P.PORTO

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

M **MESTRADO**
Gestão de Projetos

A problemática da Cibersegurança em operadores de serviços essenciais e administração pública – uma abordagem pela gestão de risco em projetos

Ana Catarina Marinho Ribeiro

11/**2022**

P.PORTO

ESCOLA SUPERIOR DE TECNOLOGIA E GESTÃO
POLITÉCNICO DO PORTO

M **MESTRADO**
Gestão de Projetos

A problemática da Cibersegurança em operadores de serviços essenciais e administração pública – uma abordagem pela gestão de risco em projetos
Ana Catarina Marinho Ribeiro

11/**2022**

Ana Catarina Marinho Ribeiro. **A problemática da Cibersegurança em operadores de serviços essenciais e administração pública – uma abordagem pela gestão de risco em projetos**

ESCOLA
SUPERIOR
DE TECNOLOGIA
E GESTÃO
POLITÉCNICO
DO PORTO

P.PORTO

M

MESTRADO
Gestão de Projetos

A problemática da Cibersegurança em operadores de serviços essenciais e administração pública – uma abordagem pela gestão de risco em projetos

Ana Catarina Marinho Ribeiro

Orientadores
Professora Doutora Maria Teresa Morais Taveira de Barros,
Professor Doutor João Paulo Ferreira de Magalhães

AGRADECIMENTOS

Quero agradecer a todas as pessoas que, ao longo deste ano de trabalho, me ajudaram e tornaram possível concluir uma grande etapa da minha vida, pois sem a ajuda de todos, tudo isto não seria possível. Em especial aos Professores Teresa Barros e João Paulo Magalhães que, graças aos seus conselhos e orientações, possibilitaram a conclusão deste projeto.

Um agradecimento especial à Escola Superior de Tecnologia e Gestão (ESTG|P.PORTO), a todos os meus amigos que estiveram presentes nos momentos de estudo e de lazer, mas que também foram um grande apoio para a conclusão desta etapa.

Aos meus pais, que sempre me apoiaram nos momentos mais importantes e que acreditaram em mim mesmo nos piores momentos.

A todos que de alguma forma estiveram envolvidos em todo este processo, o meu muito Obrigada!

RESUMO

A gestão de projetos alcançou um papel primordial no mundo organizacional quer se trate de organizações privadas ou púbicas. Um dos tópicos de relevo na gestão de projetos é a gestão do risco. As organizações enfrentam diversos riscos e com a crescente digitalização quer do setor público quer do privado, a segurança do ciberespaço passou a ter uma importância crescente. Daí que tenha surgido legislação que exija às organizações que utilizem sistemas que garantam elevados níveis de segurança, sob pena de incorrerem em incumprimento o qual se traduz em pesadas multas além de outras consequências legais ao nível do não cumprimento das normas. Foi neste contexto que surgiu a Lei n.º 46/2018, de 13 de agosto, que aprovou o Regime Jurídico da Segurança do Ciberespaço, transpôs para o ordenamento jurídico nacional a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa às medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União Europeia. A referida lei remete para legislação complementar a definição, por um lado, dos requisitos de segurança das redes e sistemas de informação e, por outro lado, das regras para a notificação de incidentes, que devem ser cumpridos pela Administração Pública, Operadores de Infraestruturas Críticas, Operadores de Serviços Essenciais (OES) e Prestadores de Serviços Digitais (DSP). Do ponto de vista das organizações, o cumprimento do novo requisito é um desafio na medida em que requer uma acumulação de atividades que por si só são complexas (e.g., inventariação completa de ativos digitais críticos).

Para mitigar os desafios acima apresentados, este projeto visa criar um processo composto por procedimentos e documentos de suporte. Os procedimentos e documentação têm em consideração a qualidade da informação a recolher, os recursos necessários, os procedimentos operacionais a seguir e as responsabilidades estabelecidas no âmbito do mesmo. A existência de um processo, contribui para a padronização das operações relativas ao cumprimento das normas e requisitos legais exigidos pelo Decreto-Lei (DL) n.º 65/2021, com enfoque na Administração Pública e nos Operadores de Serviços essenciais. Desta forma, torna-se mais simples e clarificam-se as tarefas a realizar, como as realizar, quem as deve realizar e quando o deve fazer e, não menos importante, estabelece uma base documental que evidencia o cumprimento do estipulado no DL. Subjacente à execução do projeto de implementação do DL está uma metodologia de gestão de risco necessária para uma gestão de projetos eficiente nas diversas organizações de estudo.

Este projeto adotou uma metodologia *action-research* que se revelou eficaz. pelo facto de se tratar de um projeto avançado em que, as características inerentes à metodologia tornaram a execução do projeto mais eficaz. Entre estas características destaca-se que o autor foi parte integrante do projeto, contribuindo para que o estudo processual em causa fosse realizado e validado em ambiente

produtivo, sendo melhorado à medida que foi testado. Com a aplicação do processo verificou-se que, através do mesmo, as organizações deram cumprimento aos requisitos do DL, evitando assim as sanções pelo seu incumprimento.

Palavras-chave:

Projeto; Gestão de Projeto; Gestão de Risco; Cibersegurança; Decreto-Lei n.º 65/2021

ABSTRACT

Project management has reached a paramount role in the organisational world whether in private or public organisations. One of the prominent topics in project management is risk management. Organisations face a variety of risks and with the increasing digitalisation of both the public and private sector, cyberspace security has become increasingly important. Therefore, legislation has emerged that requires organisations to use systems that ensure high levels of security, under penalty of non-compliance, which translates into heavy fines and other legal consequences in terms of non-compliance. It was in this context that Law no. 46/2018, of 13 August, which approved the Legal Framework for Cyberspace Security, transposed to the national legal system the Directive (EU) 2016/1148, of the European Parliament and of the Council, of 6 July 2016, on measures to ensure a high common level of security of network and information systems throughout the European Union, came into being. The referred law refers to complementary legislation to define, on the one hand, the security requirements of networks and information systems and, on the other hand, the rules for the notification of incidents, which must be complied with by Public Administration, Critical Infrastructure Operators, Essential Service Operators (ESOs) and Digital Service Providers (DSPs). From the organisations' point of view, compliance with the new requirement is a challenge in that it requires an accumulation of activities that are complex in themselves (e.g., complete inventorying of critical digital assets).

To mitigate the challenges presented above, this project aims to create a process composed of procedures and supporting documents. The procedures and documentation take into consideration the quality of the information to be collected, the necessary resources, the operational procedures to be followed and the responsibilities established within it. The existence of a process contributes to the standardization of the operations related to the compliance with the norms and legal requirements demanded by Decree-Law 65/2021, with focus on Public Administration and Essential Service Operators. In this way, it becomes simpler and clarifies the tasks to be performed, how to perform them, who should perform them and when, and no less important, establishes a documentary basis that evidences compliance with the stipulations of the Decree-Law. Underlying the execution of the project is a methodology for risk management in project management in various organisations, complying with the Decree-Law.

This project adopted an action-research methodology that proved to be appropriate for the project in question. The fact that this is an advanced project, and the inherent characteristics of the methodology made the execution of the project more effective. Among these characteristics the author was an integral part of the project, contributing to the process study being carried out and validated in a productive environment, being improved as it was tested.

With the application of the process, it was verified that, through it, the organisations included. In this research complied with the requirements of the DL, avoiding the sanctions foreseen for their non-compliance due to a risk management methodology process was designed.

Keywords:

Project; Project Management; Risk Management; Cybersecurity; Decree Lawn.º65/2021

ÍNDICE

LISTA DE ACRÓNIMOS E SIGLAS

ANACOM	Autoridade Nacional de Comunicações
ANEPC	Autoridade Nacional de Emergência e Proteção Civil
API	*Application Programming Interface*
APT	*Advanced Persistent Threats*
CERT.PT	Equipa de Resposta a Incidentes de Segurança Informática Nacional
CNCS	Centro Nacional de Cibersegurança
CNPD	Comissão Nacional de Proteção de dados
CPM	*Critical Path Method*
CSIRT	*Computer Security Incident Response Team*
DL	Decreto-Lei
DR	Dono do Risco
DSP	Operadores de Serviços Digitais
ENISA	European Union Agency for Cybersecurity
ENSC	Estratégia Nacional de Segurança do Ciberespaço
EVM	*Earned Value Management*
GR	Gestor de Risco
GT	Gestão de Topo
HTCC	*High-Tech Crime Center*
IS	*Information Security*
ISO	*International Organization for Standardization*
IT	*Information Technology*
OES	Operadores de Serviços Essenciais
PCP	Ponto de Contato Permanente
PERT	*Program Evaluation and Review Technique*
PGP	*Pretty Good Privacy*
PM	*Project Management*
PME	Pequena Média Empresa
PMI	*Project Management Institute*
QNRCS	Quadro Nacional de Referência para a Cibersegurança
RACI	*Responsible, Accountable, Consulted, Informed*
RBS	*Risk Breakdown Structure*
RJSC	Regime Jurídico de Segurança do Ciberespaço

RS	Responsável de Segurança
SI	Sistemas de Informação
SIEM	*Security Information and Event Management*
SOC	*Security Operations Center*
SR	Segurança de Redes
SRI	Segurança das Redes e da Informação
STI	Sistemas e Tecnologias de informação
SWOT	*Strengths, Weaknesses, Opportunities, Threats*
TIC	Tecnologias de Informação e Comunicação
UE	União Europeia
WBS	*Work Breakdown Structure*

LISTA DE FIGURAS

LISTA DE TABELAS

1. Introdução

Neste capítulo é apresentado o tema de investigação escolhido qual teve por base a experiência profissional da autora a qual cruza com as necessidades do tema, nomeadamente o facto de as questões de cibersegurança serem crucias para o sistema empresarial, designadamente para os Operadores de Serviços Essenciais (OES) e Administração Pública. O tema da cibersegurança está em constante atualização procurando dar resposta aos avanços tecnológicos.

No decorrer do capítulo evidencia-se, ainda, o enquadramento adjacente à realização do projeto, assim como os objetivos e a metodologia de investigação. É ainda descrita a estrutura geral do trabalho.

1.1 Enquadramento e Motivação

A gestão de projetos e cibersegurança em Portugal tem sofrido uma evolução notável nos últimos anos, sendo alvo de diversos estudos na utilização de práticas em determinados setores.

A cibersegurança passou a ser uma prioridade das organizações, que implica e se traduz num investimento contínuo na proteção de todos os seus ativos, contribuindo para uma melhor capacidade de prevenção, deteção e resposta aos incidentes ou potenciais incidentes de segurança. Em reforço a esta necessidade surge legislação e regulamentação aplicável, que promove a adoção e a utilização de práticas comuns ou normalizadas para os procedimentos de gestão de risco de forma a mitigar os ciberataques contribuindo para a maturidade da organização, no que diz respeito à cibersegurança.

Porém, nos dias de hoje, as organizações deparam-se com uma grande dificuldade no que diz respeito ao cumprimento dos requisitos legalmente exigidos. A escassez de informação que as auxilie a compreender de que forma devem atuar, a falta de profissionais instruídos e com competências técnicas e legais para abordar o assunto assim como a falta de instruções técnicas com *baselines* claras, limita as organizações sobre a forma como devem atuar. Criar mecanismos que simplifiquem a tarefas às organizações e lhes permita cumprir com os requisitos legais é necessário, útil e urgente.

Com a publicação da Lei n.º 46/2018, de 13 de agosto, que aprovou o regime jurídico da segurança do ciberespaço foi transposta para o ordenamento jurídico nacional a Diretiva(UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União (Assembleia da República, 2018).

A referida lei remete para legislação complementar a definição, por um lado, dos requisitos de segurança das redes e sistemas de informação e, por outro lado, das regras para a notificação de incidentes, que devem ser cumpridos pela Administração Pública, Operadores de Infraestruturas Críticas, Operadores de Serviços Essenciais (OES) e Prestadores de Serviços Digitais.

Os requisitos previstos no DL n.º 65/2021, de 30 de julho, constituem o mínimo a assegurar pelas entidades abrangidas pela Lei n.º 46/2018, de 13 de agosto, não prejudicando as regras que, em função da natureza das entidades, de aspetos específicos da atividade desenvolvida ou do contexto em que esta se desenvolva, possam vir a ser estabelecidas por outras autoridades, nomeadamente pelo Ministério Público, pela Autoridade Nacional de Emergência e Proteção Civil, pelo Conselho Nacional de Planeamento Civil de Emergência, pela Autoridade Nacional de Comunicações, pela Comissão Nacional de Proteção de Dados (CNPD), ou por outras autoridades setoriais (Decreto-Lei nº 65, 2021).

Tendo presente que o ciberespaço é uma realidade dinâmica e fluida, em permanente mutação, colocando desafios de alcance transnacional e que atravessa vários setores de atividade, o presente DL reconhece a necessidade de articular as disposições legais consagradas com a aplicação de normativos complementares setoriais. Para este efeito, o Centro Nacional de Cibersegurança (CNCS), enquanto Autoridade Nacional de Cibersegurança, nos casos em que se considere necessário e em articulação com as entidades reguladoras e de supervisão setoriais, procede a uma avaliação de equivalência, conferindo, assim, segurança jurídica aos requisitos constantes de legislação setorial que sejam considerados equivalentes aos consagrados no DL n.º 65/2021, de 30 de julho (Assembleia da República, 2018; Decreto-Lei nº 65, 2021).

1.2 Contexto e Relevância do Estudo

Um dos desenvolvimentos organizacionais mais importantes nos últimos anos foi o crescimento significativo no trabalho dos projetos em diferentes setores e indústrias. De acordo com Winter, Mark & Szczepanek (2008) várias pesquisas realizadas confirmam esse desenvolvimento onde se destaca a crescente importância das práticas de gestão de projetos e portfólios para as organizações.

Os projetos, que apresentam um início e fim bem definidos permitem a melhoria de processos e procedimentos numa organização (PMI, 2017a). A mesma referência tem em consideração que um projeto não está isento de riscos, e, como tal as organizações devem optar por assumir o risco dos projetos de forma controlada e intencional, a fim de criar valor, mesmo que para isso seja necessário aceitar alguns dos riscos identificados.

Com o desenvolvimento da Gestão de Projetos e a grande dependência das organizações para com as tecnologias da informação houve, de certa forma, um aumento crescente da utilização de Sistemas e Tecnologias de Informação (STI), aumentando assim o número de ataques no contexto

da cibersegurança, o que obrigou as organizações a atender a questões de segurança da informação, com o objetivo de manter a estabilidade funcional da organização. Nesta perspetiva, Sêmola (2003) afirma que toda informação é influenciada por três princípios básicos que são a confidencialidade, integridade e disponibilidade. Para o autor, a segurança da informação é a preservação desses elementos, além de outros aspetos que podem estar envolvidos como a autenticidade.

Para Wheeler (2011), a confidencialidade garante que a informação não é divulgada a pessoas ou entidades estranhas, pois o acesso à informação é somente para aqueles que estejam devidamente autorizados. O conceito de integridade consiste em garantir que a informação permaneça exata, sem sofrer modificação ou destruição, que possa comprometer a sua autenticidade. Por fim, a disponibilidade permite garantir que a informação esteja disponível para o acesso confiável e sempre que necessário a todos os utilizadores autorizados.

Tendo em conta o mencionado anteriormente, as ameaças relacionadas aos ciberataques e seus potenciais impactos entraram na agenda da União Europeia (UE) e assumiram elevada importância na elaboração de políticas e legislação para a garantia de um nível mais elevado de cibersegurança. De acordo com a Estratégia da UE para cibersegurança, lançada em 2013, o principal objetivo centra-se em tornar o ambiente cibernético mais seguro. Neste sentido, ao estabelecer uma estratégia a nível da UE, deve-se considerar a natureza complexa e multilateral da cibersegurança, altamente dependente de cooperação institucional e de confiança mútua a nível nacional e internacional, do setor público e privado (C. Europeia, 2013). De forma a atingir tal objetivo, a UE desenvolveu a Diretiva (UE) 2016/11486 sobre a Segurança das Redes e da Informação (SRI), que estabelece a adoção de uma estratégia de cibersegurança pelos Estados-Membros e a designação de uma autoridade competente em cada Estado-Membro para lidar com esta matéria específica, bem como institui requisitos de segurança e de notificação de incidentes para operadores que prestam serviços essenciais (em setores críticos como a energia, os transportes, a saúde e as finanças) e pelos prestadores de serviços digitais (P. E. e o C. da U. Europeia, 2016).

1.3 Objetivos do Estudo

O presente projeto avançado tem como principal objetivo a aplicação de uma metodologia de gestão de risco no contexto da segurança da informação, através da criação de um processo de implementação dos requisitos obrigatórios do DL n. º65/2021, permitindo:

- Aplicar metodologias de gestão de risco do projeto para criar um processo composto por procedimentos e respetivos documentos de suporte que permitam identificar pontos chave descritos na Lei n.º 46/2018 e no DL n.º 65/2021;
- Contribuir para o aumento do nível de maturidade das organizações em termos de cibersegurança;

- Reduzir o risco de ataques cibernéticos com as consequências nefastas ao nível do impacto no negócio;
- Simplificar o processo de cumprimento do DL n.º 65/2021;
- Normalizar o processo de implementação dos requisitos definidos pelo Decreto-Lei junto das organizações;
- Dar cumprimento por parte da Administração Pública e dos OES, ao DL n.º 65/2021;
- Reduzir o risco de coimas decretadas na Lei n.º 46/2018.

1.4 Estrutura do Documento

Este documento encontra-se dividido em capítulos. No segundo capítulo é feita a **Revisão da Literatura**, apresentando-se o suporte bibliográfico, evidenciando primeiramente uma contextualização da gestão de projetos e da gestão de portefólios e sua relação com a cibersegurança. De seguida aborda-se a importância da gestão dos riscos na gestão de projetos, nomeadamente na segurança da informação que é o foco deste trabalho. No terceiro capítulo é apresentada a **Metodologia de Investigação** adotada para o processo de investigação, no que concerne à filosofia de investigação, à abordagem da mesma e à estratégia utilizada. Neste capítulo, realiza-se ainda uma caracterização das organizações envolvidas no estudo, apresenta-se, ainda, o processo criado que suporta a implementação do Decreto-Lei nº 65/2021. Neste capítulo é apresentada a metodologia de gestão de risco da gestão de projetos aplicada ao projeto avançado em questão. No capítulo 4 é feita a **Análise fina e discussão dos resultados** onde se analisa e discute os resultados obtidos anteriormente. Neste capítulo é apresentada a metodologia de gestão de risco da gestão de projetos aplicada ao projeto avançado em questão. No quinto capítulo, por fim, é realizada uma **Conclusão** do trabalho sendo apresentadas as principais conclusões do projeto e apresentadas propostas para trabalhos futuros.

2. Revisão da Literatura

Neste capítulo é apresentada uma revisão da literatura relacionada com o estudo proposto no projeto avançado. Inicia-se com uma descrição da metodologia utilizada para selecionar os materiais de suporte à revisão da literatura. Seguido da apresentação mais detalhada dos temas identificados na metodologia como relevantes para este estudo: gestão de projetos; gestão de portfolios; gestão do risco na gestão de projetos/portefólios nomeadamente na Segurança de Informação

2.1 Metodologia utilizada para selecionar os materiais de suporte

Para a implementação da Revisão da Literatura da presente dissertação, foram inicialmente selecionadas as bases de dados mais utilizadas no desenvolvimento científico, como é o caso da *Web of Science*, *Science Direct* e da *Scopus*. É importante ressalvar que os dados obtidos através da Scopus apenas permitiram identificar os *journals* relevantes na área, uma vez que a instituição (ESTG|P.PORTO) não dispõe de licença para uma consulta mais detalhada.

Uma vez selecionadas as bases de dados de pesquisa bibliográfica, foi necessário selecionar as *keywords*. Dada a escassa literatura sobre a aplicação da gestão de projetos na cibersegurança, sentiu-se a necessidade de criar dois grupos de *keywords*, sendo elas:

1. *project management, risk management, cybersecurity*;
2. *portfolio management, project management, risk management, cybersecurity.*

Em cada uma das bases de dados foi necessário a aplicação de filtros diferentes, como é possível observar na Figura 1. No *Web of Science* apenas foram selecionados os artigos publicados com uma data superior ou igual a 2010 e filtro de *keywords*. No primeiro grupo apenas foram obtidos 18 artigos dos quais, apenas cinco tinham permissão de acesso. Na mesma base de dados, utilizando as *keywords* do segundo grupo não foi possível obter qualquer tipo de resultado.

Tendo em conta a falta de resultados no *Web of Science* com a utilização de "*portfolio management*" sentiu-se a necessidade de adaptar as *keywords* a utilizar na pesquisa desta base de dados, assim sendo, substitui-se a *keyword* "*project management*" por "*portfolio management*" tendo-se obtido cinco artigos dos quais dois com permissões de acesso.

No *Science Direct*, para além de ser aplicado o filtro inicial da base de dados anterior, foi aplicado um filtro por tipo de artigo, tendo apenas sido considerados os artigos de revisão e artigos de pesquisa. Obteve-se um total de 62 artigos com as *keywords* do grupo um. Na mesma base de dados e com os mesmos filtros, mas com a aplicação das *keywords* do grupo dois foram obtidos 10 artigos dos quais três com permissão de acesso.

Por fim, foi utilizada a base de dados *Scopus*, onde apenas foram considerados trabalhos com data superior ou igual a 2010. Obteve-se um total 28 *journals* aplicando as *keywords* do grupo um e 33 *journals* no grupo dois de *keywords*.

Com o total dos 97 artigos foi realizada uma análise de bibliometria, de forma a destacar informação relevante de forma visual e quantitativa. Tanto os ficheiros exportados da Web of Science como os de Science Direct foram combinados e usados no programa VOSViewer (van Eck & Waltman, 2010). Este programa permite a análise de inter-relações entre artigos, os seus resumos, *keywords*, autores, entre outras informações.

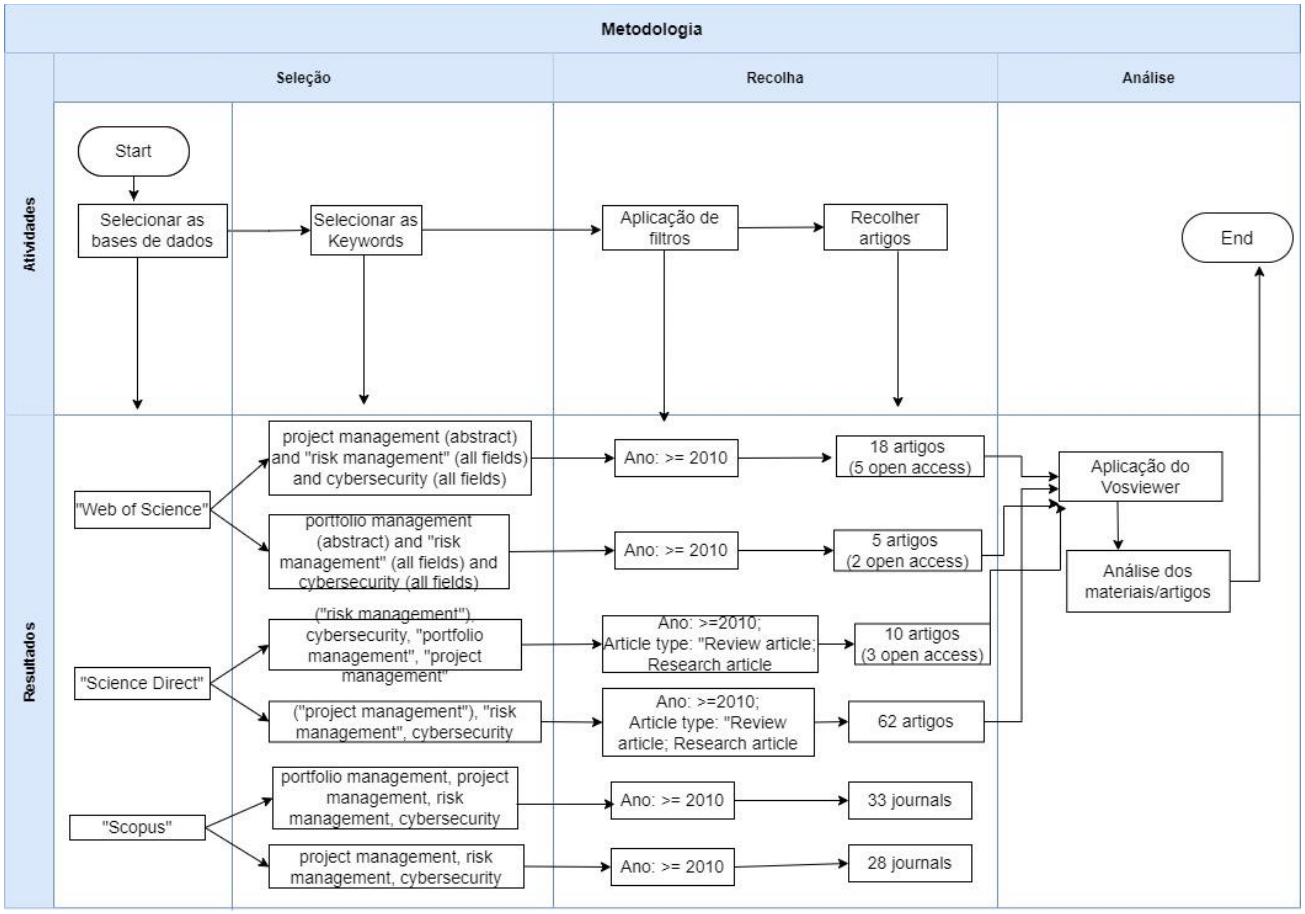


Figura 1 - Metodologia da Revisão da Literatura,
Fonte: Elaboração própria a partir do VOSviewer

Mesmo não estando mencionada na metodologia usada para selecionar os materiais para a revisão da literatura foi, de forma complementar, realizada uma pesquisa na base de dados do *Google Scholar*.

