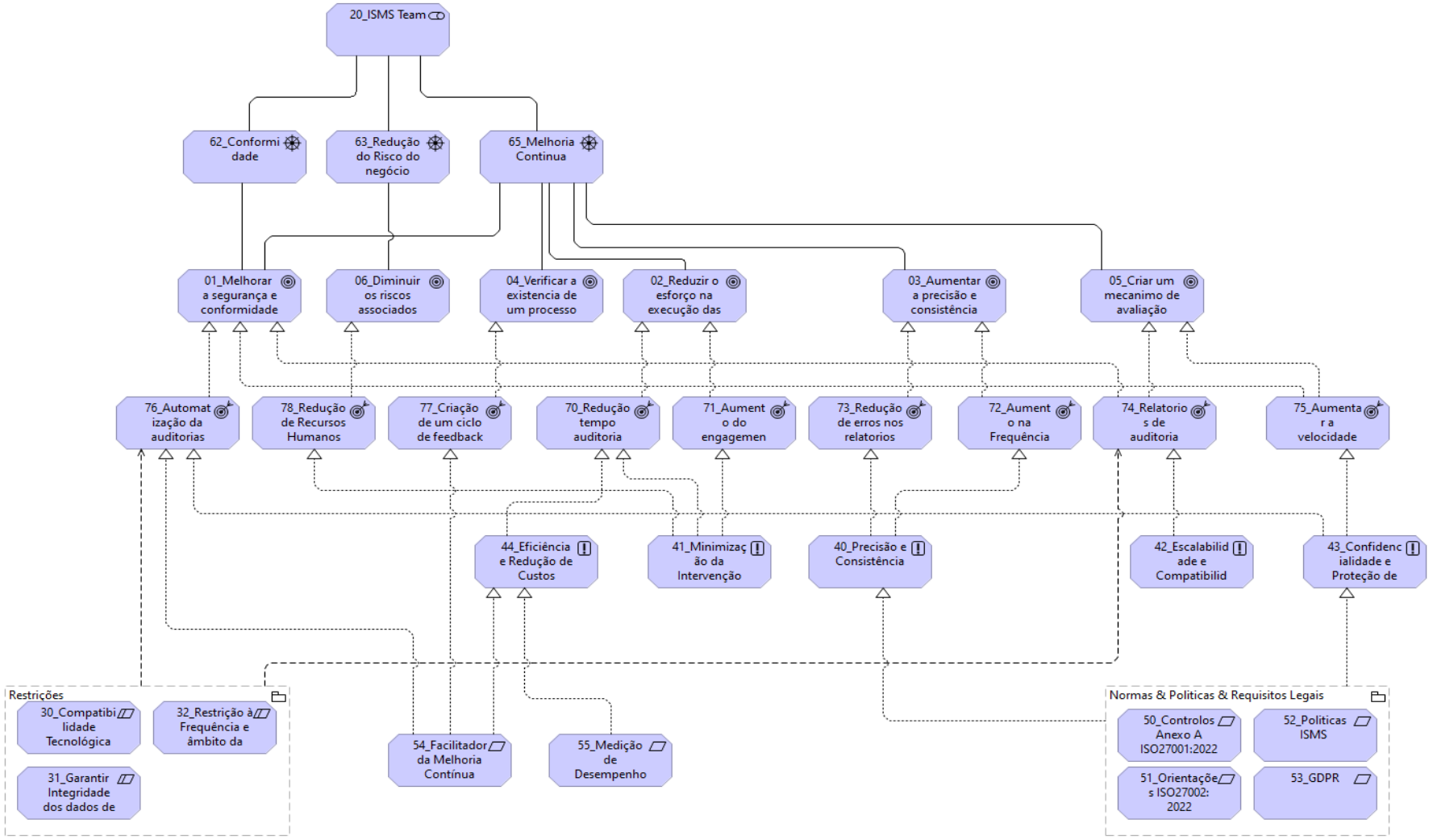
$$FTE\ _{final} = \frac{1}{8} = 0{,}125$$

Cálculo da redução percentual no FTE:

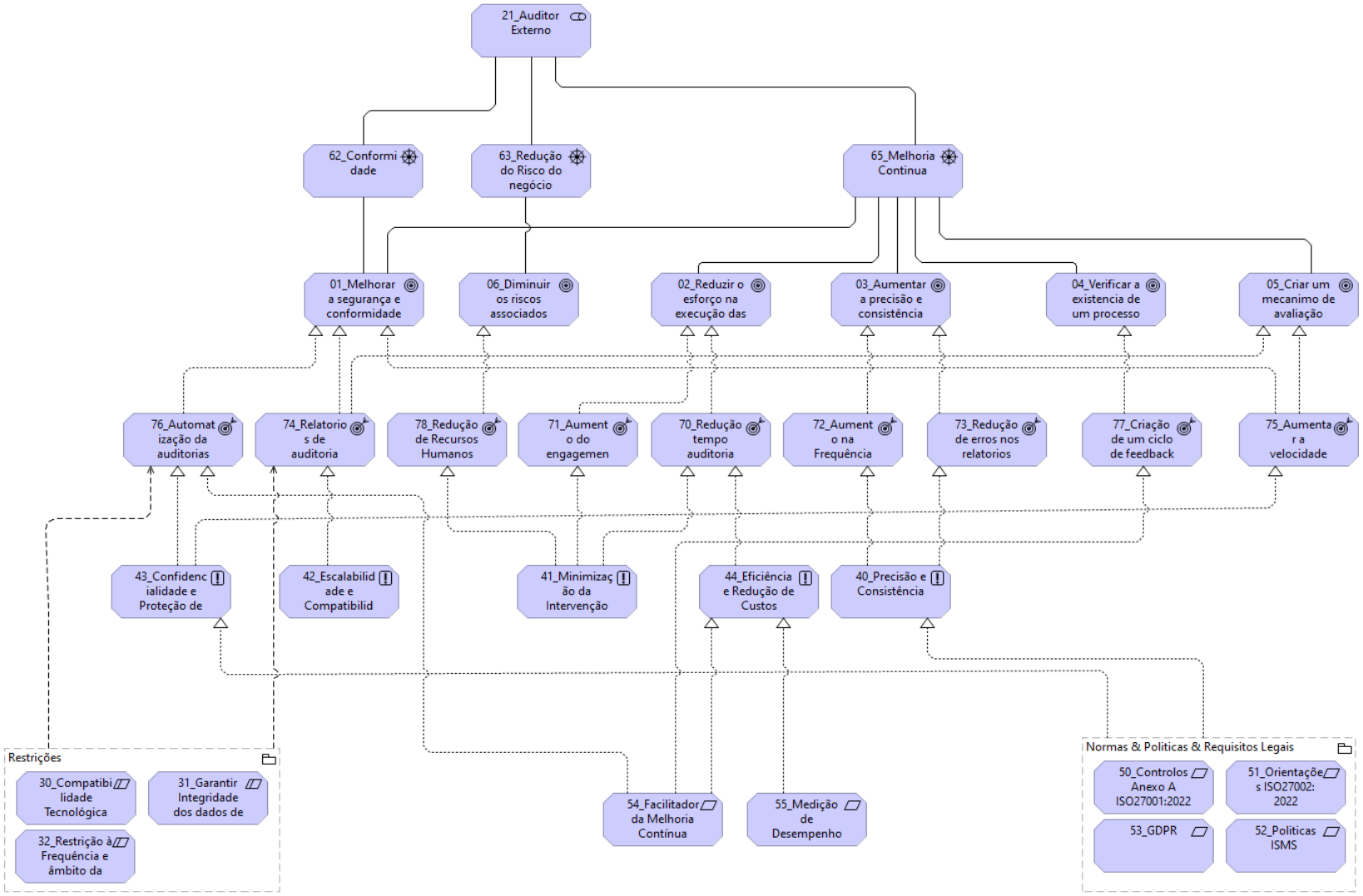
$$Redução\ FTE\ (\%) = \left(\frac{FTE_{inicial} - FTE_{final}}{FTE_{inicial}}\right) x100$$

$$Redução\ FTE\ (\%) = \left(\frac{1{,}5 - 0{,}125}{1{,}5}\right) x100 \approx 92\%$$