2.1.1 Análise Bibliométrica dos Autores

Nesta fase dos trabalhos foi realizada a análise bibliométrica dos autores dos artigos recolhidos do *Web of Science* e do *Science Direct* para os dois grupos de *keywords* referidos anteriormente.

2.1.1.1 *Web of Science*

Na referida análise e relativamente ao grupo um foram recolhidos 52 autores diferentes, mas notou-se que as redes de autores não estão relacionadas umas com as outras (ilustrado na Figura 2). Assim sendo, optou-se por analisar o maior conjunto de itens relacionados entre si. Em resultado desta análise, verificou-se que existem nove autores que se relacionam entre si em termos de área científica (ilustração na Figura 3).

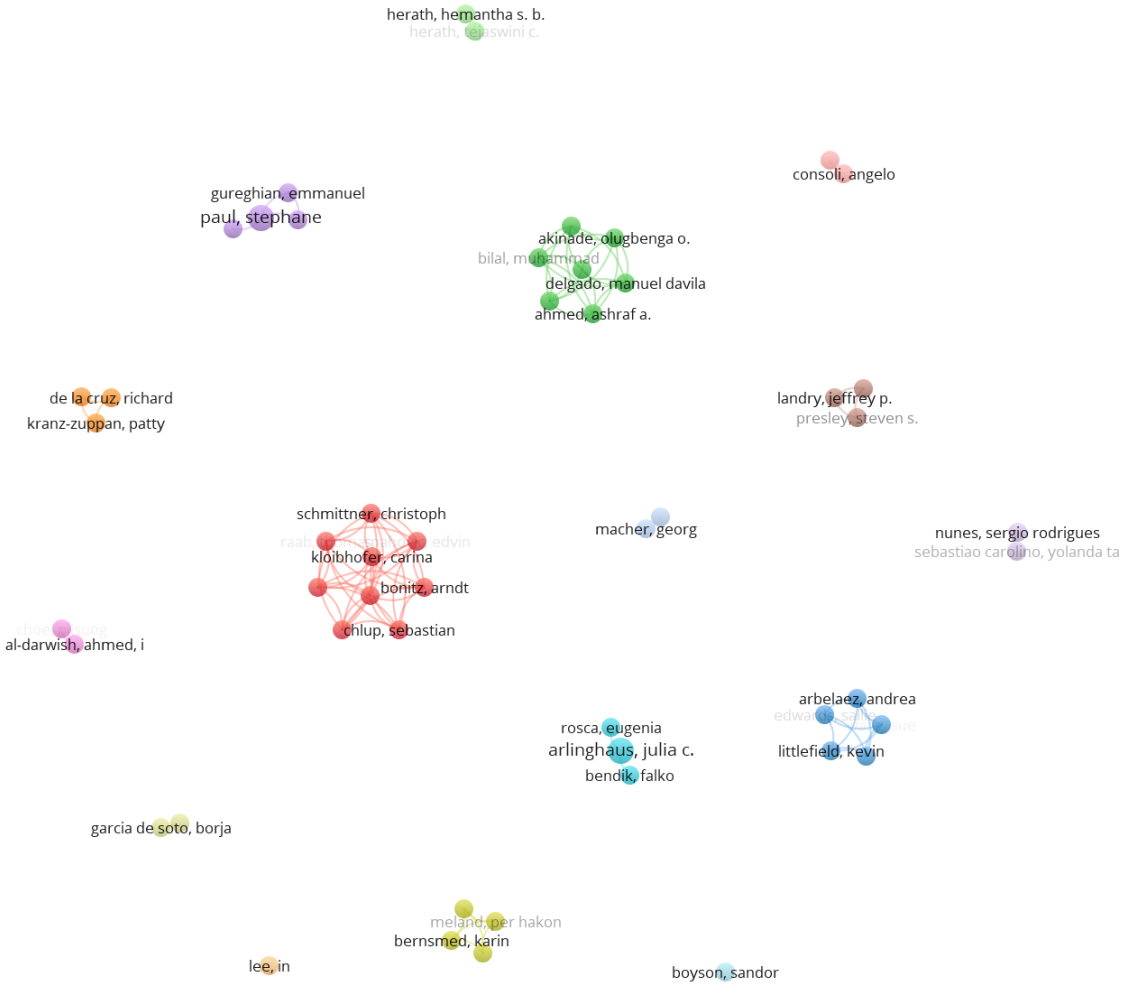


Figura 2 - "*Co-authorship authors*" grupo um - *Web of Science*
Fonte: Elaboração própria a partir do VOSviewer

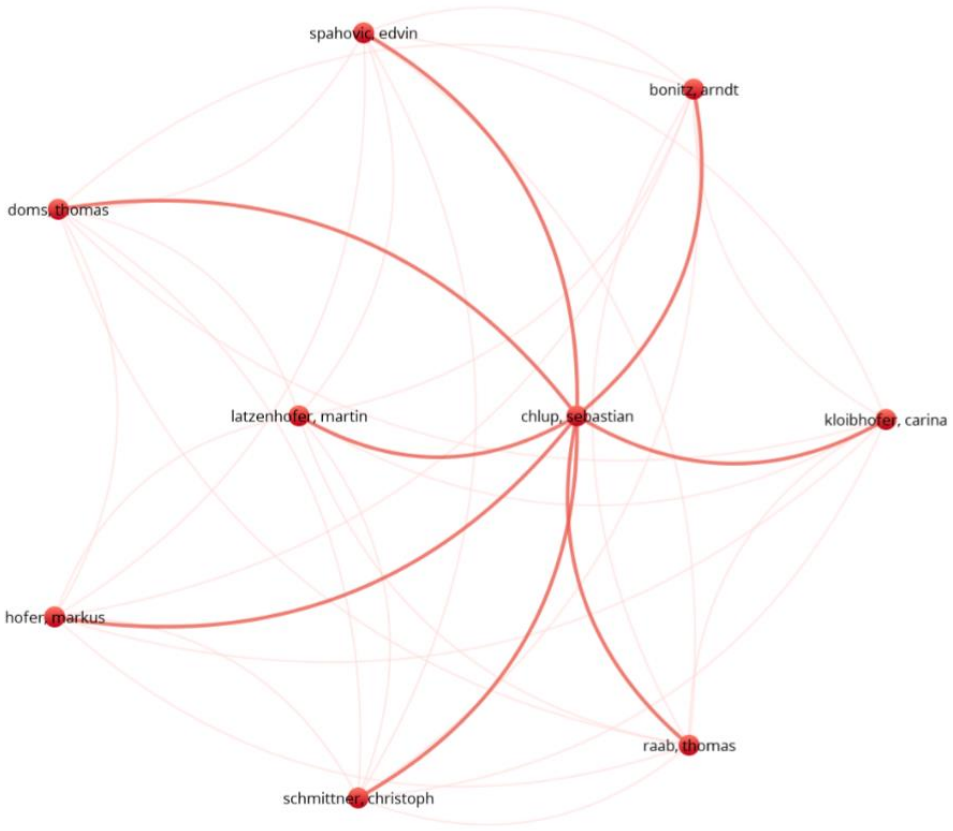


Figura 3 - Análise bibliométrica "*co-authorship authors*" grupo um – *Web of Science*
Fonte: Elaboração própria a partir do VOSviewer

No que diz respeito ao conjunto de cinco artigos compostos pelas keywords “portfolio management”, "risk management", “cybersecurity” os autores identificados pela análise bibliométrica e a forma como se relacionam entre si estão ilustrados na Figura 4.

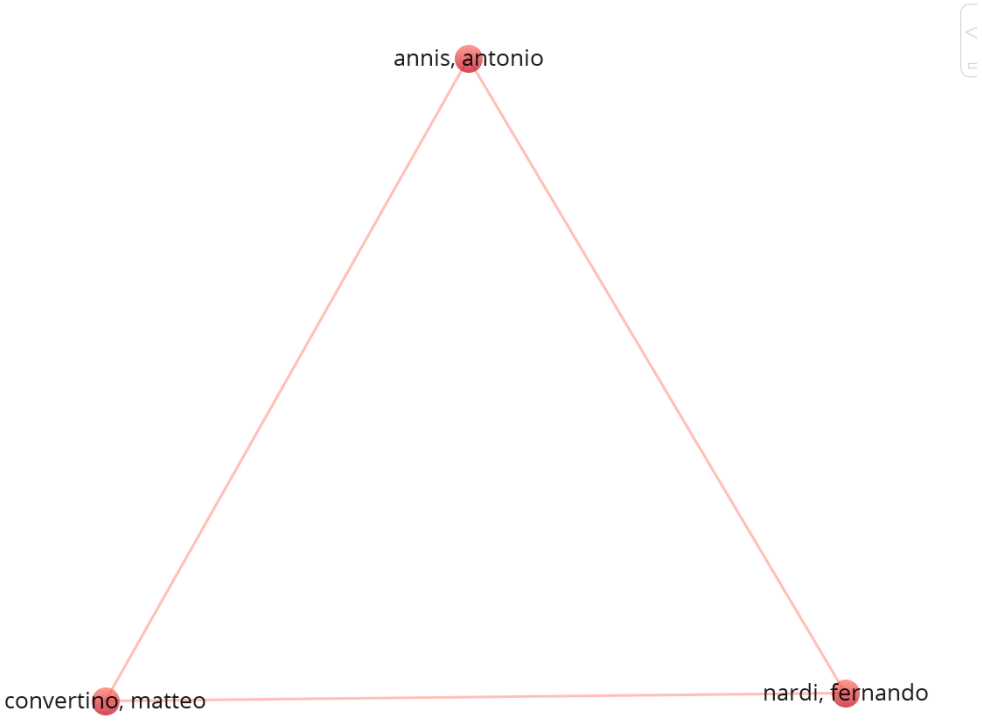


Figura 4 - Análise bibliométrica "*co-authorship authors*" grupo dois – *Web of Science*
Fonte: Elaboração própria a partir do VOSviewer

2.1.1.2 *Science Direct*

No que diz respeito à análise dos autores dos 62 artigos recolhidos no *Science Direct* para o grupo um, não se encontram interligações entre os autores. Considerando essa situação, mais uma vez optou-se pela análise do tipo *cluster* tendo-se encontrado, como ilustrado na Figura 5 um maior relacionamento entre autores.

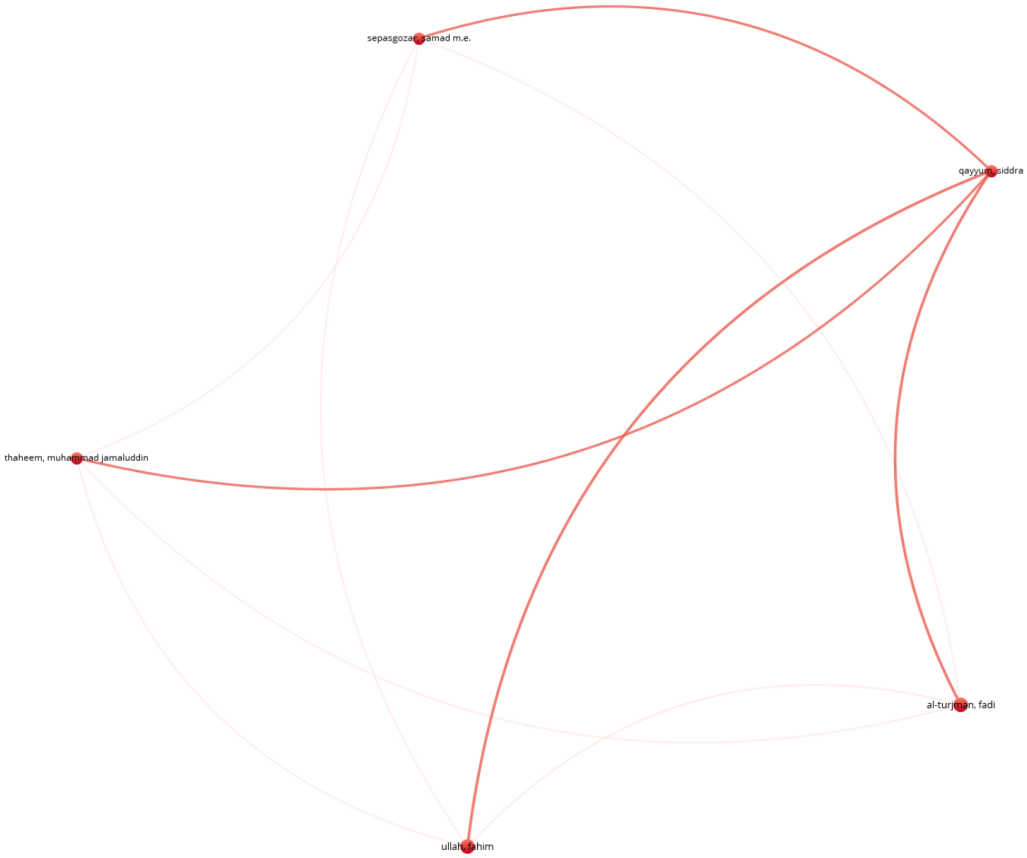


Figura 5 - Análise bibliométrica "*co-authorship authors*" grupo um – *Science Direct*
Fonte: Elaboração própria a partir do VOSviewer

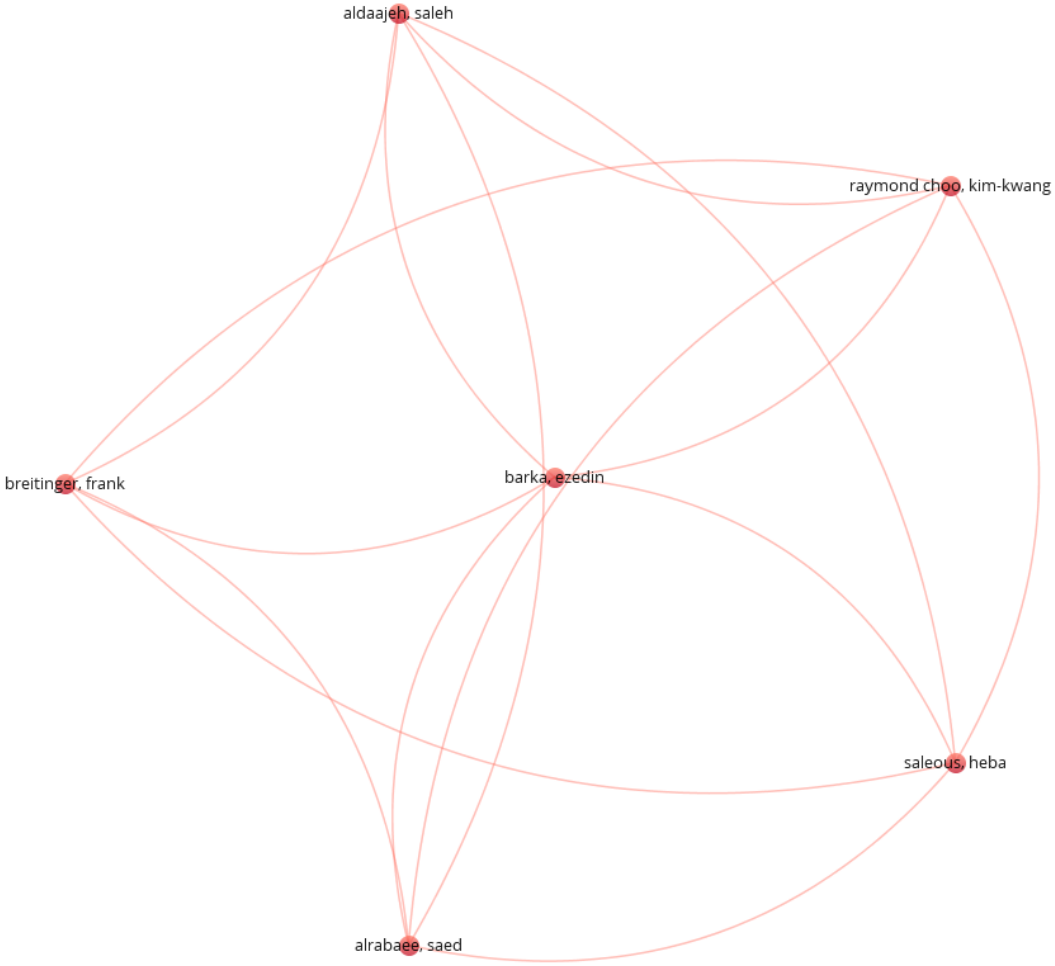


Figura 6 - Análise bibliométrica "*co-authorship authors*" grupo dois – *Science Direct*
Fonte: Elaboração própria a partir do VOSviewer

Dos 15 artigos encontrados no grupo dois, a realização da análise bibliométrica por autores destacou seis autores (ilustrados na Figura 6).

2.1.2 Análise Bibliométrica por Países

A análise bibliométrica por países, apenas está disponível para a base de dados da *Web of Science*, ainda assim é possível verificar que se destacam 14 países no conjunto de *keywords* do grupo um.

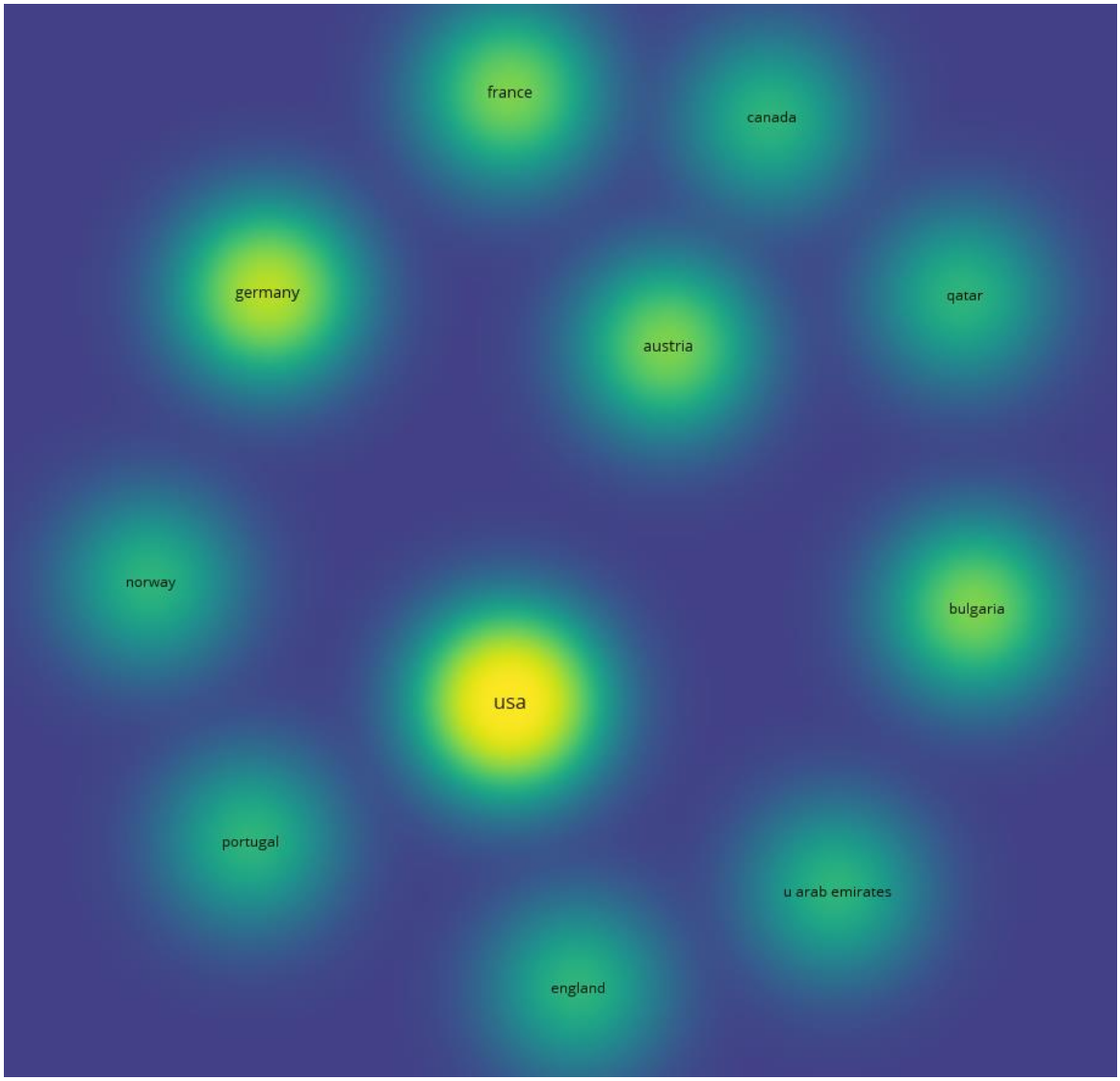


Figura 7 - Análise bibliométrica por países. grupo um
Fonte: Elaboração própria a partir do VOSviewer

Como se pode verificar pela Figura 7, os países que mais publicam sobre o tema em estudo, são Estados Unidos da América, seguindo-se a Alemanha, Áustria e a França.

Para o segundo grupo de *keywords*, como é possível verificar na Figura 8, a mesma análise revelou que apenas países como os Estados Unidos da América, Itália, Grécia e Alemanha publicam sobre o tema em questão.

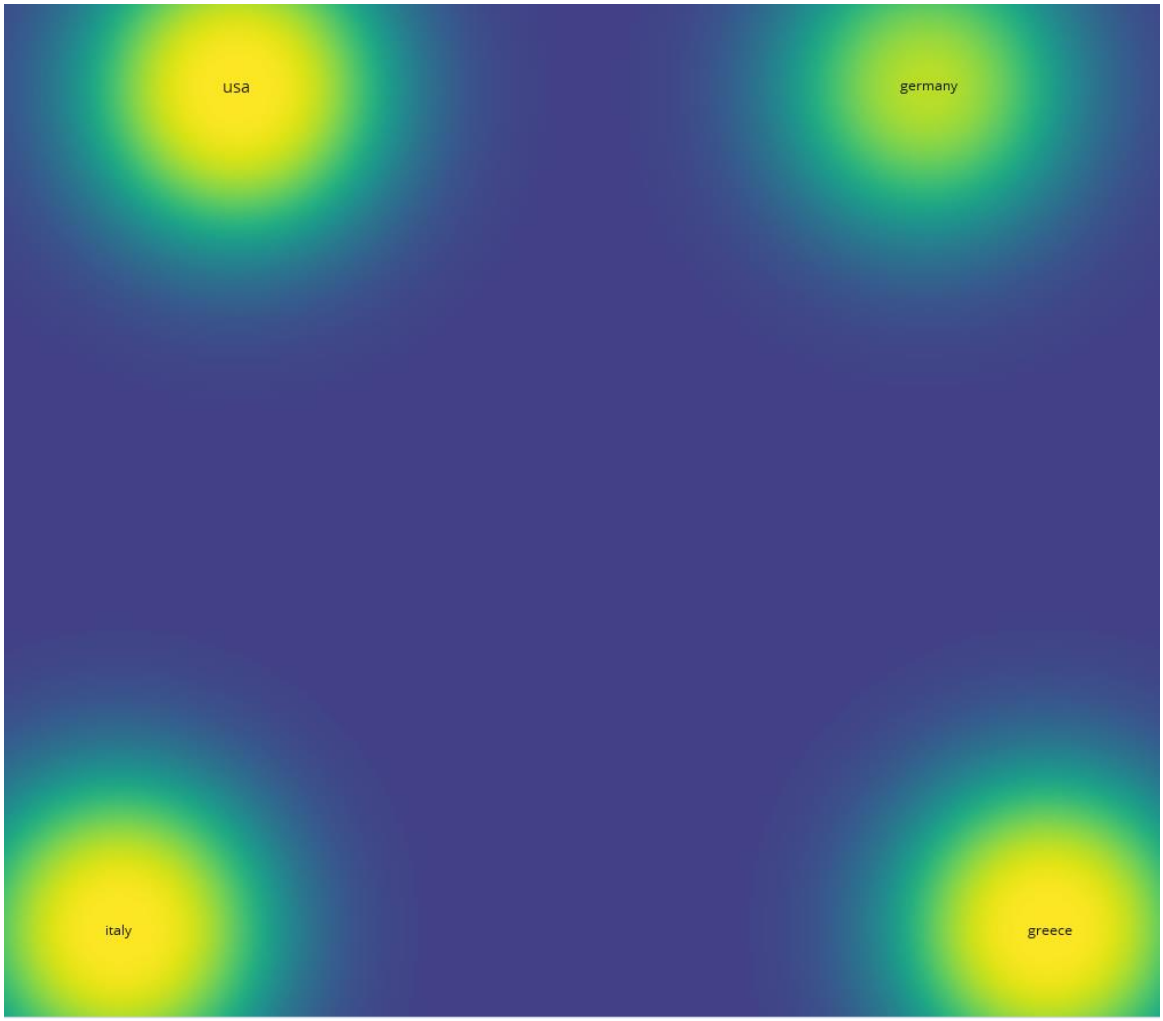


Figura 8 - Análise bibliométrica por países grupo dois
Fonte: Elaboração própria a partir do VOSviewer

2.1.3 Análise Bibliométrica por *Keywords*

A análise bibliométrica da presente dissertação termina com a análise dos artigos recolhidos do *Science Direct* para os dois grupos de *keywords*. Como referido anteriormente o *Web of Science* não permite a realização de análise bibliométrica por *co-occurrence keywords*.

2.1.3.1 *Science Direct para o grupo um de keywords*

Para a realização da análise da coocorrência de todas as *keywords* utilizadas nos artigos retirados do *Science Direct*, apenas foram consideradas as *keywords* com uma ocorrência mínima de duas vezes, e deste modo identificados os cinco *clusters* principais, conforme ilustrado na Figura **9**.

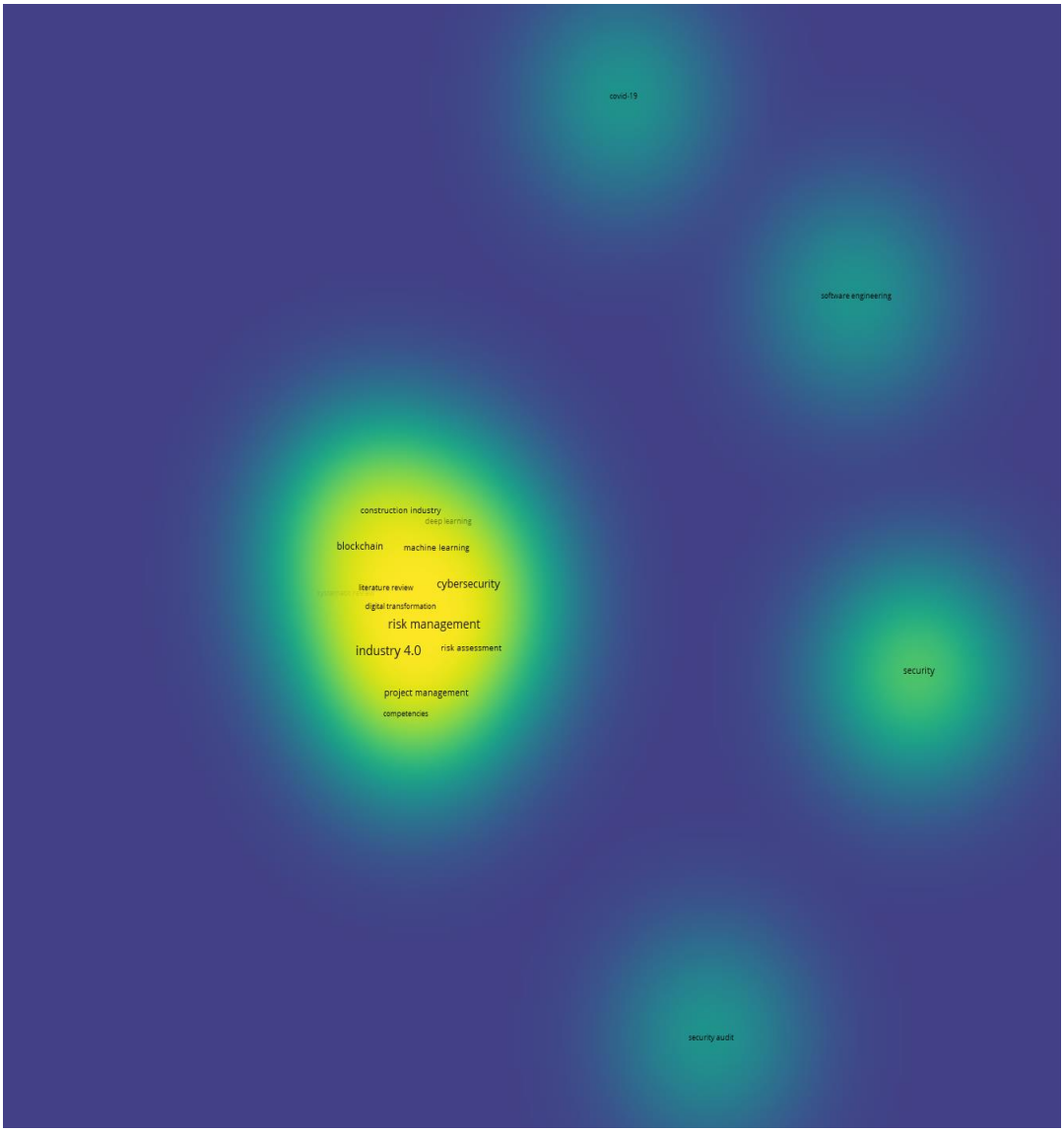


Figura 9 - Análise bibliométrica "*co-occurrence keywords*" grupo um - *Science Direct*
Fonte: Elaboração própria a partir do VOSviewer

Uma vez que um dos clusters apresenta uma maior densidade, procedeu-se à análise dos resultados, que permitiu verificar que, utilizando a mesma ocorrência mínima acima identificada, é possível observar três *clusters* de rede principais (Figura **10**, Figura **11** e Figura **12**), onde se verifica a existência das *keywords* utilizadas para a realização da metodologia da revisão da literatura, "*risk management*", "*cybersecurity*", "*project management*". Com a análise dos *clusters* é possível fortalecer, tal como sucede na revisão de literatura, que apenas a gestão de risco permite a analisar uma existência de gestão de projetos em cibersegurança.

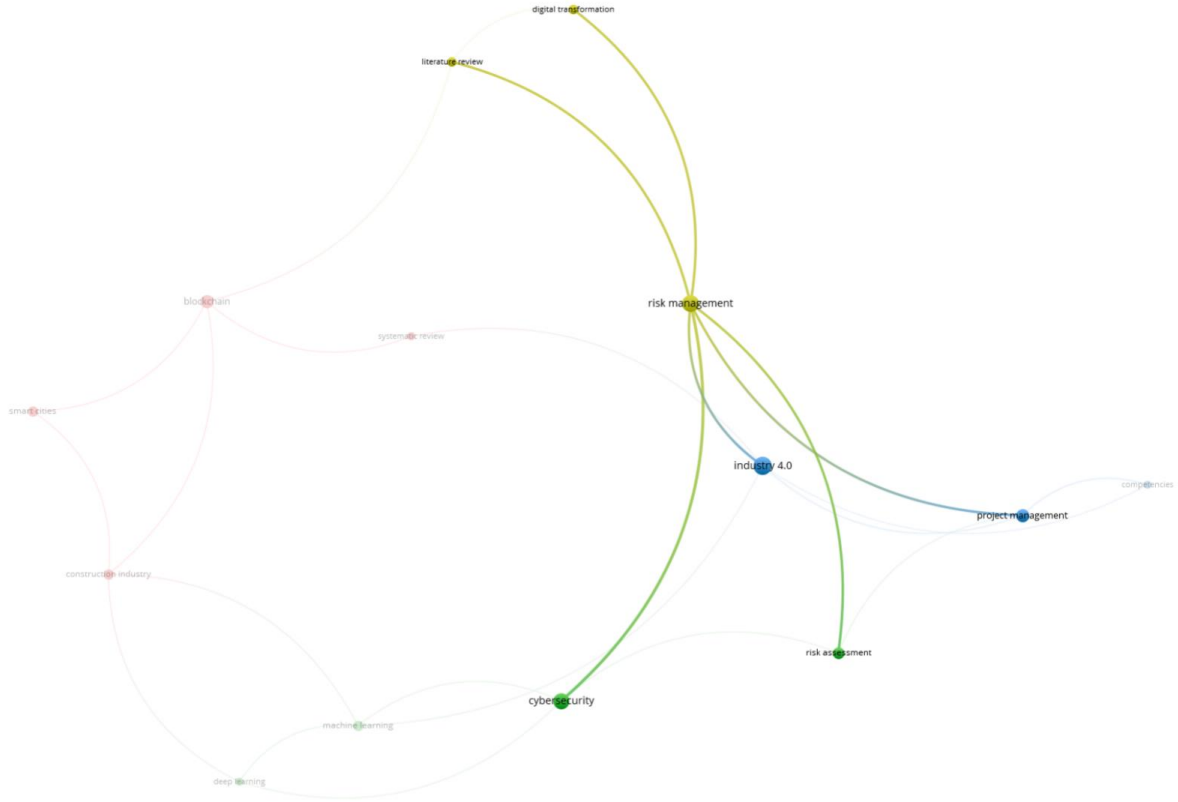


Figura 10 - *Cluster* focado na palavra "*risk management*" grupo um – *Science Direct*
Fonte: Elaboração própria a partir do VOSviewer

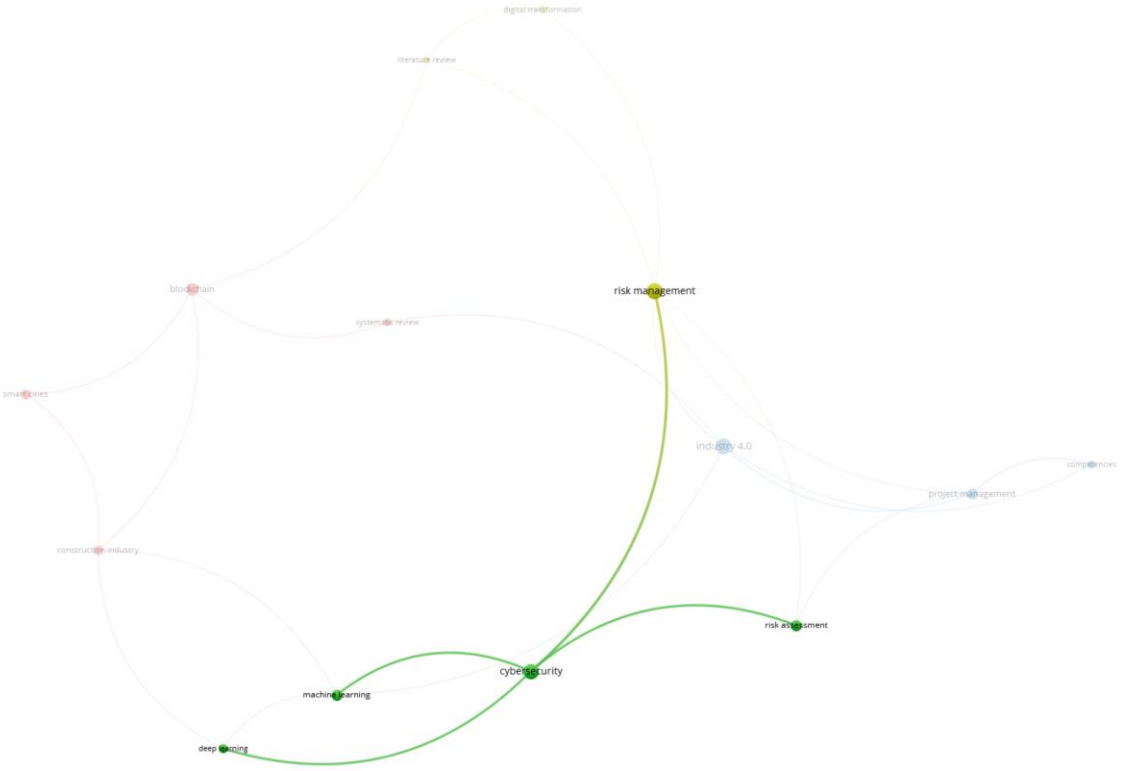


Figura 11 - *Cluster* focado na palavra "*cybersecurity*" grupo um – *Science Direct*
Fonte: Elaboração própria a partir do VOSviewer

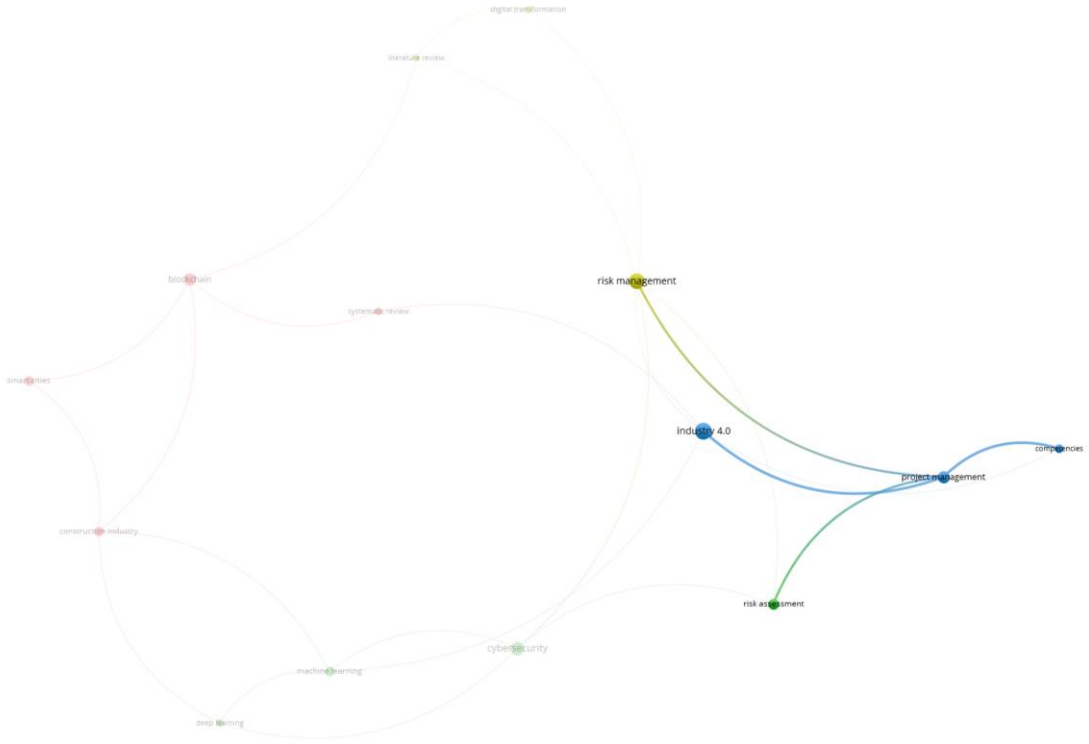


Figura 12 - *Cluster* focado na palavra "*project management*" grupo um – *Science Direct*
Fonte: Elaboração própria a partir do VOSviewer

2.1.3.2 *Science Direct para o grupo dois de keywords*

Utilizando a mesma ocorrência mínima de duas vezes para as *keywords* do grupo dois, e tal como ilustrado na Figura **13**, obtiveram-se seis *clusters*.

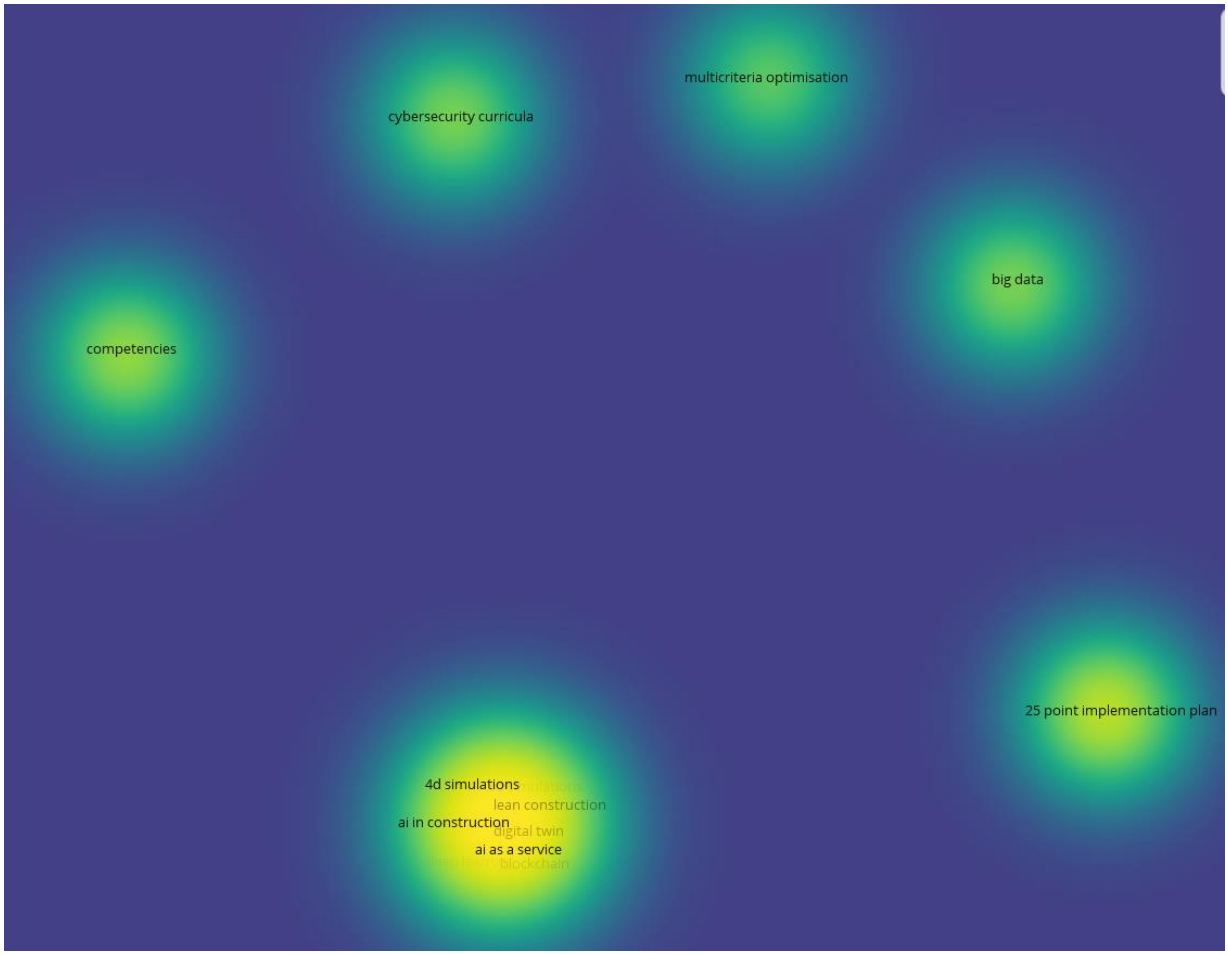


Figura 13 - Análise bibliométrica "*co-occurrence keywords*" grupo dois - *Science Direct*
Fonte: Elaboração própria a partir do VOSviewer

Ao contrário do realizado na análise para o grupo um, a análise do *cluster* com maior intensidade não fornece informação referente às *keywords* que compõe o grupo dois. Dito de outra forma as palavras como "*project management*", "*cybersecurity*" e "*portfolio*" são representadas em *clusters* de densidade baixa o que significa que são pouco usadas em conjunto, reforçando a inexistência de projetos de investigação que juntam esses temas/áreas.

2.1.4 Análise dos *Journals*

No que diz respeito à utilização da base de dados do *Scopus*, foi possível analisar que dos 28 *journals* encontrados no grupo um de *keywords*, oitoo deles encontram-se classificados no 1º quartil, dos quais se destacam o "*International Journal of Project management*" com uma avaliação de 99%, o "*Climate Risk Management*", avaliado em 98% e o "*Journal of Flood Risk Management*" com 94%.

Realizando uma avaliação aos *journals* classificados no segundo quartil, verifica-se que apenas quatro se encontram nessa classificação sendo o "*International Journal of Informations Systems and Project Management*", com 74% e o "*Cybersecurity*" com 63% os que mais se destacam.

No que diz respeito ao grupo dois, foi possível analisar que dos 30 *journals* referentes às *keywords*, 10 deles estão classificados no 1º quartil, destacando-se, com 97% o "*International Journal of Project Management*" e o "*Journal Cybersecurity*", com 95% o "*Journal of Flood Risk Management*".

No 2º quartil foram avaliados com cinco resultados, destacam-se com uma percentagem de 70% e de 64% o "*International Journal of Information Systems and Project Management*" e "*International Journal of Information Technology Project Management*", respetivamente.

2.2 Gestão de Projetos

Ao longo da história, grandes empreitadas da humanidade, como a grande Pirâmide de Gizé, a Grande Muralha da China ou o Coliseu, foram criadas graças ao engenho dos recursos humanos que tiveram de assumir o papel de gestores de projeto e assim pensar cuidadosamente em todos as fases do projeto. Para cada um dos projetos referidos, foi necessário gerir os recursos humanos alocados a cada um dos mesmos, garantir o seu financiamento e por fim, garantir que o projeto cumpria com todos os requisitos a fim de atingir os objetivos propostos (Seymour & Hussein, 2014).

Kwak, (2011) identificou quatro períodos na história da gestão projeto: antes de 1958, 1958 – 1979, 1980 – 1994 e 1995 até o presente, afirmando que as origens da gestão de projetos moderno começaram entre 1900 e 1950. Durante esse período, a gestão de projetos passou de um sistema "*craft system*" para "*human relations administration*". Naquela época, os sistemas de transporte e telecomunicações permitiram uma maior mobilidade, a alocação eficaz de recursos e a agilidade da comunicação, esta época ficou marcada pela inserção do Gráfico de *Gantt* e pelo *Work Breakdown Structure* (WBS).