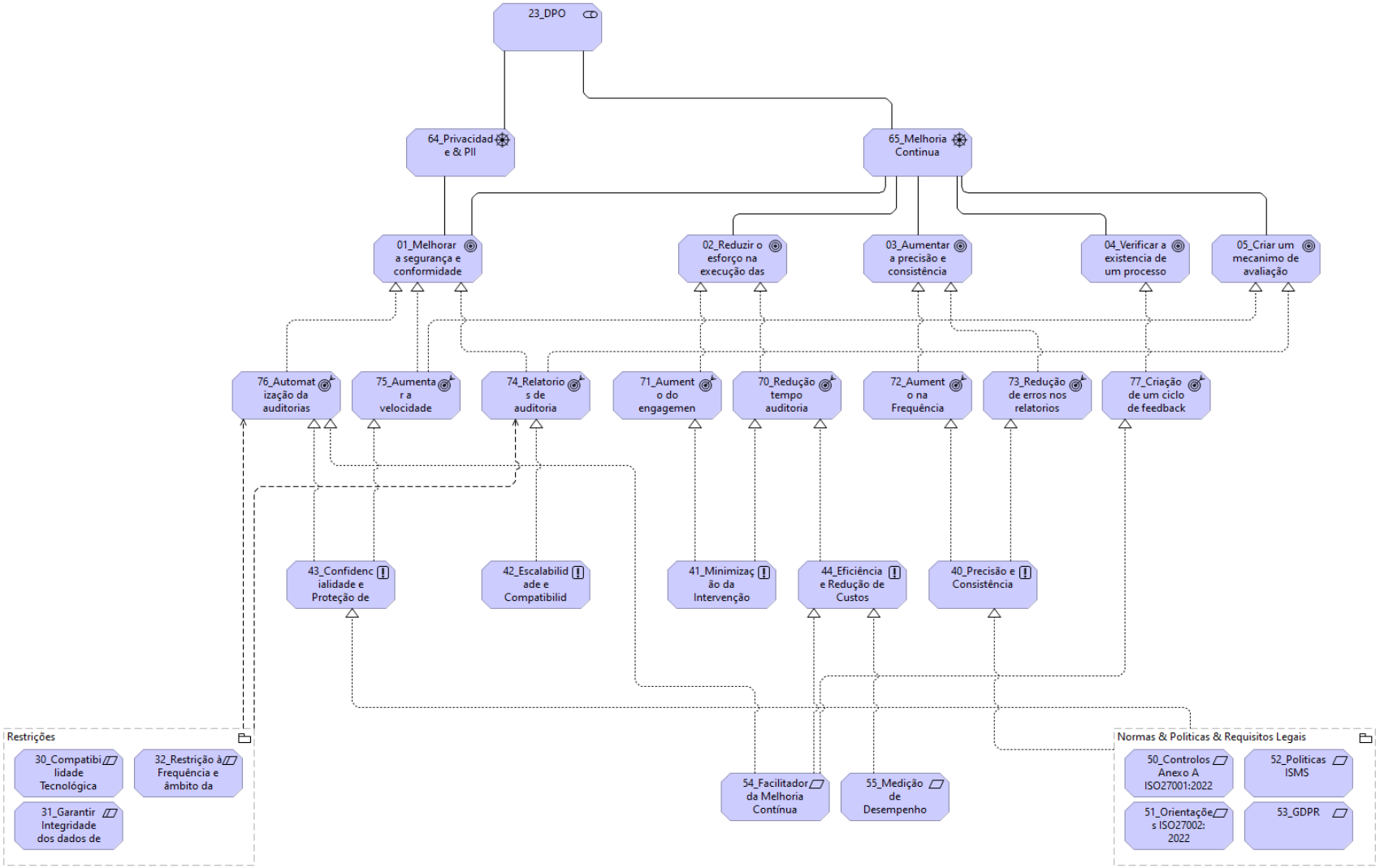
ANEXO III - Motivação (20_Equipe ISMS)