No segundo período, 1958-1979, como define Carayannis (2005) e Kwak (2011),1950 houve avanço tecnológico significativo, marcado pelo "*application of management science*". Durante este período, ocorreram avanços tecnológicos significativos, tal como o projeto Apollo da NASA que marcou um evento histórico da humanidade (NASA, 1969). Neste segundo período temporal, foram introduzidas também as ferramentas de gestão de projetos como como P*rogram Evaluation and Review Technique* (PERT) e *Critical Path Method* (CPM) (Meredith, J. R. e Mantel, Jr, 2006).

O terceiro período de 1980 a 1994, representa a revolução do setor de *Information Technology* (IT)/*Information Security* (IS) introduzindo o uso de computador pessoal com alta eficiência na gestão e controlo de cronogramas de projetos complexos (Leiner et al., 2009). O *software* de gestão de projetos tornou-se amplamente disponível, o que possibilitou qua as técnicas de gestão de projetos fossem de fácil acesso.

O último período que Kwak, (2011) identificou que de 1995 até ao presente, onde a tecnologia continua a ser uma força motriz para a mudança e tem um grande impacto nas atividades dos gestores de projeto. De acordo com António Miguel (2019), a *Internet* começou a mudar praticamente todas as práticas de negócios, o que possibilitou à comunidade de gestão de projetos adotar a tecnologia da internet de forma a tornar-se mais eficiente no controlo e gestão de vários aspetos dos projetos.

Atualmente, o desenvolvimento da Gestão de Projetos tem sido amplamente reconhecido, e desempenha um papel vital na gestão de vários projetos numa organização (Gholamzadeh Chofreh et al., 2016). Assim sendo, é necessário esclarecer alguns conceitos neste âmbito, como suporte à gestão de projetos.

Assim sendo, um projeto pode assumir várias definições como:

- um conjunto de atividades e tarefas que contenham um objetivo específico a concluir dentro de determinadas especificações, com datas de início e de fim definidas. No caso de ser aplicável, o projeto deve ter limites de financiamento, alocação de recursos humanos e não humanos (por exemplo dinheiro, pessoas, equipamentos) e contendo várias linhas funcionais, isto é, são multifuncionais (Kerzner, 2009);
- um esforço temporário empreendido para criar um produto, serviço ou resultado único. A natureza temporária dos projetos significa que eles têm um início e um fim definidos. A rescisão ocorre quando os objetivos do projeto são alcançados, quando os mesmos não podem ser atingidos, ou quando a necessidade do projeto deixa de existir (PMI, 2017a);
- um "conjunto único de processos consistindo em atividades coordenadas e controladas com datas de início e de fim, desenvolvidas para alcançar um objetivo" (ISO 21500, 2021);
- um esforço único, temporário, multidisciplinar e organizado para alcançar os entregáveis de acordo com os requisitos e restrições predefinidas. O alcance dos objetivos definidos no projeto requer entregáveis para atender aos requisitos específicos, incluindo as restrições como tempo, custo, recursos e padrões ou requisitos de qualidade (IPMA, 2015).

Um projeto assume determinadas características, tais como (António Miguel, 2019):

- De projeto para projeto, os requisitos são diferentes fazendo com que estes se tornem únicos;
- Todos os projetos têm uma data de início e de fim, o que faz com que sejam temporários;
- A diversidade de objetivos dos intervenientes leva a alguma complexidade nos projetos;
- Existem várias incertezas ao longo do projeto, pelo que o risco está presente;
- Um projeto está limitado em termos de tempo, capital e recursos;

- Os esforços realizados entre diferentes áreas da organização, ou entre organizações diversas que requerem integração.

O conceito de gestão de projetos centra-se assim na aplicação de métodos, ferramentas, técnicas e competências, podendo ser executada através de processos e aplicação de várias fases do ciclo de vida do projeto como início, organização e preparação, execução do trabalho e encerramento (IPMA, 2015).

O projeto será dividido, de acordo com cada um dos requisitos do DL n.º65/2021, em diferentes projetos, formando, dessa forma um portefólio com necessidade de ser gerido.

2.3 Gestão de Portefólios

O conceito de "portefólio" tem diferentes significados, dependendo de como é usado em vários contextos. O significado principal tem a ver com a ideia de uma coleção ou coleção de "coisas" (Wheelwright, S. C., & Clark, 1982). Por outro lado, a ISO 21502 (2020) define o termo como um conjunto de projetos, programas, subportefólios e operações geridas como um grupo de modo a satisfazer objetivos estratégicos de negócio.

De acordo com o PMI (2013), uma organização pode ter mais do que um portefólio, cada um abordando estratégias e objetivos organizacionais exclusivos. As iniciativas propostas são estruturadas à medida que portefólios e componentes são identificados, avaliados, selecionados e autorizados. Além disso, os portefólios podem conter subportefólios.

A gestão de portefólios consiste numa gestão coordenada de um ou mais portefólios que visa atingir os objetivos estratégicos da organização (ISO 21502, 2020; PMI, 2013b, 2017a).

A gestão de portefólios refere-se a uma coleção de projetos ou programas e outros trabalhos agrupados para facilitar uma gestão eficaz. Uma gestão de portefólios pode ser composta por um ou mais portefólios, agrupados pelo seu nível de importância, cada um pode conter um ou mais projetos ou então um ou mais programas que por sua vez produzem projetos (PMI, 2013b, 2017a, 2017b).

Através da gestão de portefólios os diferentes projetos são controlados e modificados ao longo do tempo, de forma a melhorar a sua eficácia e eficiência, permitindo, assim obter melhores resultados com menos recursos. Os recursos são então distribuídos pelos diferentes projetos de forma a otimizar e evitar desperdício de custos. Todo este processo é realizado pelo gestor de portefólio que

é o responsável pela coordenação dos diferentes projetos que estão a decorrer em simultâneo, ou seja a realização da gestão de portefólios (Meskendahl, 2010; Robert G. Cooper, Scott J. Edgett, Elko J. Kleinschmidt, 1999).

Os objetivos da gestão de portefólios, segundo o PMI (2017a), são centrados na orientação das decisões de investimento organizacional, na seleção da combinação ideal de programas e projetos de forma a cumprir com os objetivos estratégicos, o fornecimento da transparência na tomada de decisão, a priorização da alocação dos recursos humanos e físicos, o aumento da probabilidade de alcance do retorno desejado sobre o investimento e a centralização da gestão de risco agregado a todos os componentes.

Em síntese, a gestão de portefólio visa combater o vinculo existente entre o desenvolvimento dos processos estratégicos e a implementação da estratégia, implementando o planeamento estratégico da organização com base na gestão de projetos (Meskendahl, 2010).

2.3.1 Diferenças entre Gestão de Portefólios e a Gestão de Projetos

Como referido anteriormente, a Gestão de Projetos consiste na gestão de um determinado projeto, sendo ele com um início e fim, enquanto a Gestão de Portefólios consiste na gestão de diversos projetos em simultâneo os quais podem estar em constante renovação.

Assim sendo, as diferenças estão relacionadas com diversos fatores representados na Tabela 1:

	Projetos	**Portefólios**
Âmbito	O âmbito é progressivamente elaborado ao longo do ciclo de vida do projeto. São os requisitos para atingir os objetivos.	Dispõe de um âmbito capaz de suportar os objetivos estratégicos da organização.
Alterações	São esperadas mudanças e implementação de processos de forma a gerir e controlar as alterações.	São monitorizadas continuamente nos ambientes internos e externos mais abrangentes.
Planeamento	A informação é elaborada progressivamente em planos detalhados ao longo do ciclo de vida do projeto.	São criados e mantidos processos e a comunicação relativa ao portfólio agregado.

Gestão	A equipa de projeto é gerida para satisfazer os objetivos estabelecidos.	Os gestores de portefólio coordenam e gerem os recursos que vão apoiar na gestão do portefólio.
Sucesso	Medido pela qualidade do projeto, pelo cumprimento dos prazos, do orçamento e pelo grau de satisfação do cliente.	Medido em termos de desempenho do investimento agregado e da realização dos benefícios do portefólio.
Monitorização	Os gestores do projeto monitorizam e controlam a produção dos produtos, serviços ou resultados que o projeto pretende atingir.	Os gestores de portefólio monitorizam as alterações estratégicas e agregam a alocação dos recursos, resultados do desempenho e risco do portefólio.

Tabela 1 - Diferenças entre Gestão de Projetos e Gestão de Portefólios,
Fonte: Adaptado de António Miguel (2019); PMI, (2017a)

A gestão do risco tem um enfoque diferente conforme se esteja numa ótica de gestão de projetos ou de gestão de portefólios.

A gestão de risco na gestão de projetos tem como objetivo prevenir uma derrapagem na execução do projeto proposto, assim como cumprir com as variáveis impostas pelo triângulo de ferro (tempo, custo e âmbito) (PMI, 2017a). Por outro lado, a gestão de risco do portefólios foca-se na gestão dos riscos abrangentes a todos os projetos inseridos no portefólio, de modo a prevenir riscos que vão contra a estratégia e objetivos da organização (PMI, 2013b, 2017b).

A abordagem da gestão de risco está em linha com a exigência do cumprimento dos requisitos impostos pelo DL n. º65/2021 evitando a aplicação de coimas pelo Estado e pela Autoridade Nacional de Cibersegurança (Assembleia da República, 2018). No que diz respeito à gestão de risco na segurança da informação, esta temática torna-se um requisito imposto pelo Decreto-Lei no 65(2021).

Este projeto avançado integrado no mestrado em gestão de projetos é explorado numa ótica de gestão do risco. Daí que esta temática seja explorada de seguida para posteriormente se fazer a sua ligação com o quadro normativo.

2.4 Gestão de Risco

De acordo com António Miguel (2019) um risco é uma condição ou evento incerto que pode provocar um impacto positivo ou negativo sobre um ou vários objetivos do projeto. No que diz respeito à segurança da informação, um risco é uma circunstância ou evento razoavelmente identificável, com um efeito potencial adverso à segurança das redes e dos sistemas de informação (Assembleia da República, 2018). Por sua vez, a gestão de risco permite às organizações a tomada de decisão de forma priorizada e informada, no contexto da segurança da informação. Estas decisões devem, sempre, considerar a confidencialidade, disponibilidade e integridade na prestação do bem ou serviço (CNCS, 2019).

Na Gestão de Projetos, e segundo o PMI (2017) um risco é definido como "um evento ou condição incerta que, se ocorrer, tem um efeito positivo ou negativo em um ou mais objetivos do projeto". A definição de risco compreende tantos os eventos incertos (ameaças), que afetam negativamente o projeto, como os que podem provocar efeitos positivos no decorrer do projeto (oportunidades).

O risco de um projeto tem como origem a incerteza existente em todos os projetos, por outro lado, os riscos conhecidos são aqueles que são identificados e analisados, possibilitando assim um planeamento de respostas (Alhawari et al., 2012; PMI, 2013a, 2017a).

Os riscos individuais do projeto são diferentes do risco geral do projeto. O risco geral do projeto representa o efeito da incerteza no projeto como um todo, tornando-se mais do que a soma dos riscos individuais do projeto, uma vez que inclui todas as fontes de incerteza existentes no projeto (PMI, 2009, 2013a, 2017a, 2019).

As organizações definem o risco como um efeito da incerteza nos projetos e objetivos definidos, estando dispostas a aceitar vários graus de riscos, dependendo da sua atitude em relação aos riscos. Essa atitude pode ser influenciada por vários fatores que são classificados de forma ampla em três definições (Alhawari et al., 2012; ISO Guide 73, 2009; NP ISO 31000:2009, 2013; PMI, 2009, 2013a, 2017a, 2019):

- **Apetite do risco (*risk appetite*):** grau de incerteza que uma entidade está disposta a aceitar.
- **Tolerância ao risco (*risk tolerance*):** quantidade ou o volume de risco que uma organização ou um indivíduo está disposto a tolerar.
- **Limite do risco (*risk threshold*):** a medida de variação aceitável em torno de um objetivo que reflete o apetite de risco da organização e das partes interessadas.

Por consequência, a Gestão de Riscos consiste no conjunto de processos, técnicas e ferramentas que têm como objetivo identificar, analisar e responder aos riscos de um projeto (PMI, 2009). Os resultados da gestão de riscos do projeto devem ser considerados, uma vez que estes podem modificar e ter impacto (PMI, 2009):

- Na estimativa dos requisitos dos recursos, custo e duração;
- Na avaliação do impacto das alterações do âmbito proposto;
- No planeamento ou replaneamento da estratégia de avanço do projeto;
- Na alocação dos recursos para as tarefas do projeto;
- Na realização de relatórios de projetos.

A Gestão de Riscos dos projetos, inclui normalmente os processos de planeamento, identificação, análise, planeamento e implementação de respostas e monitorização dos riscos. Estes processos têm como objetivo o aumento da probabilidade e/ou impacto positivo dos riscos, diminuindo a probabilidade e/ou impacto negativo dos mesmos, a fim de otimizar o sucesso do projeto.

Ao longo do tempo foram implementadas várias metodologias de gestão de riscos de projetos e de segurança de informação, como por exemplo:

- ISO/IEC 31000 – Gestão do Risco – Linhas Orientadoras: é a primeira norma global de gestão do risco e abrange todos os tipos de risco: financeiros, económicos, crises nacionais e mundiais. Estabelece princípios e linhas orientadoras que visam auxiliar qualquer tipo de organização a desenvolver e a implementar a sua própria gestão do risco adequada às suas exigências e características (NP ISO 31000:2009, 2013).
- IEC 31010 – Gestão do Risco – Técnicas de Avaliação do Risco: é uma norma complementar da ISO 31000, dando orientação sobre a seleção e aplicação de técnicas para a avaliação do risco, contribuindo deste modo para a gestão do risco (NP ISO 31010, 2009).
- ISO/IEC 27005:2008 – Tecnologia de Informação – Técnicas de Segurança – Gestão do Risco de Segurança da Informação: atualizada em julho de 2018, a norma foi concebida para auxiliar na implementação de um Sistema de Gestão de Segurança de Informação (SGSI) baseado numa abordagem de gestão do risco. (ISO/IEC 27005, 2018).
- *Practice Standard for Project Risk Management* (PMI): desenvolvido com o propósito de fornecer um padrão para a definição dos aspetos de gestão de riscos de projetos e para a aplicação de um padrão global (PMI, 2009).

A metodologia a adotar para o projeto avançado será a o *standard* da gestão de risco desenvolvido pelo PMI. A motivação para a escolha centra-se na sua aplicabilidade e simplicidade de

implementação nos projetos, pela maturidade e credibilidade da instituição e ainda pelo facto de a mesma ter sido desenvolvida ao longo de todo o ciclo de mestrado em gestão de projetos no qual este projeto é desenvolvido.

2.4.1 Metodologia da Gestão de Risco na Gestão de Projetos

Segundo o PMI (2017a) a gestão de risco do projeto inclui sete processos, sendo eles:

- **Planeamento da Gestão de Risco:** permite a definição dos processos necessários no planeamento da Gestão de Riscos;
- **Identificação dos riscos:** processo capaz de definir os riscos que podem afetar o projeto;
- **Análise qualitativa dos riscos:** processo de priorização de riscos para análise ou posterior análise, através da avaliação da sua probabilidade de ocorrência e impacto, assim como outras características;
- **Análise quantitativa dos riscos:** processo de análise numérico do efeito combinado dos riscos identificados e outras fontes de incerteza nos objetivos gerais do projeto;
- **Planeamento das respostas aos riscos:** processo de desenvolvimento de alternativas e ações que permitam a seleção de estratégias para lidar com a exposição geral aos riscos;
- **Implementação de respostas aos riscos:** processo de implementação dos planos desenvolvidos para a resposta ao risco;
- **Monitorização dos riscos:** processo de monitorização de implementação dos planos desenvolvidos para a resposta ao risco, acompanhar os riscos identificados, identificar e analisar novos riscos, avaliar a eficácia do processo;

A Figura 14 representa o ciclo de vida da gestão de risco, apresentando um fluxo de trabalho dedicado, processual e iterativo de atividades e processos, suportado e executado em toda a organização e dentro dos domínios de projeto. Devido à natureza evolutiva do risco, o ciclo de vida gestão de risco garante um fluxo de trabalho repetível de processos que suportam a tomada de decisões estratégicas. Todas essas atividades são realizadas de forma integrada dentro e entre os domínios do projeto (António Miguel, 2019; PMI, 2019).

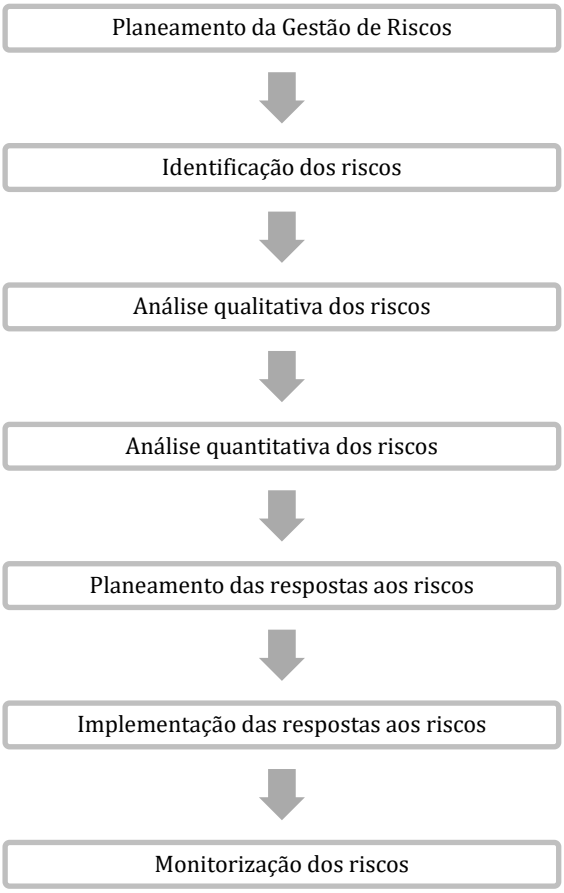


Figura 14 - Framework do ciclo de vida da Gestão de Risco,
Fonte: Adaptado de PMI (2019)

O fluxo de trabalho iterativo do ciclo de vida da gestão de riscos é incorporado numa estrutura de execução estratégica em que a gestão de projetos está vinculada aos fundamentos culturais organizacionais, recursos e ao uso de funções organizacionais ou domínios de desempenho. Entende-se que, uma vez encerrado um projeto, o processo de gestão de riscos termina e as lições aprendidas são documentadas. A estrutura permite que os processos gerais de risco sejam implementados por meio de um plano de gestão de risco em cada domínio (PMI, 2019).

2.4.1.1 Planeamento da Gestão do Risco

O Planeamento da Gestão do Risco consiste no processo de definição das atividades de gestão de risco que devem ser aplicadas ao longo do ciclo de vida da gestão dos projetos. Esta fase garante que o grau, tipo e a visibilidade da gestão de riscos sejam proporcionais tanto aos riscos quanto à importância do projeto para a organização. O plano da gestão do risco é vital na comunicação, obtenção de acordo e apoio das partes interessadas de modo a garantir que o processo de gestão de riscos seja apoiado e executado de maneira efetiva (PMI, 2009, 2013a, 2019).

A etapa de planeamento e gestão de riscos é constituída por um conjunto de tarefas que permite descrever como deve ser estruturada e realizada a gestão de risco, podendo esta incluir alguns (ou todos) os elementos (António Miguel, 2019):

- **Estratégia:** abordagem geral para a gestão de riscos do projeto;
- **Metodologia:** abordagens específicas, ferramentas e fontes de dados utilizadas para a realização da gestão de risco;
- **Papéis e Responsabilidades:** definição da constituição da equipa responsável por cada uma das atividades de gestão de risco, distribuição de tarefas e respetivas responsabilidades;
- **Orçamento:** identificação dos custos necessários para a realização das atividades da gestão de risco, os quais serão imputados aos custos do projeto;
- **Prazo:** definição de um cronograma com as atividades que serão desenvolvidas na gestão de risco e da frequência com que as mesmas serão realizadas;
- **Categorias de riscos:** definição dos meios para agrupar os riscos do projeto de forma a contribuir para a identificação sistemática e detalhada dos riscos. As categorias do risco podem ser estruturadas através de uma ferramenta de estrutura e decomposição dos riscos (*Risk Breakdown Structure*);
- **Definições de probabilidade e impacto dos riscos:** matriz de condições que permitem uma classificação qualitativa dos riscos;
- **Matriz de probabilidade e impacto:** mapeamento da probabilidade de ocorrência de cada risco e respetivo impacto, caso o risco ocorra;
- **Formatos de relatórios:** formato dos registos do risco, assim como qualquer outro documento exigido.
- **Monitorização dos riscos:** descrição de como serão registados e rastreados os riscos assim como o registo das atividades e lições aprendidas com o processo de gestão de risco.

2.4.1.2 Identificação dos riscos

O processo de identificação dos riscos consiste na produção de uma lista constituída por todos os riscos possíveis capazes de materializar consequências que possam prejudicar o alcance dos objetivos definidos para o projeto (António Miguel, 2019).

É necessário que durante a realização desta fase se desenvolva documentação com registos claros dos riscos identificados, evidenciado as suas características, informações causas e efeitos, possíveis

respostas aos riscos, reconhecendo de certa forma a possibilidade da ocorrência de novos riscos, consequência das ações realizadas anteriormente (PMI, 2009, 2019).

Desta forma, este processo visa em determinar os riscos capazes de afetar o projeto, bem como a criação da documentação com as respetivas características do risco.

Para auxiliar na realização do processo existem diversas técnicas e ferramentas desenvolvidas amplamente utilizadas para identificação de problemas como é o caso do *brainstorming*, *checklist*, diagramas de causa efeito, análise SWOT, entre outras (António Miguel, 2019; PMI, 2009, 2019):

Brainstorming

O objetivo do brainstorming é obtenção de uma lista completa dos riscos do projeto, realizada através de reuniões que obedecem a regras bem definidas. As reuniões devem ser lideradas e conduzidas por um recurso humano externo ao projeto (facilitador), de modo que as ideias sobre os riscos no projeto sejam geradas de forma livre e estruturada, utilizando técnicas de entrevista em grupo (António Miguel, 2019; PMI, 2009, 2019).

Técnica *Delphi*

A presente técnica baseia-se numa pesquisa anônima facilitada com o objetivo de identificar riscos. Inicialmente, são reunidas pelo facilitador as respostas iniciais da equipa, e distribuídas sem atribuição a todo o grupo de trabalho, cabe ao grupo de trabalho rever as contribuições (António Miguel, 2019; PMI, 2009).

A técnica Delphi ajuda a reduzir a parcialidade nos dados e evitando que estes influenciem indevidamente o resultado(António Miguel, 2019).

Análise SWOT

A técnica SWOT examina o projeto do ponto de vista das suas **forças e fraquezas, oportunidades e ameaças** (SWOT), com o objetivo de aumentar a abrangência dos riscos identificados, incluindo os riscos gerados internamente (António Miguel, 2019).

Tal como esquematizado na Figura 15, a técnica inicia com a identificação das forças e fraquezas da organização, em seguida, identifica as oportunidades do projeto resultantes das forças da organização, assim como as ameaças decorrentes das fraquezas (PMI, 2013a).

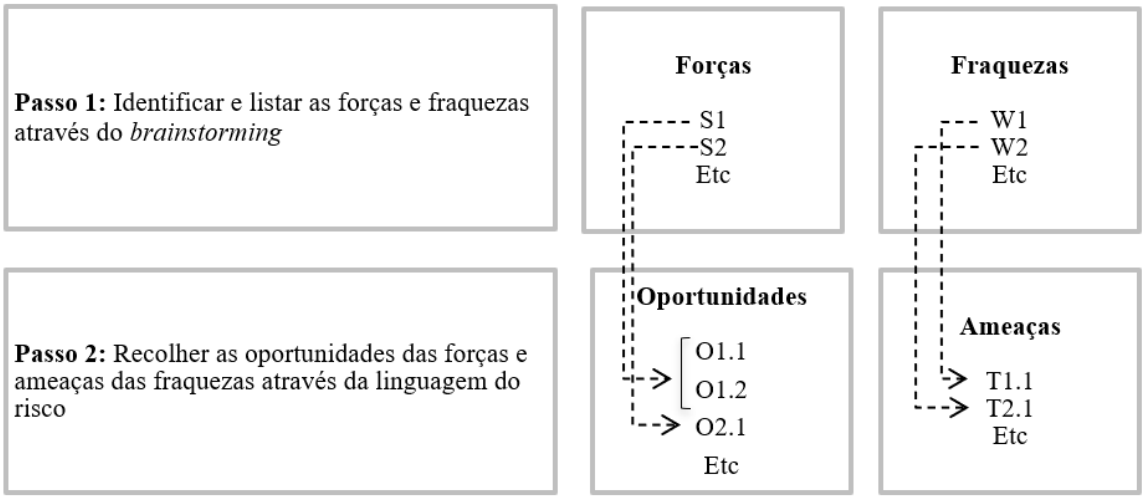


Figura 15 - Exemplo de uma estrutura de Análise SWOT,
Fonte: Adaptado de PMI (2009, 2019)

Registos dos Riscos

O principal resultado do processo de identificação dos riscos consiste na criação de um documento com os riscos identificados, a descrição dos riscos, análise qualitativa, plano de resposta aos riscos e o estado da monitorização (PMI, 2017a).

Checklists

As listas de verificação (*checklists*) são desenvolvidas tendo em conta as informações históricas e o conhecimento acumulado, através de projetos anteriormente realizados. O nível mais baixo da *risk breakdown structure* (RBS) também pode ser usado como uma lista de verificação (PMI, 2009, 2013a, 2019).

Apesar de uma *checklist* ter como o objetivo rapidez e simplicidade, é praticamente impossível criá-la de forma completa, uma vez que é necessário assegurar que a mesma não será utilizada com propósito de evitar o esforço da identificação adequada dos riscos. É importante que *checklist* seja revista periodicamente com o propósito de remover ou arquivar itens relacionados. Na fase de encerramento a lista dever ser revista para incorporar as lições aprendidas (António Miguel, 2019). Na Figura 16 é apresentado um exemplo de uma estrutura de *checklist*.

Categoria do risco	Subcategoria	Exemplos de Riscos	Esse risco pode afetar o projeto? **Sim, Não** **Não sei, Não se aplica**
1. Risco Técnico	1.1 Definição do âmbito	Mudanças do âmbito podem surgir durante o projeto	
		Âmbito redundante pode ser visível	
		Etc…	
	1.2 Interfaces técnicas	Etc…	

Figura 16 - Exemplo de uma *Checklist*,
Fonte: Adaptado (PMI, 2009, 2019)

Análise de Causa e Efeito

Os diagramas de causa e efeito, também conhecidos como diagramas de *Ishikawa* ou em espinha-de-peixe mostram as relações entre os efeitos do problema e as suas respetivas causas dos riscos. Este tipo de diagrama representa todos os tipos de causas e subcausas potenciais de um problema, assim como o efeito que cada uma das soluções apresentadas terá sobre o problema (António Miguel, 2019; PMI, 2017a, 2019).

Esta técnica apresenta em forma de diagrama as causas que contribuem para um determinado resultado/efeito. Cada causa principal pode ser dividida em diferentes subcausas. O diagrama identifica os riscos como aqueles eventos incertos que podem resultar na ocorrência do impacto (PMI, 2009). Um exemplo do diagrama subjacente a esta técnica é ilustrado na Figura 17.

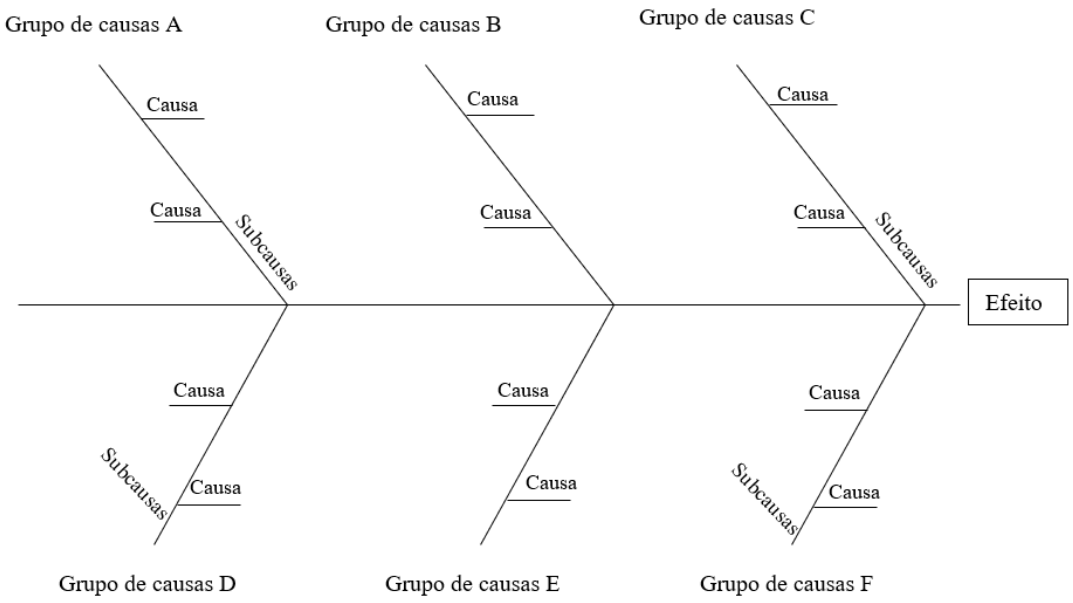


Figura 17 - Diagrama Causa e Efeito,
Fonte: Adaptado (António Miguel, 2019; PMI, 2009)

Registo de Lições Aprendidas

O Registo de Lições Aprendidas consiste na junção de informações relevantes para os riscos de um projeto, podendo ser construídos através da revisão de bases de dados de riscos que ocorreram em projetos anteriores. Este registo permite identificar a necessidade da definição de regras ou diretrizes para alinhar as diversas atividades do projeto(PMI, 2017a).

Risk Breakdowns Structure (RBS)

A estrutura de decomposição dos riscos consiste numa lista hierarquicamente organizada dos riscos identificados, onde estes se encontram agrupados de acordo com a sua origem (Hillson, 2002; PMI, 2019; Vitkin et al., 2010).

Esta estrutura apresenta uma série de vantagens, visto que se trata de uma visão sintética dos riscos e é compatível com a natureza evolutiva e com a dinâmica dos riscos do projeto (Mehdizadeh et al., 2012).

Na Figura 18 é possível observar um exemplo de um RBS.

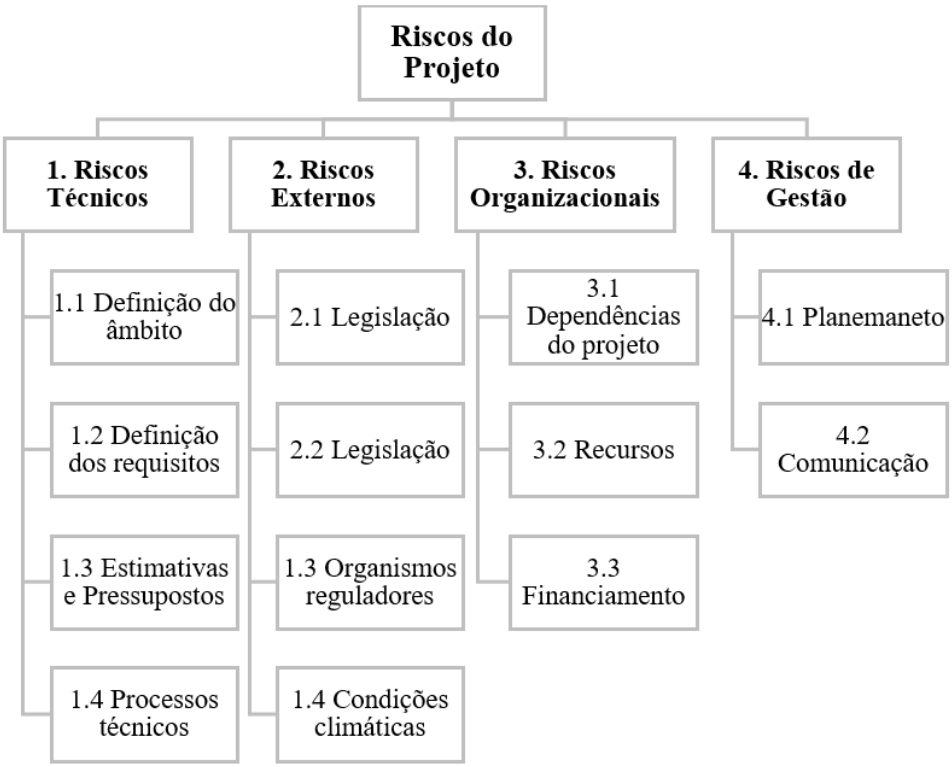


Figura 18 – Exemplo de um *Risk Breakdown Structure* (RBS),
Fonte: Adaptado António Miguel (2019); PMI, (2013a)

2.4.1.3 Análise qualitativa dos riscos

A Análise Qualitativa dos Riscos consiste num processo de priorização dos riscos individuais do projeto para analise ou ação posterior, através da avaliação da sua probabilidade e impacto de ocorrência. Essas avaliações são subjetivas, uma vez que se baseiam na perceção do risco. O processo estabelece as prioridades relativas dos riscos individuais do projeto para o processo de Planeamento das Respostas aos Riscos, identificando um responsável que assuma a responsabilidade por planear uma resposta adequada ao risco e garantir que esta seja implementada. O presente processo, também, estabelece as bases necessárias para a realização do processo Análise Quantitativa dos Riscos, e é realizado regularmente durante todo o ciclo de vida do projeto (PMI, 2009, 2017a, 2019).

Segundo Peixoto et al. (2014), os riscos podem ser priorizados para o planeamento das respostas aos riscos ou talvez uma análise posterior. As classificações dos riscos são designadas com base na avaliação da sua probabilidade e impacto.

A escala de probabilidade de ocorrência de riscos (Tabela 2) apresentado pelo PMI (2013a) permite uma avaliação utilizando uma escala ordinal que correspondem respetivamente a uma variação de ocorrência.

Ocorrência	**Muito baixo**	**Baixo**	**Moderado**	**Alto**	**Muito alto**
Probabilidade	0.1	0.3	0.5	0.7	0.9

Tabela 2 - Escala de probabilidade,
Fonte: Adaptado de PMI (2013a)

No que diz respeito à escala de avaliação do impacto do risco, o mesmo pode ser realizado relativamente aos quatro parâmetros de um projeto (custo, cronograma, âmbito e qualidade), e a cada grau de impacto é associada uma consequência e um valor relativo de impacto (Keshk et al., 2018). A organização lógica entre parâmetros, consequências e valores relativos de impacto são apresentados na Tabela 3.

	Muito baixo 0.05	**Baixo 0.1**	**Moderado 0.2**	**Alto 0.4**	**Muito alto 0.8**
Custo	Aumento insignificante do custo	<5% de aumento de custo	5-10% de aumento de custo	10-20% de aumento de custo	>20% de aumento de custo
Cronograma	Desvio insignificante do cronograma	Desvio total do cronograma <5%	Desvio total do cronograma 5-10%	Desvio total do cronograma 10-20%	Desvio total do cronograma >20%
Âmbito	Diminuição quase impercetível do âmbito	São afetadas áreas de pouca importância do âmbito	São afetadas Áreas importantes do âmbito	Redução do âmbito inaceitável para o cliente	Produto final do projeto inadequado
Qualidade	Degradação quase impercetível da qualidade	São afetadas apenas as aplicações mais exigentes	Redução da qualidade requer a aprovação do cliente	Redução da qualidade inaceitável para o cliente	Projeto e produto final do projeto inutilizável

Tabela 3 - Escala de avaliação do impacto dos riscos,
Fonte: Adaptado de Keshk et al. (2018)

De acordo com a literatura existente, a determinação do nível de risco deve ser calculada da seguinte forma(Keshk et al., 2018):

$$Nível\ do\ Risco = Probabilidade\ x\ Impacto$$

A avaliação da importância de cada risco e a prioridade de atenção é normalmente conduzida usando uma matriz de probabilidade e impacto (Tabela 4), que especifica as diferentes as combinações de probabilidade e impacto que resultam numa classificação dos riscos como de prioridade baixa, moderada ou alta. O nível de risco pode ser definido com um código de cores: verde para riscos baixos, amarelo para moderados e vermelho para riscos de alto impacto.

	Impacto				
Probabilidade	0.05	0.1	0.2	0.4	0.8
0.9	0.05	0.09	0.18	0.36	0.72
0.7	0.04	0.07	0.14	0.28	0.56
0.5	0.03	0.05	0.10	0.20	0.40
0.3	0.02	0.03	0.06	0.12	0.24
0.1	0.01	0.01	0.02	0.04	0.08

Legenda:

	Baixo		Moderado		Alto

Tabela 4 -Matriz de Probabilidade e Impacto,
Fonte: Adaptado de Peixoto et al. (2014)

2.4.1.4 Análise quantitativa dos riscos

A análise quantitativa dos riscos consiste num processo de análise numérica do efeito dos riscos identificados nos objetivos globais do projeto. O principal benefício deste processo foca-se na produção de informações quantitativas dos riscos para apoiar a tomada de decisões, a fim de reduzir o grau de incerteza dos projetos(PMI, 2009).

O presente processo tem como objetivo a realização de uma avaliação aos impactos dos riscos considerados mais significativos, atribuindo-lhes valores numéricos de forma a quantificá-los no que diz respeito à exposição do projeto ao risco, bem como permitir uma abordagem quantitativa à tomada de decisão em condições de incerteza (António Miguel, 2019; Chapman & Ward, 2003).

De acordo com o António Miguel (2019) e PMI (2019) existem algumas técnicas de análise de dados que podem auxiliar o processo. Entre as quais destacam-se:

Análise de Sensibilidade

A análise de sensibilidade verifica o impacto potencial de riscos no projeto, mediante a compreensão das variações dos objetivos do projeto, correlacionadas com as variações em diferentes graus de incerteza. De modo oposto, examina até que ponto a incerteza de cada elemento

do projeto afeta o objetivo examinado quando todos os outros elementos incertos são mantidos em valores estáveis (PMI, 2009).

Earned Value Management (EVM)

O EVM é amplamente empregado na área de gestão de projeto para medir o desempenho de projetos, uma vez que combina medidas do Triângulo de Ferro do PM (Muriana & Vizzini, 2017). Segundo Chen et al.(2016), "O EVM produz índices de variação e desempenho para os custos e cronogramas do projeto e, portanto, prevê os custos e cronogramas do projeto na conclusão, fornecendo indicações antecipadas dos resultados esperados do desempenho do projeto."

Na análise de risco, o EVM das oportunidades é representado por um valor positivo, ao contrário das ameaças que é representado por valor negativo. O seu objetivo é estimar qual o valor monetário a esperar como gasto da ocorrência das várias situações resultantes do risco, incluindo situações de incerteza (António Miguel, 2019; PMI, 2009).

Árvores de Decisão

Árvores de decisão são utilizadas para apoiar a seleção do melhor entre vários caminhos de ação alternativos. Os caminhos alternativos pelo projeto aparecem na árvore de decisão através de ramos representando os vários eventos ou decisões, e cada qual pode ter custos associados e riscos individuais de projeto relativos (incluindo ameaças ou oportunidades). Os pontos finais dos ramos da árvore de decisão representam o resultado a adotar nesse determinado caminho, que pode ser negativo ou positivo (PMI, 2017a). Na Figura 19 é ilustrado um exemplo de uma árvore de decisão.

A análise da árvore de decisão é realizada geralmente utilizando um *software* especifico, permitindo ao utilizador especificar a estrutura da decisão com nós de decisão, nós de chance, custo, benefícios e probabilidades, A árvore permite também avaliar as diferentes decisões através de funções de utilidade lineares baseadas em EVM ou funções de utilidade não lineares de várias formas (PMI, 2019).

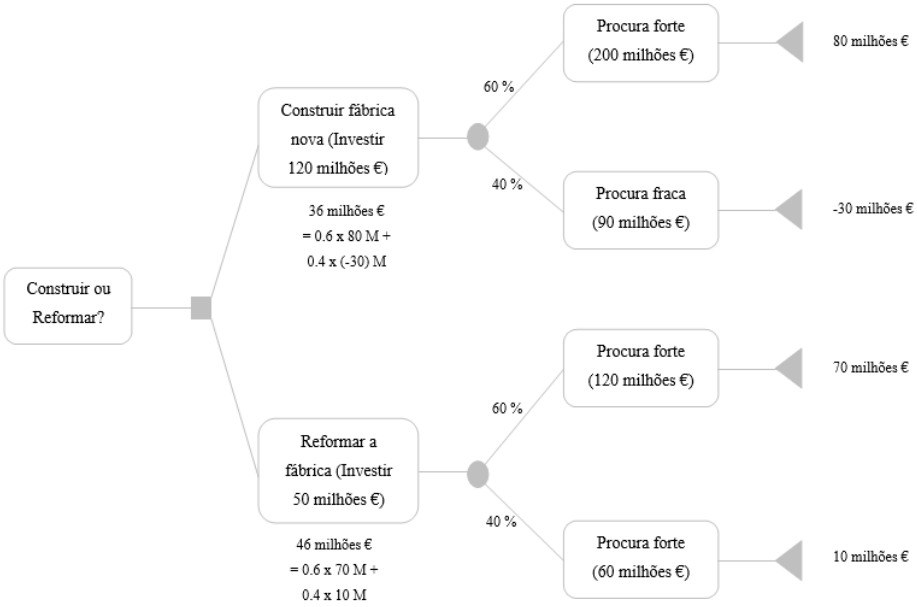


Figura 19 - Exemplo de Árvore de Decisão,
Fonte: Adaptado de PMI (2017a)

Simulação de Monte Carlo

A análise quantitativa dos riscos usa um modelo que simula os efeitos combinados dos riscos individuais a fim de avaliar o seu impacto nos objetivos do Projeto (PMI, 2017a). A simulação de Monte Carlo é reconhecida pela precisão dos seus resultados, fazendo parte dos métodos probabilísticos utilizados na simulação de riscos. O método de Monte Carlo primeiro gera valores de variáveis artificiais, utilizando um gerador de números aleatórios uniformemente distribuído no intervalo [0, 1] e a função de distribuição cumulativa associada. Em seguida, o método utiliza os resultados obtidos para extrair valores da distribuição de probabilidade que descreve o comportamento da variável estocástica (Purnus & Bodea, 2013).

Os resultados típicos da análise de Monte Carlo incluem geralmente um histograma que apresenta o número de iterações dos resultados do Projeto (cronograma e/ou custo) ou uma distribuição de probabilidade cumulativa (curva S), representando a probabilidade de alcançar qualquer resultado (PMI, 2017a)

2.4.1.5 Planeamento das respostas aos riscos

De acordo com (Tworek, 2012) não é possível gerir riscos em projetos de investimento de forma eficaz sem conhecer as formas e métodos de responder a esses riscos. Procurar uma resposta

adequada aos riscos é um processo complexo que requer uma abordagem multifacetada, tendo em conta as possíveis consequências que podem ser causadas por soluções específicas. Os métodos de resposta ao risco são agora bastante variados; incluem diferentes padrões de comportamento, resultantes de anos de experiência nesta área, mas apresentados de forma contemporânea.

O Planeamento das Respostas aos Riscos é um processo de desenvolvimento de alternativas, que permite selecionar estratégias e determinar ações para lidar com a exposição geral aos riscos, e também tratar os riscos individuais do projeto. O principal benefício deste processo é a identificação de formas apropriadas de abordagem ao risco geral e os riscos individuais do projeto. (PMI, 2017a).

Desse modo, o processo determina as ações de resposta efetivas mais apropriadas para a prioridade dos riscos individuais e para o risco geral. Este processo tem em consideração as atitudes de risco das partes interessadas, além de quaisquer restrições e premissas que foram determinadas aquando da identificação e análise dos riscos. Uma vez priorizados os riscos individuais, são desenvolvidas as respostas de risco adequadas às ameaças e oportunidades. Este processo continua até que um conjunto ótimo de respostas seja desenvolvido (PMI, 2009).

Para o PMI (2019), existe quatro tipos de estratégias possíveis para o tratamento de ameaças na gestão de risco do projeto:

- **Evitar:** envolve uma alteração no plano de gestão do projeto com o objetivo de eliminar a ameaça de um risco, assegurando que a ameaça não ocorrerá;
- **Transferir:** envolve a transferência do risco para terceiros para gerir o risco e suportar o impacto, caso a ameaça ocorra;
- **Mitigar:** ação é realizada para reduzir a probabilidade de ocorrência e/ou o impacto de uma ameaça. Antecipada a ação é quase sempre mais efetiva do que tentar reparar o dano depois que a ameaça ocorreu;
- **Aceitar:** reconhece a existência de uma ameaça, mas nenhuma ação proativa é tomada. Essa estratégia pode ser correta para ameaças de baixa prioridade e também pode ser adotada quando não é possível, nem económico, resolver a ameaça de qualquer outra forma;

De acordo com a mesma literatura, as quatro estratégias de tratamento das oportunidades na gestão de projetos são:

- **Explorar:** visa eliminar a incerteza associada a uma oportunidade, aumentado a probabilidade de ocorrência para 100%;

- **Partilhar:** envolve transferir a responsabilidade por uma oportunidade a terceiro para que este compartilhe alguns dos benefícios, caso a oportunidade ocorra;
- **Melhorar:** usada para aumentar a probabilidade e/ou o impacto de uma oportunidade**;**
- **Aceitar:** aceitação de uma oportunidade reconhece a sua existência, mas nenhuma ação proativa é tomada. Essa estratégia pode ser apropriada para oportunidades de baixa prioridade e também pode ser adotada quando não é possível, nem econômico, resolver uma oportunidade de qualquer outra forma.

As respostas são planeadas a um nível estratégico, e a estratégia é validada e acordada antes do seu desenvolvimento. Feito isso, as respostas aos riscos são expandidas e integradas aos planos de gestão relevantes. Esta atividade pode gerar riscos secundários adicionais, que precisam ser abordados (PMI, 2017a).

Além das respostas aos riscos individuais, outras ações podem ser tomadas para responder ao risco geral do projeto. Todas as estratégias e ações de resposta devem ser documentadas e comunicadas às partes interessadas e incorporadas aos planos relevantes (PMI, 2019).

2.4.1.6 Implementação das respostas aos riscos

Uma vez terminado o processo de planeamento das respostas aos riscos, todas as ações de resposta aprovadas são incluídas e definidas nos planos de gestão relevantes. O dono do risco monitoriza as ações de modo a determinar a sua efetividade, e identificar outros riscos secundários que possam surgir devido à implementação das respostas aos riscos. O dono do risco e o dono das ações do risco são informados sobre as alterações que possam afetar as suas responsabilidades (PMI, 2019). Apenas e só, se os responsáveis pelo risco aplicarem o nível de esforço exigido para implementar as respostas acordadas, a exposição geral ao risco do projeto, às ameaças e às oportunidades individuais serão geridas de modo proativo.(PMI, 2017a)

O principal benefício deste processo é a garantia de que as respostas acordadas aos riscos são executadas conforme o planeado a fim de abordar a exposição ao risco geral do projeto, minimizar ameaças e maximizar as oportunidades individuais do projeto (PMI, 2017a).