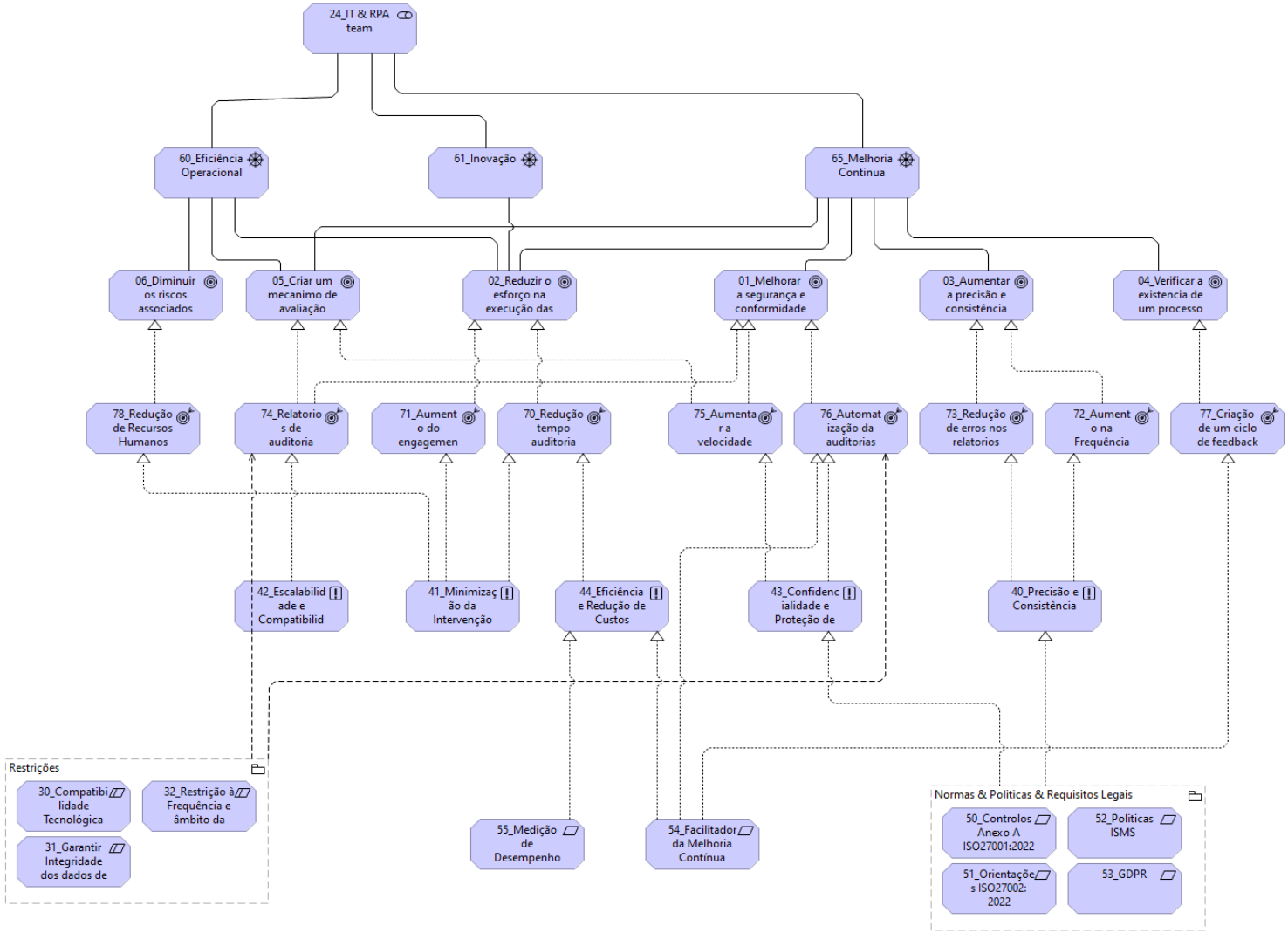
ANEXO IV – *ViewPoint*: Motivação (21_Auditor Externo)



ANEXO V – *ViewPoint*: Motivação (23_DPO)



ANEXO VI – *ViewPoint*: Motivação (24_IT & RPA team)



ANEXO VII – *ViewPoint*: Motivação (25_Business Managers)