2.4.1.7 Monitorização dos riscos

A monitorização dos riscos é um processo de monitorização da implementação dos planos definidos no processo de resposta aos riscos, de acompanhamento dos riscos identificados, identificação e análise dos novos riscos, e avaliação da eficácia do processo de riscos realizados ao longo do

projeto. O principal benefício deste processo é a habilitação de decisões do projeto com base em informações atuais sobre a exposição geral do risco e riscos individuais do projeto. Este processo é realizado ao longo de todo o projeto (PMI, 2017a).

De forma a garantir que a equipa do projeto e as partes interessadas estão cientes do nível atual de exposição ao risco, o trabalho deve ser constantemente monitorizado relativamente aos riscos individuais novos, alterados, defasados e para as mudanças no nível do risco geral do projeto (PMI, 2009).

2.4.2 Metodologia de Gestão de Risco de Segurança da Informação

Para a Segurança da Informação, o risco é frequentemente caracterizado por referência a potenciais "eventos" e "consequências", ou uma combinação destes. O risco é expresso em termos de uma combinação das consequências de um evento (incluindo mudanças nas circunstâncias) e a "probabilidade" associada de ocorrência (ISO Guide 73, 2009). Uma característica intrínseca do risco é o facto de este não poder ser totalmente eliminado, tornando-se fundamental a concretização de uma estratégia global da organização (controlos) para garantir a implementação de um processo eficaz de gestão do risco (CNCS, 2019).

A gestão do risco de uma organização é um exercício sistematizado, no âmbito do qual a organização identifica possíveis ameaças sobre os seus ativos, bem como os níveis do risco associado, avaliando-se a probabilidade de ocorrência e o impacto (CNCS, 2019; ISO/IEC 27005, 2018).

No que diz respeito à Segurança de Informação, a gestão de risco aplicado ao projeto avançado em questão irá basear-se unicamente ma ISO/IEC 27005 – Tecnologia de Informação – Técnicas de Segurança – Gestão de Risco de Segurança da Informação(ISO/IEC 27005, 2018).

É importante realçar que a segurança de informação tem como principal objetivo a proteção dos ativos, onde as ameaças se classificam como um potencial risco. Todas as categorias de ameaças devem ser consideradas, tendo em conta que estas possam estar relacionadas com atividades maliciosas, dando-se dessa forma mais atenção às ameaças (Webb et al., 2014). Através da Figura 20 é o possível verificar as relações existentes entre risco, ameaça e vulnerabilidades, considerando que:

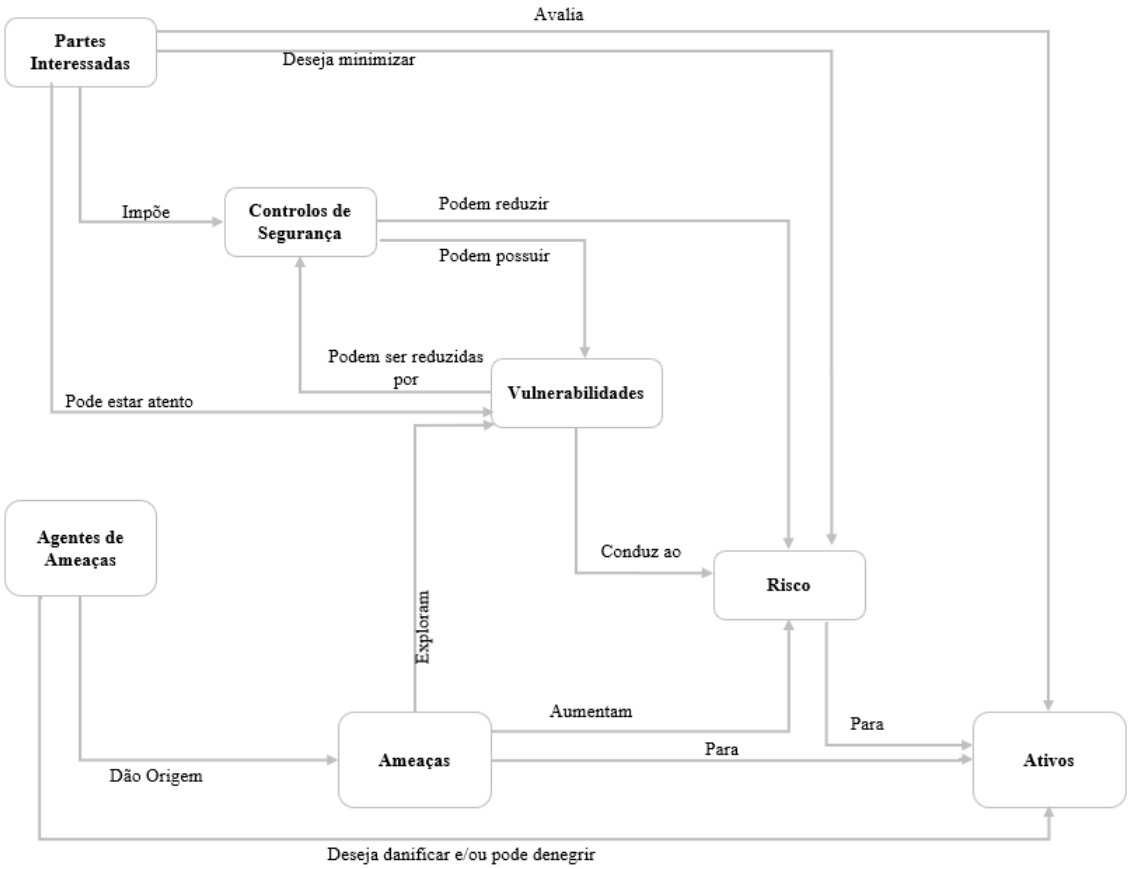


Figura 20 - Conceitos básicos e relações de alto nível,
Fonte: Adaptado de ISO/IEC 27032 (2012)

- **Risco:** uma circunstância ou um evento razoavelmente identificável, com um efeito potencial adverso na segurança das redes e dos sistemas de informação (Assembleia da República, 2018);
- **Ameaça:** potencial causa de um incidente indesejado, que pode provocar danos a um sistema, individuo ou organização (ISO/IEC 27032, 2012);
- **Vulnerabilidades:** fraqueza de um ativo ou de um controlo que pode ser explorada por uma ameaça (ISO/IEC 27032, 2012).

A abordagem da metodologia da gestão de risco apresentada consiste em estabelecer o contexto, levantamento do risco (que inclui a identificação, análise e avaliação do risco), Tratamento do risco, a fase de Aceitação do Risco, dando-se depois sequência às fases de Comunicação e Consulta e de Monitorização e Revisão do Risco (ISO/IEC 27005, 2018).

As principais fases do processo de gestão de riscos são apresentadas de forma esquematizada na Figura 21.

Figura 21 - Fases da Gestão de Risco,
Fonte: Adaptado da ISO/IEC 27005 (2018)

Em sumário, o processo de gestão de riscos é sistemático, estruturado e oportuno, procurando sempre a implementação de uma melhoria contínua do processo.

2.4.2.1 Estabelecer Contexto

A fase de estabelecer o contexto envolve um conjunto de critérios base necessários à gestão do risco, incluindo a definição do âmbito de aplicabilidade do processo de gestão de risco e os critérios e avaliação do risco.

Organização na gestão do risco

A organização deve identificar os recursos humanos e materiais necessários a envolver no processo de modo a garantir uma correta execução. Dessa forma e juntamente com a aprovação da gestão de topo, deve-se definir (CNCS, 2019; ISO/IEC 27005, 2018):

- Metodologia de governo a aplicar no processo de gestão de risco;
- As partes interessadas internas e externas e as respetivas responsabilidades na gestão de risco;

- As ferramentas, documentos e registos que suporte o processo.

Abordagem à gestão do risco

A organização, juntamento com a aprovação da gestão de topo, deverá definir e desenhar as políticas[1], processos[2] e procedimentos[3], necessários, no âmbito de todo o processo de gestão e tratamento do risco (CNCS, 2019).

Critérios de avaliação do risco

A organização deverá identificar os critérios utilizados para a avaliação do risco, de forma a avaliar a relevância do risco. Considerando-se o valor estratégico, a criticidade dos ativos e a importância operacional e comercial em termos de confidencialidade[4], integridade[5] e disponibilidade[6] da informação (CNCS, 2019).

Critérios de impacto

A organização deverá determinar em termos de grau de danos e/ou custos que um evento de segurança da informação tem para a entidade. Na determinação dos níveis de impacto definidos, a organização deverá de ter em consideração a classificação dos ativos de informação, as falhas na segurança de informação no que diz respeito à confidencialidade, integridade e disponibilidade da informação, à disrupção dos custos e prazos e aos danos causados à organização (CNCS, 2019).

Critérios de aceitação do risco

A organização deverá identificar a partir de que nível do risco terá de ser necessária a aprovação da gestão de topo para que o mesmo possa ser aceite. Deverão ser definidas as escalas de níveis de aceitação dos riscos. Na definição dos critérios de aceitação do risco podem incluir diversos limites e requisitos tratamento futuro (CNCS, 2019).

Definição de âmbito e fronteiras

A definição do âmbito e fronteiras do sistema de gestão do risco de segurança da informação. Torna-se relevante, dada a necessidade de garantir que todos os ativos relevantes para a entidade estarão incluídos na fase de levantamento. Ao realizar essa definição a organização deve ter em conta os

[1] Intenções e orientação de uma organização, conforme formalmente expressas pela gestão de topo (ISO/IEC 27000, 2018; ISO 22301, 2019).
[2] Conjunto de atividades interrelacionadas ou interatuantes que transformam entradas em saídas (ISO/IEC 27000, 2018; ISO 22301, 2019).
[3] Modo especificado de realizar uma atividade ou um processo (ISO/IEC 27000, 2018; ISO 22301, 2019).
[4] Propriedade de a informação não ser divulgada a pessoas ou entidades não autorizadas ou segundo processos não autorizados (ISO/IEC 27000, 2018).
[5] Propriedade de salvaguardar o caráter exato e completo da informação e dos ativos (ISO/IEC 27000, 2018).
[6] Propriedade de estar acessível e de poder ser utilizada a pedido de uma entidade autorizada (ISO/IEC 27000, 2018).

objetivos estratégicos, os processos relativos à atividade exercida, às funções e estrutura interna e externa da entidade e expetativas das partes interessadas identificadas acima, aos ativos de informação e finalmente à sua política de segurança da informação.

2.4.2.2 Levantamento do Risco

O processo de levantamento de riscos consiste nas seguintes atividades:

i. identificação de riscos;
ii. análise de riscos;
iii. avaliação de riscos.

i. Identificação do Risco

O propósito da identificação de riscos consiste na determinação do que possa causar uma perda potencial e deixar claro como, onde e porque essa perda pode acontecer. É de esperar que a identificação de riscos inclua os riscos cujas fontes estejam ou não sob controlo da organização, mesmo que a fonte ou a causa dos riscos não seja evidente (ISO/IEC 27005, 2018).

Identificação dos ativos

Para a identificação dos ativos, deve-se ter em conta que um sistema de informação compreende mais do que hardware e software, abarcando também dados, informações e até mesmo pessoas. De acordo com ISO/IEC 27005 (2018) os ativos subdividem-se em:

1.1 **ativos primários:** são os riscos relacionados à exposição indevida (confidencialidade), alterações impróprias (integridade) e impedimento de acesso (disponibilidade) das informações relevantes para as atividades principais da organização.
2.1 **ativos secundários:** são aqueles utilizados para manter os ativos primários.

De acordo com o CNCS (2019) ativos são tudo o que tem valor e que requer proteção para a organização, podendo ser ativos:

- Tecnológicos (hardware, software);
- Dispositivos de rede;
- Pessoas;
- Localizações;
- Etc.

Identificação das ameaças

Uma ameaça tem o potencial de poder criar impactos e consequências negativas nos ativos da entidade, podendo, esta ser de origem natural ou humana e ser acidental ou intencional. É

conveniente que tanto as fontes das ameaças acidentais, quanto as intencionais, sejam identificadas, visto que uma ameaça pode surgir de dentro ou de fora da organização. Recomenda-se, ainda, que as ameaças sejam identificadas genericamente e por classe e, quando apropriado, as ameaças específicas identificadas dentro das classes genéricas. Isto significa que, nenhuma ameaça é ignorada, incluindo as não previstas. Algumas ameaças podem afetar mais do que um ativo e nesses casos, podem provocar impactos diferentes, dependendo dos ativos afetados (ISO/IEC 27005, 2018).

Identificação dos controlos

A identificação dos controlos existentes deve ser realizada com o propósito de evitar trabalho ou custo desnecessários para a organização, além disso, ao identificar os controlos existentes, deve ser feita uma verificação de modo a garantir que os controlos estão implementados corretamente. É de notar que o fato de um controlo não funcionar corretamente pode levar à existência de vulnerabilidades (ISO/IEC 27005, 2018).

Para a identificação dos controlos existentes ou planeados, de acordo com o CNCS (2019) as atividades que se seguem podem ser úteis:

- rever os documentos que contêm informações sobre os controlos (por exemplo, planos de implementação de tratamento de riscos) se os processos de gestão de segurança da informação estiverem bem documentados, todos os controlos existentes ou planeados e o estado de sua implementação devem estar disponíveis;
- verificar com os responsáveis pela segurança da informação e os utilizadores sobre a os controlos que realmente estão implementados;
- realizar uma revisão presencial aos controlos físicos de modo a perceber o nível de implementação.

Identificação das vulnerabilidades

Tendo em conta as ameaças, os ativos e os controlos identificados, as vulnerabilidades devem ser consideradas para uma identificação de riscos mais ampla e precisa. O ambiente da organização pode estar sujeito a uma grande variedade de vulnerabilidades tecnológicas (CNCS, 2019).

Segundo o Anexo D da (ISO/IEC 27005, 2018) as vulnerabilidades podem ser identificadas nas seguintes áreas:

- organização;
- processos e procedimentos;
- rotinas de gestão;
- recursos humanos;

- ambiente físico;
- configuração do sistema de informação;
- hardware, software ou equipamentos de comunicação;
- dependência de entidades externas.

Identificação das consequências

As consequências dos riscos devem ser identificadas de modo aferir qual o impacto que uma possível vulnerabilidade poderá ter em termos de confidencialidade, integridade e/ou disponibilidade dos ativos identificados (CNCS, 2019; ISO/IEC 27005, 2018).

ii. Análise de Risco

Na análise de riscos, verifica-se quais as prováveis origens dos riscos identificados, as consequências e qual a probabilidade de que elas ocorram, bem como quais objetivos podem ser atingidos(ISO/IEC 27005, 2018).

Nos critérios de aferição do impacto do risco recomendam-se ser igualmente observadas as seguintes dimensões (CNCS, 2019):

- **Reputação:** área focada no impacto trazido pela materialização do risco para a imagem e reputação que a Organização possuí externamente;
- **Legal ou Regulatório:** onde se expressa qualquer consequência que a Organização poderá sofrer a nível judicial e regulamentar a nível nacional e internacional;
- **Serviço a clientes:** área que pondera o impacto causado ao nível interno na prestação do serviço ou do sistema que force os colaboradores a não cumprir com as suas funções e responsabilidades;
- **Financeiro:** área que pesa a perda de capacidades de garantir a operacionalidade dos serviços prestados, nomeadamente dos serviços de TI e do SGI, e a perda financeira inevitável por forma a recuperar a capacidade anterior à materialização do risco.

Metodologia de análise de Risco

A análise de risco pode ser realizada em vários graus de detalhe, dependendo da criticidade dos ativos, extensão das vulnerabilidades conhecidas e incidentes anteriores envolvendo a organização. Assim sendo, uma metodologia de análise de risco pode ser qualitativa ou quantitativa, ou uma combinação destas, dependendo das circunstâncias (CNCS, 2019; ISO/IEC 27005, 2018).

- **Análise qualitativa:** utiliza uma escala de atributos de qualificação para identificar a severidade dos potenciais impactos (por exemplo: Baixo, Médio e Alto) e a probabilidade de tais ocorrências;

- **Análise quantitativa:** utiliza uma escala de valores numéricos (em oposição às escalas descritivas usadas na análise do risco qualitativa) para aferição dos impactos e probabilidades, sendo suportada em diversas fontes.

Levantamento dos impactos

O conceito de impacto é utilizado para a medição das consequências, o seu valor pode ser expresso de forma qualitativa e/ou quantitativa. Qualquer método de atribuição de valor monetário tende a fornecer mais informações para a tomada de decisão e, portanto, tornar o processo de tomada de decisão mais eficiente (ISO/IEC 27005, 2018).

De acordo com a ISO/IEC 27005 (2018) e CNCS (2019) os ativos identificados devem ser classificados por níveis de criticidade, em termos da sua importância para o cumprimento dos objetivos da organização. Essa avaliação é realizada através da utilização das seguintes medidas:

- o valor de reposição do ativo: o custo da limpeza de recuperação e substituição da informação;
- as consequências comerciais da perda ou comprometimento do ativo, como as potenciais consequências comerciais adversas e/ou legais ou regulatórias da divulgação, modificação, indisponibilidade e/ou destruição de informações e outros ativos de informações.

A avaliação de ativos é um fator chave na avaliação de impacto de um cenário de incidente, porque o incidente pode afetar mais de um ativo, ou apenas uma parte de um ativo. Diferentes ameaças e vulnerabilidades podem ter diferentes impactos nos ativos, como perda de confidencialidade, integridade ou disponibilidade (ISO/IEC 27005, 2018). A Tabela 5 exemplifica a definição de um grau de impacto para todas as áreas de consequências associadas.

Níveis de impacto	**Legal ou Regulatório**	**Financeiro**	**Serviço a clientes**	**Reputacional**
Muito alto (5)	Impacto legal/regulatório muito alto, com altas coimas associadas, podendo interromper a	Quebra operacional significativa, podendo ser total e/ou definitiva.	Impacto interno e externo comprometendo a prestação do serviço ou sistema forçando os colaboradores a não cumprir com as	O evento foi publicado por fontes de comunicação social

	prestação do serviço.		suas funções e responsabilidades	
Alto (4)	Impacto legal/regulatório de alto impacto com coimas associadas.	Quebra operacional parcial com impacto elevado nas operações.	Impacto externo comprometendo a prestação do serviço ou sistema forçando os colaboradores a não cumprir com as suas funções e responsabilidades	O evento foi publicado por pessoas individuais.
Médio (3)	Impacto legal/regulatório de médio impacto.	Quebra operacional parcial com impacto residual nas operações.	Impacto interno comprometendo a prestação do serviço ou sistema forçando os colaboradores a não cumprir parcialmente com as suas funções e responsabilidades	O evento ficou circunscrito internamente na organização.
Baixo (2)	Impacto legal/regulatório de baixo impacto.	Quebra operacional parcial com baixo impacto nas operações.	Impacto interno comprometendo a prestação do serviço ou sistema, porém não interrompendo os colaboradores a cumprir com suas funções e responsabilidades	Evento ficou circunscrito internamente no departamento.
Muito baixo (1)	Inspeção com ausência de recomendações do regulador.	Sem impacto operacional/financeiro para a organização.	Impacto interno não comprometendo a prestação do serviço ou sistema, e não interrompendo os colaboradores a cumprir com suas funções e responsabilidades	Evento ficou circunscrito internamente na área afetada.

Tabela 5 - Exemplo de uma definição para cada nível de impacto para todas as áreas de consequências

Fonte: Elaboração própria

A tabela seguinte dá um exemplo de uma definição para cada nível de impacto.

Risco	Impacto
Muito alto (5)	Perigo de continuidade da empresa com elevadas perdas financeiras, danos para a imagem e reputação ou perdas humanas. Evento que gera impacto em toda a organização ou representa perda de confidencialidade, integridade e disponibilidade, causando prejuízos de forma generalizada, inviabilizando ou proporcionando perceção negativa.
Alto (4)	Fortes consequências para a empresa, com perdas financeiras de imagem e reputação, ou possibilidade de perdas humanas. Evento que gera impacto sobre vários grupos ou representa perda de confidencialidade, integridade e disponibilidade, prejudicando as funções primárias de trabalho de múltiplas áreas da organização
Médio (3)	Consequências moderadas para a empresa com perdas financeiras ou de imagem e reputação associadas. Evento que gera impacto sobre um grupo relevante ou representa perda de confidencialidade, integridade e disponibilidade, prejudicando as funções primárias de trabalho.
Baixo (2)	Consequências a nível departamental com possíveis perdas financeiras para a empresa. Evento que gera impacto sobre um pequeno grupo ou representa perda de confidencialidade, integridade e disponibilidade, prejudicando as funções secundárias de trabalho, não sendo o bastante para intervir nas funções principais.
Muito baixo (1)	Consequências a nível departamental sem perdas financeiras para a empresa. Evento que gera impacto sobre uma pessoa ou representa perda de confidencialidade, integridade e disponibilidade que não necessita de intervenção ou paralisação imediata.

Tabela 6 - Exemplo de uma definição para cada nível de impacto
Fonte: Elaboração própria

Realizada o levantamento do risco, existe a necessidade de analisar a probabilidade do risco identificado.

Análise da probabilidade

Após a identificação das ameaças, vulnerabilidades e lista dos incidentes ocorridos, existe a necessidade de realizar uma avaliação à probabilidade de ocorrência de cada um dos cenários e respetivo impacto (CNCS, 2019). Isso deve levar em conta a frequência com que as ameaças

ocorrem e a facilidade com que as vulnerabilidades podem ser exploradas, considerando (ISO/IEC 27005, 2018). Entre os fatores a considerar para a análise temos:

- experiência e estatísticas aplicáveis;
- motivação e as capacidades, que mudam ao longo do tempo, e os recursos disponíveis para possíveis invasores, bem como a perceção de atratividade e vulnerabilidade dos ativos para um possível invasor;
- fatores geográficos;
- vulnerabilidades.

Na Tabela que se segue é apresentado um exemplo da definição probabilidade de ocorrência por nível de risco.

Risco	**Probabilidade**
Muito alto (5)	Ocorrerá a muito curto Prazo (até 6 meses)
Alto (4)	Ocorrerá a curto prazo (até 12 meses)
Médio (3)	Ocorrerá a médio prazo (até 18 meses)
Baixo (2)	Provavelmente ocorrerá (até 24 meses)
Muito baixo (1)	Improvável que Ocorra (mais de 24 meses)

Tabela 7 - Exemplo de uma definição para cada nível de probabilidade
Fonte: Elaboração própria

Terminada a análise à probabilidade da ocorrência dos riscos identificados, a próxima atividade, foca-se na determinação do nível de risco, como explicado a seguir.

Determinação do nível de risco

O objetivo da realização do processo de análise de riscos é a designação de valores para a probabilidade e para as consequências de um risco, valores esses que, como apresentado anteriormente, podem ser de natureza quantitativa ou qualitativa (ISO/IEC 27005, 2018).

A análise de riscos é baseada nas consequências (impacto) e na probabilidade avaliadas, dessa forma e de acordo com a literatura analisada. O risco estimado é uma combinação da probabilidade de um cenário de incidente e suas consequências. Este risco pode ser traduzido pela seguinte equação:

$$Risco = Probabilidade\ x\ Impacto$$

Assim sendo, é possível desenhar a matriz de risco tal como esquematizado na Tabela 8.

	Impacto				
Probabilidade	Muito baixo (1)	Baixo (2)	Médio (3)	Alto (4)	Muito alto (5)

Muito alto (5)	Médio (5)	Médio (10)	Alto (15)	Muito alto (20)	Muito alto (25)
Alto (4)	Baixo (4)	Médio (8)	Alto (12)	Alto (16)	Muito alto (20)
Médio (3)	Baixo (3)	Médio (6)	Médio (9)	Alto (12)	Alto (15)
Baixo (2)	Baixo (2)	Baixo (4)	Médio (6)	Médio (8)	Médio (10)
Muito baixo (1)	Muito baixo (1)	Baixo (2)	Baixo (3)	Baixo (4)	Médio (5)

Legenda:

	Muito baixo		Baixo		Médio		Alto		Muito alto

Tabela 8 - Exemplo de Matriz de Nível de Risco,
Fonte: Adaptado da ISO/IEC 27005, (2018)

A escala do nível de risco poderá ser definida da seguinte forma:

- 20 a 25 – muito alto;
- 12 a 19 – alto;
- 5 a 11 – médio;
- 2 a 4 – baixo;
- 1 – Muito baixo.

iii. Avaliação do Risco

Segundo a ISO/IEC 27001 (2013), a Avaliação do Risco tem como propósito a priorização dos riscos contra critérios de avaliação, definidos no estabelecer do contexto, e objetivos relevantes para a organização.

Os níveis de riscos são valorizados e comparados de acordo com os critérios de avaliação e de aceitação de riscos estabelecidos. Conforme a ISO/IEC 27005 (2018) devem ser considerados os seguintes aspetos:

- as decisões que serão apoiadas nos critérios estabelecidos durante a etapa de Estabelecer Contexto;
- as decisões e o contexto devem ser revistos com maior detalhe, visto que mais informações são conhecidas sobre os riscos;
- critérios de avaliação devem ser consistentes com os cenários de segurança da informação interno e externo;
- critérios de avaliação devem considerar os objetivos da organização e as perceções dos intervenientes;
- decisões são principalmente baseadas no nível de risco aceitável;
- deve-se observar atentamente a relevância dos critérios, pois alguns objetivos de segurança da informação podem ser irrelevantes para uma organização

No final da Avaliação, os riscos devem ser identificados, estimados e avaliados, e produzida uma lista de riscos priorizados conforme critérios previamente estabelecidos. Se a Apreciação do Risco não produzir resultados satisfatórios, deve-se retornar à fase de Estabelecer o Contexto, para repetir novamente todo o processo, caso contrário deve avançar-se para o Tratamento (ISO/IEC 27005, 2018).

2.4.2.3 Tratamento do Risco

Para a ISO/IEC 27001 (2013), a organização deverá definir e aplicar um processo de tratamento de risco da segurança da informação de modo a selecionar as ações necessárias de tratamento, considerando os resultados obtidos na realização da etapa anterior, deve ainda determinar todos os controlos necessários de forma a implementar as opções de tratamento selecionadas, e por fim, realizar uma comparação dos controlos existentes de forma a constatar se todos os controlos necessários estão identificados ou implementados.

De acordo com a ISO/IEC 27005, (2018) e com a Figura 22 - que traduz atividade de tratamento do risco dentro do processo de gestão de riscos - para a realização do tratamento do risco, as organizações possuem quatro opções disponíveis:

- **Evitar:** Eliminar a causa do risco, eliminando o processo que o gera. Visa a descontinuação das atividades de negócio ou ativos de informação ou de suporte que atuam como fonte do risco para a organização, eliminando de forma permanente o risco. Tipicamente esta opção é considerada quando o plano de tratamento apresenta custos demasiado elevados e que a atividade de negócio ou ativo visadas já não possuam uma importância tão visível para os objetivos de negócio da organização.
- **Aceitar:** Tomar conhecimento do risco sem adotar controlos. Somente riscos de nível baixo e muito baixo podem ser retidos; suportar a decisão de não aplicar qualquer tipo de ação corretiva ao risco e assumir as consequências que o mesmo pode trazer à organização em caso de materialização. Esta opção é utilizada em situações em que:
    - O risco se encontra dentro dos critérios de aceitação definidos pela organização;
    - Quando a implementação dos controlos para a redução do nível apresenta custos superiores àqueles que o risco provoca em caso de materialização.
- **Mitigar:** Diminuir a exposição dos riscos, elaborando planos de ação e aplicando controlos específicos, podendo haver lugar à implementação de controlos adicionais de forma a mitigar o risco ou reduzi-lo de modo a enquadrar-se nos critérios de aceitação de risco definidos pela organização.

- **Transferir:** No caso do seguro, por exemplo. Esse tipo de processamento é específico, pois tende a reduzir o impacto do risco e não a vulnerabilidade. O risco residual não pode ser calculado.

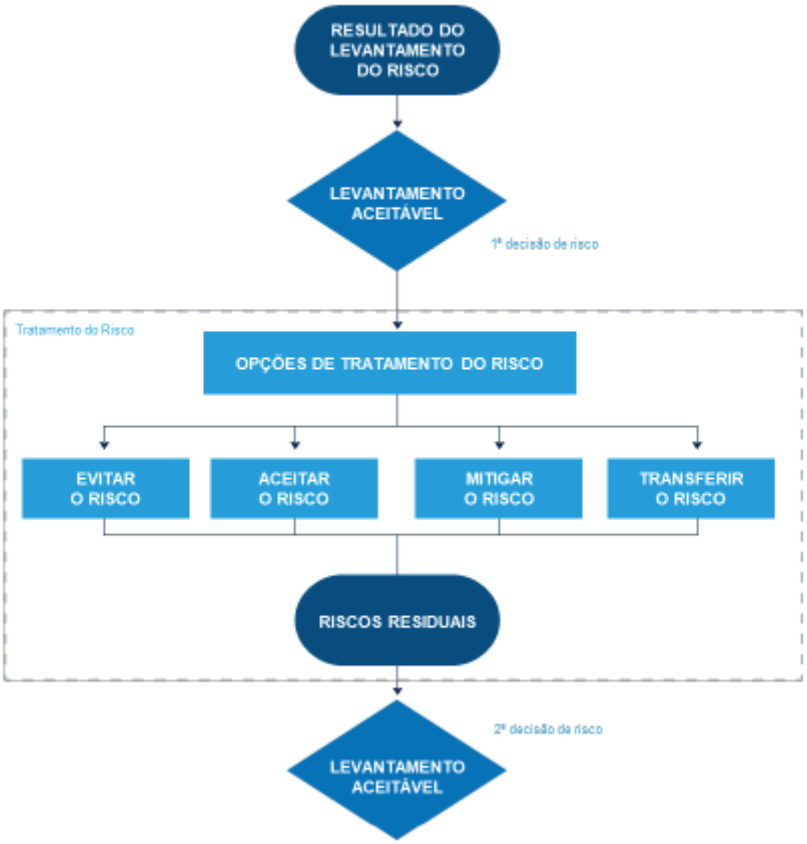


Figura 22 - Tratamento do Risco,
Fonte: Adaptado de ISO/IEC 27005 (2018)

Uma vez definido o plano de tratamento do risco, é necessário determinar os riscos residuais[7], o que envolve uma atualização ou uma repetição do processo de avaliação de riscos. Caso o risco residual ainda não satisfaça aos critérios para a aceitação do risco da organização, uma nova iteração do tratamento do risco pode ser necessária antes de se prosseguir à aceitação do risco.

2.4.2.4 Comunicação e Consulta do Risco

A comunicação do risco é uma atividade com o objetivo alcançar um consenso sobre a gestão dos riscos através da partilha de informação com as partes interessadas. A comunicação eficaz entre as partes interessadas é importante, uma vez que isso pode ter um impacto significativo sobre as decisões a ser tomadas, assegurando que os responsáveis pela implementação da gestão de riscos

[7] O risco residual é representado pela quantidade de risco que permanece ou que aparece após a inclusão dos controlos adicionais e/ou ajustes dos controlos já existentes(ISO/IEC 27000, 2018).

tenham o entendimento do porquê das decisões tomadas e dos motivos. É importante frisar que a comunicação é bidirecional (ISO/IEC 27001, 2013; ISO/IEC 27005, 2018).

De acordo com o CNCS (2019) a comunicação do risco deve ser realizada de modo a:

- fornecer garantia do resultado da gestão de riscos da organização;
- recolher as informações sobre os riscos;
- partilhar os resultados do processo de avaliação de riscos e apresentar o plano de tratamento do risco;
- evitar ou reduzir tanto a ocorrência quanto as consequências das violações da segurança da informação que aconteçam devido à falta de entendimento mútuo entre as partes interessadas;
- dar suporte ao processo;
- obter novo conhecimento sobre a segurança da informação;
- coordenar com outras partes e planear respostas para reduzir as consequências de um incidente;
- dar às partes interessadas determinadas responsabilidades sobre riscos;
- melhorar a consciencialização.

A organização deve, de acordo com a ISO/IEC 27001 (2013) e ISO/IEC 27005 (2018), desenvolver os planos de comunicação dos riscos, é importante ressalvar que a atividade de comunicação deve ser realizada continuamente.

2.4.2.5 Monitorização e Revisão do Risco

A última atividade do processo de gestão de risco implica que todos os riscos e os seus fatores (valores dos ativos, impactos, ameaças, vulnerabilidades, probabilidade de ocorrência) sejam monitorizados e analisados criticamente, com o propósito de identificar, o mais rapidamente possível, eventuais mudanças no contexto da organização e de manter uma visão geral dos riscos (ISO/IEC 27005, 2018).

Assim sendo, de acordo com CNCS (2019) e ISO/IEC 27005 (2018), as organizações devem monitorizar continuamente as seguintes atividades:

- novos ativos que devam ser incluídos;
- modificações necessárias na criticidade dos ativos;
- novas ameaças que podem estar ativas tanto fora quanto dentro da organização e que não tenham sido avaliadas;
- a possibilidade de que as vulnerabilidades novas ou ampliadas venham a permitir que alguma ameaça as explore;

- as vulnerabilidades já identificadas, para determinar aquelas que se estão a tornar expostas a ameaças novas;
- as consequências ou o impacto ampliado de ameaças, vulnerabilidades e riscos avaliados, resultando num nível inaceitável de risco;

A organização deve efetuar a revisão de forma regular ou sempre que ocorram alterações significativas.

2.5 A Segurança da Informação e Cibersegurança

Com a evolução da importância da informação para as organizações, os termos como "segurança da informação" e "cibersegurança" estão cada vez mais presentes no dia-a-dia das organizações.

De acordo com a ISO/IEC 27000 (2018), a segurança da informação é alcançada através da implementação de um conjunto aplicável de controlos, selecionados através do processo de gestão de riscos escolhidos e geridos por um Sistema de Gestão de Segurança de Informação (SGSI), incluindo políticas, processos, procedimentos, estruturas organizacionais, software e hardware para proteger os ativos de informação identificados.

Relativamente ao termo "cibersegurança", a ENISA (2017) refere que este cobre todos os aspetos de prevenção, previsão, tolerância, deteção, mitigação, remoção, análise e investigação de ciberincidentes. Em suma, cibersegurança é um termo amplamente utilizado para designar todas as medidas e garantias necessárias com o objetivo de proteger o conjunto de dispositivos, equipamentos, serviços e dados associados a esses sistemas (que vão desde aparelhos telefónicos de uso pessoal, até centrais de geração de energia elétrica, ou mesmo hospitais).

2.5.1 Fases das Abordagens e Perspetivas da União Europeia (UE) para a Cibersegurança

Devido à importância das tecnologias de informação e comunicação do mercado interno, as questões de cibersegurança tornaram-se cada vez mais importantes, o que permitiu à UE iniciar a legislação e se envolver proactivamente num processo de tomada de decisão, fortalecendo a natureza económica da política de cibersegurança. Este foco da cibersegurança deu início à proposta da Comissão para uma estratégia de segurança da informação e da rede em 2001, sendo este o primeiro documento que representa uma política de cibersegurança identificável na UE (Beláz, 2019).

Entre 2002 e 2006, começou a ser definido o papel da UE no ramo cibernético, sendo criado um departamento no âmbito da Europol (2002) especializado em criminalidade *"high-tech*" (HTCC -

High-Tech Crime Centre), sendo em 2004 criada a ENISA, que visa estabelecer um quadro harmonizado para a regulamentação dos serviços de TIC e segurança das redes e da informação para a UE (EUROPEIA, 2017; Morgan, 2011).

Beláz, (2019) classifica o período 2007 a meados de 2016 como o "o Despertar" da política de cibersegurança, onde este tema passou a ser uma prioridade da UE e, como consequência disso, o autor verificou que, entre 2007 e 2013, 73 dos 143 documentos legais aceites estão relacionados com a cibersegurança. A esta altura, os ataques também foram considerados uma ameaça à estabilidade do mercado interno o que impulsionou uma série de medidas para o fortalecimento da segurança digital.

Em 2009, o Tratado de Lisboa postula em seu artigo 83.º, que as questões relativas à cibercriminalidade situam-se no domínio da cooperação judiciária em matéria penal, o que levou à criação da Europol EC3 (antigo HTCC), que se tornou um centro de referência oficial para políticas e regulação de combate ao cibercrime, devido ao seu caráter transfronteiriço (União Europeia, 2016). Dessa forma foi possível uma abordagem mais holística da cibersegurança, o que culminou na Estratégia da EU para a cibersegurança de 2013: Um ciberespaço aberto, seguro e protegido (C. Europeia, 2013).

Segundo Beláz, (2019), a 6 de julho de 2016, o Parlamento adotou a primeira peça de legislação de cibersegurança para toda a EU, que foi apresentada a proposta de diretiva relativa à segurança das redes e dos sistemas de informação (Diretiva SRI). No entanto, foram necessários mais três anos para finalizar o documento e moldar ainda mais o papel da UE no ciberespaço. A Diretiva SRI criou um quadro jurídico e institucional para aumentar o nível geral de cibersegurança na UE, incluindo os seguintes critérios:

- Os Estados Membros são obrigados a nomear uma autoridade NIS nacional e um CERT (ou Computer Security Incident Response Team - CSIRT);
- Construir uma cultura de segurança em todos os setores que são vitais para a economia e a sociedade e, que além disso, dependem fortemente das TICs, como energia, transporte, água, bancos, infraestruturas do mercado financeiro, saúde e infraestrutura digital. As empresas destes setores que sejam identificadas pelos Estados-Membros como operadoras de serviços essenciais (OES) terão de tomar as medidas de segurança adequadas e notificar incidentes graves à autoridade nacional competente. Os principais operadores de serviços digitais (DSP) terão de cumprir os requisitos de segurança e notificação ao abrigo da nova diretiva.

Nestes últimos anos tem sido vários os instrumentos jurídicos emitidos pela UE. Estes instrumentos são apresentados já de seguida, destacando-se as principais disposições da Diretiva (UE) 2016/114871 sobre a segurança das redes e da informação (SRI), a Lei n. º46/2018 de 13 de agosto e o Decreto-Lei n.º 65/2021, de 6 de julho.

2.5.2 Instrumentos Jurídicos

2.5.2.1 A Diretiva SRI

A **Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho**, aprovada em 2016, relativa a medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na União (Diretiva SRI) é o primeiro instrumento do mercado interno que tem por objetivo melhorar a resiliência da UE contra os riscos de cibersegurança. Visa assegurar a continuidade dos serviços que permitem o bom funcionamento da economia e da sociedade na União, introduzindo medidas concretas destinadas a reforçar as capacidades em matéria de cibersegurança em toda a EU(P. E. e o C. da U. Europeia, 2016).

Esta Diretiva fornece medidas jurídicas para aumentar o nível geral de cibersegurança na UE, garantindo (P. E. e o C. da U. Europeia, 2016):

- Preparação dos Estados-Membros, exigindo que estejam devidamente equipados. Por exemplo, com "*Computer Security Incident Response Team*" (CSIRT), Autoridade Nacional competente NIS e Estratégia nacional de segurança das redes e dos sistemas de informação;
- Cooperação entre todos os Estados-Membros, mediante a criação do grupo de cooperação para apoiar e facilitar a cooperação estratégica e o intercâmbio de informações entre os Estados-Membros;
- Uma cultura de segurança em todos os setores que são essenciais para a economia e sociedade e que dependem fortemente das TICs, como energia, transporte, água, bancos, infraestruturas do mercado financeiro, saúde e infraestruturas digitais.

2.5.2.2 Lei n.º 46/2018, 13 de agosto

A Lei n. º46/2018 de 13 de agosto, que estabelece o Regime Jurídico da Segurança do Ciberespaço, transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União (Diretiva SRI). A Lei aplica-se a toda a administração pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais e a quaisquer outras entidades que utilizem redes e sistemas de informação (Assembleia da República, 2018).

A presente legislação visa definir (Assembleia da República, 2018):

- **Estratégia Nacional de Segurança do Ciberespaço (ENSC):**
    - Define o enquadramento, os objetivos e as linhas de ação do Estado nesta matéria, de acordo com o interesse nacional.
- **Conselho Superior de Segurança do Ciberespaço:**
    - Órgão específico de consulta do Primeiro-Ministro, ou ao membro do Governo em quem este delegar, para os assuntos relativos à segurança do ciberespaço.
    - Assegura a coordenação político-estratégica para a segurança do ciberespaço.
- **Centro Nacional de Cibersegurança (CNCS) - Autoridade Nacional de Cibersegurança:**
    - Ponto de contacto único nacional para efeitos de cooperação internacional, sem prejuízo das atribuições legais da Polícia Judiciária relativas a cooperação internacional em matéria penal.
    - Exerce as funções de regulação, regulamentação, supervisão, fiscalização e sancionatórias nos termos das suas competências.
    - Tem o poder de emitir instruções de cibersegurança e de definir o nível nacional de alerta de cibersegurança.
    - Atua em articulação e estreita cooperação com as estruturas nacionais responsáveis pela ciberespionagem, ciberdefesa, cibercrime e ciberterrorismo, devendo comunicar à autoridade competente, no mais curto prazo, os factos de que tenha conhecimento relativos à preparação e execução de crimes.
    - Atua em articulação com a Comissão Nacional de Proteção de Dados (CNPD) quando estejam em causa incidentes que tenham dado origem à violação de dados pessoais.
    - Pode solicitar a quaisquer entidades públicas ou privadas toda a colaboração ou auxílio que julgue necessários para o exercício das suas atividades.
    - Qualquer disposição legal de cibersegurança carece do parecer prévio do CNCS.
- **CERT.PT - Equipa de Resposta a Incidentes de Segurança Informática Nacional, a qual funciona no CNCS:**

- Exerce a coordenação operacional na resposta a incidentes, nomeadamente em articulação com as equipas de resposta a incidentes de segurança informática setoriais existentes.
- Monitoriza os incidentes com implicações a nível nacional.
- Ativa mecanismos de alerta rápido.
- Intervém na reação, análise e mitigação de incidentes.
- Procede à análise dinâmica dos riscos.
- Assegura a cooperação com entidades públicas e privadas.
- Promove a adoção e a utilização de práticas comuns ou normalizadas.
- Participa nos fóruns nacionais de cooperação de equipas de resposta a incidentes de segurança informática.
- Assegura a representação nacional nos fóruns internacionais de cooperação de equipas de resposta a incidentes de segurança informática.
- Participa em eventos de treino nacionais e internacionais.

- **Requisitos de segurança**
  - Definidos de forma a permitir a utilização de normas e especificações técnicas internacionalmente aceites aplicáveis à segurança das redes e dos sistemas de informação, sem imposição ou discriminação em favor da utilização de um determinado tipo de tecnologia.
  - Medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam.
- **Requisitos de notificação de incidentes**
  - Notificar o CNCS dos incidentes com um impacto relevante na segurança das respetivas redes e dos sistemas de informação.

2.5.2.3 Decreto-Lei n.º 65/2021, de 6 de julho

Com a publicação do Decreto-Lei n.º 65/2021 procede-se à regulamentação dos aspetos remetidos para legislação complementar na Lei n.º 46/2018, de 13 de agosto. Neste sentido, o decreto-lei estabelece os requisitos de segurança das redes e sistemas de informação e de notificação de incidentes que devem ser cumpridos pelas entidades identificadas na Diretiva SRI – entidades da Administração Pública, Operadores de Infraestruturas Críticas, Operadores de Serviços Essenciais dos setores da energia, transportes, bancário, infraestruturas do mercado financeiro, saúde,

fornecimento e distribuição de água potável e infraestruturas digitais e pelos Prestadores de Serviços Digitais (Decreto-Lei no 65, 2021).

- **Disposições comuns:**
    - Indicação de, pelo menos, um ponto de contacto permanente, de modo a assegurar os fluxos de informação de nível operacional e técnico com o CNCS.
    - Designação de um responsável de segurança para a gestão do conjunto das medidas adotadas em matéria de requisitos de segurança e de notificação de incidentes.
    - Elaboração e atualização de um inventário de todos os ativos essenciais para a prestação dos respetivos serviços.
    - Elaboração e atualização de um plano de segurança, devidamente documentado e assinado pelo responsável de segurança.
    - Elaboração de um relatório anual.
- **Segurança das redes e dos sistemas de informação**
    - As entidades devem cumprir as medidas técnicas e organizativas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam, devendo, para o efeito, realizar uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam, sendo, no caso dos operadores de serviços essenciais, também em relação aos ativos que garantam a prestação dos serviços essenciais.
    - Na sequência de cada análise dos riscos, as entidades devem adotar as medidas técnicas e organizativas adequadas para gerir os riscos que se colocam à segurança as redes e dos sistemas de informação que utilizam, e que resultem, nomeadamente:
        - ✓ De normativo complementar setorial aprovado pelo CNCS, sem prejuízo da aplicação de outro normativo nacional e da UE em matéria da segurança das redes e dos sistemas de informação.
        - ✓ Do Quadro Nacional de Referência de Cibersegurança (QNRCS), e respetivas disposições complementares, elaborado pelo CNCS.
- **Notificação de Incidentes**
    - As entidades devem implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacto e à notificação de incidentes com impacto relevante ou substancial.

- **Notificação inicial** - deve ser enviada logo que a entidade possa concluir que existe ou possa vir a existir impacto relevante ou substancial e até duas horas após essa verificação.
- **Uma notificação de fim de impacto relevante ou substancial** - deve ser submetida ao Centro Nacional de Cibersegurança logo que possível, dentro do prazo máximo de duas horas após a perda de impacto relevante ou substancial.
- **Notificação final** - deve ser enviada no prazo de 30 dias úteis a contar do momento em que o incidente deixou de se verificar.

2.5.2.4 Regulamento n.º 183/2022

Instrução Técnica complementar, tendo como base legal a previsão do n.º 5 do artigo 7.º da Lei n.º 46/2018, de 13 de agosto, para definir os termos de aplicação deste normativo quanto às disposições do Decreto-Lei n.º 65/2021, de 30 de julho, referentes a ponto de contacto permanente, responsável de segurança, inventário de ativos, relatório anual e notificação de incidentes (República, 2021).

Em resumo, A Lei n.º 46/2018, de 13 de agosto, estabeleceu o Regime Jurídico da Segurança do Ciberespaço (RJSC), transpondo a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União.

O Regime Jurídico da Segurança do Ciberespaço aplica-se às entidades da Administração Pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais, bem como a quaisquer outras entidades que utilizem redes e sistemas de informação, nomeadamente, no âmbito da notificação voluntária de incidentes.

2.6 Sumário da Revisão da Literatura

Em suma, tal como mencionado na literatura, um projeto é considerado um "conjunto único de processos consistindo em atividades coordenadas e controladas com datas de início e de fim, desenvolvidas para alcançar um objetivo" com o prepósito de trazer benefícios às diferentes organizações.

Tendo em conta o seu caracter inovador, os desenvolvimentos dos projetos estão em plena evolução e mudança, mudanças essas que podem acarretar riscos incalculáveis para as organizações. Dessa forma, surge a área da gestão de risco que consiste num conjunto de processos, técnicas e ferramentas que têm como objetivo identificar, analisar e responder aos riscos de um projeto com

o objetivo de minimizar a probabilidade e o impacto que estes possam causar ao seu desenvolvimento.

Acompanhando a evolução da gestão de projetos está a cibersegurança, cada vez mais presente no dia-a-dia das organizações, garantindo que estas tomam as medidas necessárias para proteger um conjunto de dispositivos, equipamentos, serviços e dados associados a esses sistemas. Com esta evolução, a UE viu-se obrigada a desenvolver instrumentos jurídicos de resposta coordenada e de recuperação de incidentes que estabelece uma série de medidas (tais como a obrigação de notificação de incidentes graves e de atender aos requisitos de segurança, gestão de risco de segurança de informação) para a prevenção e tratamento de ciberincidentes nas infraestruturas críticas essenciais para o funcionamento da sociedade.

Outro foco importante, é a implementação da gestão do risco de segurança da informação nas organizações, que tem como objetivo ajudar na identificação e na deteção de riscos, ou determinar a probabilidade de estes virem a existir. A gestão do risco não é mais do que a aplicação de sistemas, políticas, metodologias, procedimentos e boas práticas com vista a identificar, analisar, avaliar e monitorizar possíveis incidentes ligados à informação, a fim de alcançar os objetivos de negócio.

Com o prepósito de dar cumprimento aos instrumentos jurídicos criados para a cibersegurança, o projeto visa o desenho de um processo de implementação do DL n.º65/2021 em Operadores de Serviços Essenciais e Administração Pública, com o propósito de dar cumprimento a todos os requisitos da norma, incluindo a gestão de risco na segurança da informação.

Para tal a metodologia adequada é a chamada investigação-ação ou *action-research*, apresentada no próximo capítulo.

3. Metodologia de Investigação

O presente capítulo descreve a metodologia utilizada para o desenvolvimento do projeto avançado. Inicialmente é realizada uma contextualização metodológica, justificando o porquê da escolha da mesma. De seguida é realizada a contextualização do estudo desenvolvido.

3.1 Metodologia

A recolha de dados é um fator crucial de pesquisa e extremamente importante para conduzir a investigação. A metodologia adaptada para a recolha de dados é baseada em Saunders, M., Lewis, P., and Thornhill (2009) e no método da "pesquisa cebola", ilustrada na Figura 23. Este método permite explicar e justificar a metodologia, abordagem e estratégias utilizada no desenvolvimento do projeto avançado, bem como os métodos de pesquisa e recolha de dados para o seu desenvolvimento.

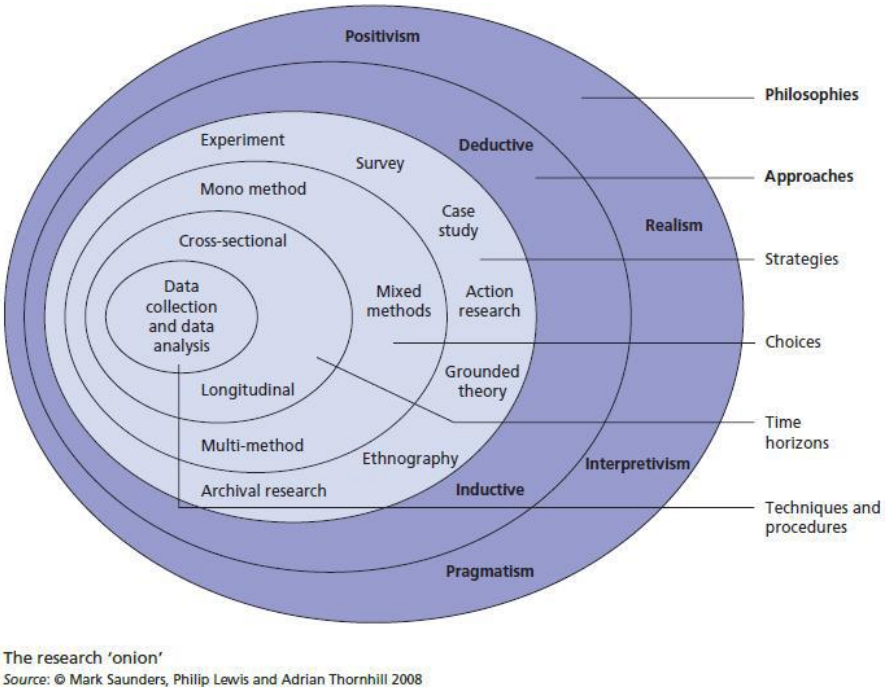


Figura 23 - "Cebola" de investigação
Fonte: Saunders, M., Lewis, P., and Thornhill (2009

Seguindo a linha de metodológica referenciada por Saunders, M., Lewis, P., and Thornhill (2009), existem três métodos principais: métodos quantitativos, qualitativos e mistos. Os dados quantitativos, comumente associados ao positivismo, referem-se a quaisquer informações recolhidas que geram informações numéricas. Em contraste, o método qualitativo, frequentemente associado ao interpretativismo, baseia-se em informação não numérica. O último, o método misto, combina os dados quantitativos e qualitativos e as suas técnicas. Alguns argumentos relativamente

aos métodos mistos, passam por estes terem o potencial de lançar novas perspetivas, aumentar a credibilidade dos resultados, interpretar os resultados juntos e desenvolver uma compreensão teórica mais rica.

Para o presente projeto, a escolha metodológica adotada foi a de uma metodologia mista, utilizando a estratégia de *action-research*, que se distingue das outras metodologias porque o autor é parte integrante da investigação em causa (Somekh, 1995).

Esta metodologia tem vindo a ganhar notoriedade devido ao facto de ser uma metodologia com um curto período de tempo entre o processo de geração de informação e a sua aplicação, o período pode mesmo ser reduzido a zero se o autor aplicar o conhecimento adquirido (Feldman & Minstrell, 2000).

A metodologia *action-research* deve ser aplicada no que está a ser feito na organização em causa, permitindo que seja feito no ambiente produtivo e dessa forma a quantidade de informação obtida pelo investigador seja maior (David Avison, Francis Lau, Michael Myers, 1999).

Feldman & Minstrell, (2000) explicam que esta abordagem pode ser vista sob duas perspetivas diferentes, dependendo do peso que é atribuído à componente de *action* e à componente de *research*.

Como referido por Baskerville (1999) a metodologia *action-research* contempla duas fases distintas:

1) a fase de diagnóstico que envolve uma análise colaborativa entre o autor do artigo e o alvo da investigação, sendo também nesta fase formuladas as teorias e os processos de acordo com a atividade-alvo;
2) a fase terapêutica e envolve experiências com base nos resultados obtidos da primeira fase. É nesta fase que as alterações são introduzidas nos processos e os resultados dessas alterações começam a ser estudados.

Por outro lado, Kemmis, S., & McTaggart, (1988) defendem que se trata de uma *action-research* quando a mesma é colaborativa e é desenvolvida através da ação. As suas fases podem ser descritas no seguinte modo:

1) Identificação, avaliação e formulação do problema;
2) Discussão preliminar e negociação entre os parceiros interessados;
3) Revisão da literatura na área de investigação;
4) Revisão da formulação inicial do problema;
5) Seleção de procedimentos de investigação;
6) Seleção dos procedimentos de avaliação;
7) Implementação do projeto;

8) Interpretação dos dados recolhidos.

A metodologia *action-research* , além de se caracterizar como uma metodologia de investigação impregnada de métodos, critérios e de onde acabam por originar teorias sobre a atividade, ela ganha consistência e marcas distintivas comparativamente a outras metodologias, na medida em que se impõe como um "projeto de ação", tendo que transportar em si "estratégias de ação" que o investigador adapta consoante as suas necessidades e face às situações com que se depara no decorrer do projeto (Latorre, 2003).

Kemmis (1989) baseia-se num modelo de caracter cíclico, direcionado concretamente para o contexto educativo, em que o processo assenta em duas vertentes: estratégia e organizativa. Na primeira temos ação e a reflexão como pontos-chave, enquanto na segunda reflete os aspetos da planificação e da observação, interagindo estes fatores de forma constante e de modo a contribuírem para a resolução de problemas e para a compreensão das práticas pedagógicas.

A *action-research*, de acordo com Kemmis (1989), integra quatro momentos (Figura 24): planificação, ação, observação e reflexão, implicando cada um deles, simultaneamente, um olhar retrospetivo e prospetivo, gerando uma espiral autorreflexiva de conhecimento e ação.

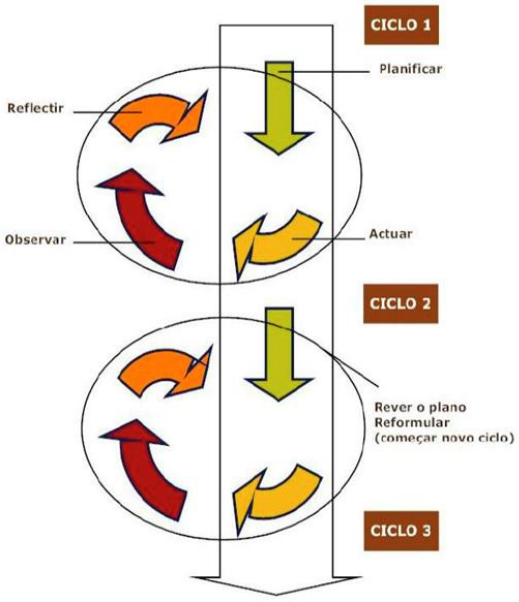


Figura 24 - Momentos de *action-research*,
Fonte: Adaptado de Kemmis, (1989)

O modelo de Kemmis (1989), representado na Figura **24**, demonstra que um processo de *action-research* não se limita única e exclusivamente à realização de um único ciclo, verificando-se:

1) O desenvolvimento de um plano de ação com base numa informação crítica e com a intenção de alterar, para melhor, determinada situação;

2) O estabelecimento de um consenso para pôr o plano em andamento;
3) A observação dos efeitos da ação revestidos da necessária contextualização;
4) A reflexão sobre esses resultados, servindo como ponto de partida para nova planificação e, assim, dar início a uma nova sequência de ciclo de espirais.

3.2 Contextualização do Estudo

O presente projeto avançado enquadra-se na prestação de serviços de uma empresa com foco em soluções e serviços de cibersegurança, a OES e organizações da Administração Pública. Dado o estabelecimento do Regime Jurídico da Segurança do Ciberespaço e o estabelecimento dos requisitos de segurança das redes e sistemas de informação e de notificação de incidentes, estes organismos viram-se obrigados a pedir ajuda à empresa de forma a ficar em conformidade com a legislação.

A Empresa

A Prestadora de Serviços é uma empresa portuguesa criada no final de 2015, que tem como principal foco o fornecimento de soluções e serviços na área de cibersegurança. O seu portfólio incluí as mais avançadas soluções, nomeadamente SIEM (*Security Information and Event Management*), *Advanced Persistent Threats* (APT), *Authentication*, *Application Security* e *Data Security*, em parceria com fornecedores líderes na área de ciberseguranca como *Microsoft*, *Micro Focus*, *Trellix*, *Palo Alto Networks*, *Fortinet*, *Rapid7*, *Sophos* entre outros.

Como forneceder de Serviços de Segurança, esta empresa ajuda as organizações na deteção e resposta a ameaças cibernéticas em tempo real, gestão completa de soluções de segurança cibernética existentes nos clientes e serviços especializados de Consultoria na área de *Security Consulting*.

Esta empresa integra ainda a "Rede Nacional de CSIRT", uma rede portuguesa de CSIRT que integra o Centro Nacional Português de Cibersegurança, CERT.PT. A empresa foi também nomeada como PME líder durante o ano de 2021.

Operador de Serviço Essencial (OES)

O processo de identificação de operadores de serviços essenciais foi realizado pelo Centro Nacional de Cibersegurança (CNCS) em conjunto com as entidades reguladoras setoriais e com as entidades com poderes de supervisão no setor dos Transportes e subsetor de Transporte Rodoviário, de acordo com os critérios por estas definidos.

A designação de uma organização como Operador de Serviço Essencial (OES) foi alcançada através do estabelecimento de definições e limites na legislação relativa ao âmbito das operações que

realiza, sendo que os limites foram definidos com base no nível de impacto social ou económico que poderia resultar da interrupção dos serviços prestados.

Todavia, de acordo com os termos do n.º 2 do artigo 29.º da Lei n.º 46/2018, de 13 de agosto, a identificação de operadores de serviços essenciais será objeto de atualização anual.

Sem prejuízo do âmbito de aplicação geral do articulado da Lei n.º 46/2018, de 13 de agosto, o regime jurídico da segurança do ciberespaço incide de forma direta sobre os operadores de serviços essenciais através dos artigos 16.º e 17.º que estabelecem a previsão de requisitos de segurança e de notificação de incidentes para estas entidades, os quais nos termos do artigo 31.º da mesma lei são definidos em legislação própria a aprovar.

Em suma, a organização foi identificada, conforme notificação do CNCS feita através de carta, como operador de serviço essencial, nos termos do n.º 1 do artigo 29.º da Lei n.º 46/2018, de 13 de agosto, no setor dos Transportes, subsetor de Transporte Rodoviário, de acordo com o Anexo da Lei n.º 46/2018, de 13 de agosto, como mostra a Figura 25 abaixo, encontrando-se assim vinculada à aplicação da Lei n.º 46/2018, de 13 de agosto, e respetiva regulamentação.

Setor	Subsetor	Tipo de entidades
Energia	Eletricidade	Empresa de eletricidade que exerce a atividade de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte.
	Petróleo	Operadores de oleodutos de petróleo. Operadores de instalações de produção, refinamento e tratamento, armazenamento e transporte de petróleo.
	Gás	Empresas de comercialização. Operadores da rede de distribuição. Operadores da rede de transporte. Operadores do sistema de armazenamento. Operadores da rede de gás natural em estado líquido (GNL). Empresas de gás natural. Operadores de instalações de refinamento e tratamento de gás natural.
Transportes	Transporte aéreo	Transportadoras aéreas. Entidades gestoras aeroportuárias, aeroportos e as entidades que exploram instalações anexas existentes dentro dos aeroportos. Operadores de controlo da gestão do tráfego aéreo que prestam serviços de controlo de tráfego aéreo.
	Transporte ferroviário	Gestores de infraestruturas. Empresas ferroviárias incluindo os operadores de instalações de serviço.
	Transporte marítimo e por vias navegáveis interiores.	Companhias de transporte por vias navegáveis interiores, marítimo e costeiro de passageiros e de mercadorias, não incluindo os navios explorados por essas companhias. Entidades gestoras dos portos, incluindo as respetivas instalações portuárias e as entidades que gerem as obras e os equipamentos existentes dentro dos portos. Operadores de serviços de tráfego marítimo.
	Transporte rodoviário	Autoridades rodoviárias. Operadores de sistemas de transporte inteligentes.
Bancário	—	Instituições de crédito.
Infraestruturas do mercado financeiro	—	Operadores de plataformas de negociação. Contrapartes centrais.
Saúde	Instalações de prestação de cuidados de saúde.	Prestadores de cuidados de saúde.
Fornecimento e distribuição de água potável.	—	Fornecedores e distribuidores de água destinada ao consumo humano, mas excluindo os distribuidores para os quais a distribuição de água para consumo humano é apenas uma parte da sua atividade geral de distribuição de outros produtos de base e mercadorias não considerados serviços essenciais.
Infraestruturas digitais	—	Pontos de troca de tráfego.

Figura 25 - Anexo da Lei n.º 46/2018 - Setores, subsetores e tipos de entidades dos operadores de serviços essenciais
Fonte: Adaptado da Assembleia da República, (2018)

Como mencionado, a organização foi identificada como OES, por ser uma das entidades responsáveis pela disponibilização da infraestrutura rodoviária para a circulação de veículos autorizados nas autoestradas em Portugal. Desta forma, deve cumprir com as medidas técnicas e organizativas adequadas e proporcionais para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utiliza na prestação do serviço essencial.

Administração Pública

No âmbito da legislação nacional, nomeadamente, no Regime Jurídico de Segurança no Ciberespaço (Lei nº 46/2018 de 14 de agosto), através do qual foi transposta a Diretiva NIS (Diretiva (UE) n.º 2016/679), existem medidas destinadas a garantir um elevado nível de segurança das redes e da informação a que a Administração Pública, Operadores de Infraestruturas Críticas, Operadores de Serviços Essenciais (OES) e Operadores de Serviços Digitais estão obrigados a cumprir.

Nesse sentido, as duas organizações, sendo uma sociedade anónima de capitais exclusivamente públicos, responsável pela gestão e exploração do sistema multimunicipal nos domínios do abastecimento de água e do saneamento de águas residuais viram-se obrigadas a cumprir os requisitos exigidos pelo regime jurídico da segurança do ciberespaço nos termos do nº 2 alínea f) do artigo 2º da Lei n.º 46/2018, de 13 de agosto (Figura 26).

Artigo 2.º

Âmbito

1 — A presente lei aplica-se:

a) À Administração Pública;
b) Aos operadores de infraestruturas críticas;
c) Aos operadores de serviços essenciais;
d) Aos prestadores de serviços digitais;
e) A quaisquer outras entidades que utilizem redes e sistemas de informação.

2 — Para efeitos do disposto na presente lei, integram a Administração Pública:

a) O Estado;
b) As regiões autónomas;
c) As autarquias locais;
d) As entidades administrativas independentes;
e) Os institutos públicos;
f) As empresas públicas;
g) As associações públicas.

Figura 26 - Artigo 2º da Lei n. º46/2018
Fonte: Adaptado de Assembleia da República, (2018)

O Projeto

Como mencionado anteriormente, o projeto avançado em desenvolvimento trata-se de um "Processo de implementação do Decreto-Lei n.º 65/2021 em Operadores de Serviços Essenciais e na Administração Pública", cujo principal objetivo centra-se na aplicação de uma metodologia de

gestão de risco no contexto da segurança da informação, através da criação de um processo. Essa metodologia baseia-se nos referenciais desenvolvidos pelo PMI no que diz respeito à gestão de projetos, e na segurança da informação baseia-se na ISO/IEC 27005.

Em resumo, o projeto avançado tem de desenvolver e melhorar os processos e procedimentos no âmbito do cumprimento dos requisitos estabelecidos pelo Decreto-Lei n.º 65/2021, o que implica que toda a informação recolhida e os processos desenhados no decorrer dos trabalhos serão implementados nas organizações descritas. Abaixo, apresenta-se o desenvolvimento dos processos e procedimentos de acordo com as metodologias descritas na revisão da literatura.

3.3 Aplicação da metodologia ao projeto

Neste capítulo é descrito o processo criado, são referidos aspetos práticos da sua aplicação nas organizações que serviram de base à validação do processo.

Aplicou-se uma metodologia de gestão do risco direcionada para a segurança da informação, com o princípio da criação de processos que permitam e facilitem o cumprimento dos requisitos exigidos pelo DL n. º65/2021.

Neste seguimento, foi desenvolvido um processo de cumprimento dos requisitos do DL n. º65/2021 para OES e Administração Pública, seguindo-se o desenvolvimento de uma metodologia de Gestão de Riscos adotando uma perspetiva de gestão de projetos.

3.3.1 Gestão de Risco do Projeto

Tendo em consideração a revisão bibliográfica elaborada e o contexto dos casos de estudo, procurou-se analisar e refletir acerca dos processos de Gestão de Riscos no projeto nas diferentes organizações e a metodologia de gestão do risco aplicada.

A metodologia de gestão do risco do projeto a apresentar tem como início a constituição do planeamento de gestão do risco onde estão incluídas as técnicas e ferramentas utilizadas na identificação, na avaliação qualitativa, na avaliação quantitativa, no planeamento das respostas aos riscos e na monitorização dos mesmos. A metodologia aplicada usa é baseada no PMI (2009, 2017a, 2019).

Planeamento da Gestão de Risco

O planeamento da Gestão de Risco visa orientar o gestor de projeto e a restante equipa na implementação das atividades que compõe a gestão de risco do projeto, definindo as diferentes práticas e processos da gestão de risco que devem ser aplicadas durante todo o ciclo de vida de

gestão do portefólios e projeto, com o objetivo de melhorar os resultados globais nos vários níveis da implementação do DL nas diferentes organizações em estudo.

Devido à baixa maturidade em gestão de projetos da empresa que implementou o processo nas organizações, a componente de análise quantitativa dos riscos nos portefólios e no projeto, não será alvo de análise.

Dessa forma, o planeamento da gestão do risco determina a existência de documentos como o registo dos riscos, o relatório de lições aprendidas, determina também, a RBS do projeto que se encontra documentado no registo do risco.

Uma vez que a Gestão de Risco é um processo cíclico, continuo e iterativo, o registo dos riscos deve ser atualizado com uma periocidade regular, com a execução de reuniões de ponto de situação, e reuniões de *Steering Committee*.

Identificação dos riscos

Inicialmente, desenvolveu-se a RBS, representada na Figura **27**, tendo como princípio a informação descrita na revisão da literatura.

Figura 27 - RBS do Projeto,
Fonte: Elaboração Própria

No que diz respeito ao registo dos riscos, foi criado um documento referente à identificação do risco, que deve ser abordado nas diversas reuniões de ponto de situação e possíveis *Steering Committee*, onde é possível considerar, conforme a Tabela **9**:

- ID do Risco;

- Data do registo do risco;
- Descrição do risco;
- Categoria da RBS;
- Responsável;
- Causa;
- Impacto.

ID do Risco	Data do registo do risco	Descrição do Risco	Categoria do RBS	Responsável	Causas	Impactos
1	08/11/2021	Falta de comprometimento dos recursos da empresa no Projeto	3. Riscos Organizacionais	Owner	Baixo desempenho do recurso; Falta de satisfação do recursos perante as suas responsabilidades no projeto	Qualidade do projeto pode não satisfazer os critérios do cliente, o que pode impedir novos projetos na área e o com cliente
2	08/11/2021	Falta de comprometimento das organizações (cliente)	2. Riscos Externos	Owner	Baixo desempenho do recurso do cliente atribuido ao projeto; Falta de satisfação do recursos perante as suas responsabilidades no projeto	Qualidade do projeto pode ser afetado, dado à escassa informação partilhada pelo cliente; Incumprimento de algum dos requisitos que pode levar a sanção impostas pela Lei n.º 46
3	08/11/2021	Falta de liderança de gestão	3. Riscos Organizacionais	Owner	Sobregarga de projetos	Não cumprimento do projeto; Incumprimento de algum dos requisitos que pode levar a sanção impostas pela Lei n.º 46
4	08/11/2021	Os recursos da empresa não são qualificados para a função	1. Riscos Técnicos	Owner	Os recursos podem não possuir o conhecimento necessário para a função que estão a desempenhar; Falta de formação e comprometimento do recurso	Atraso no cronograma; Incumprimento de algum dos requisitos que pode levar a sanção impostas pela Lei n.º 46
5	14/12/2021	Divergência entre a data de início oficial e a data de início efetiva	4. Riscos de Gestão	Gestor de Projetos	Possivel atraso na assinatura do contrato devido às burocracias	Atraso no cronograma; Incumprimento de algum dos requisitos que pode levar a sanção impostas pela Lei n.º 46
6	14/12/2021	Atrasos na execução financeira por parte das organizações	3. Riscos Organizacionais	Cliente	Falta de capital; Equipa de contabilidade com atrasos nos processos; Burocracia em demasia na administração pública	Atraso no cronograma; Incumprimento de algum dos requisitos que pode levar a sanção impostas pela Lei n.º 46
7	14/12/2021	Não cumprimento das cláusulas dos contratos	3. Riscos Organizacionais	Gestor de Projetos	Objetivos do projeto não serem atingidos; os recursos alocados não são os inicialmente mencionados	Não cumprimento do projeto; Incumprimento de algum dos requisitos que pode levar a sanção impostas pela Lei n.º 46; Sanções financeiras para a empresa
8	14/12/2021	Saída de recursos humanos chaves durante o seu ciclo de vida	1. Riscos Técnicos	Owner	Eventual precariedade nas condições de trabalho; Ofertas mais atrativas; Conflitos dentro da empresa	Atrasos na cumprimento do projeto; Incumprimento de algum dos requisitos que pode levar a sanção impostas pela Lei n.º 46; Desmotivação e sobrelotação dos restantes recursos
9	14/12/2021	Atraso nas atividades e respetiva calendarização	4. Riscos de Gestão	Gestor de Projetos	Mau planeamento das atividades; Falta de interação entre os recusos;	Atraso no cronograma; Incumprimento de algum dos requisitos que pode levar a sanção impostas pela Lei n.º 46; Aumento do custo do projeto
10	14/12/2021	Não cumprimento dos entregáveis do Projeto	1. Riscos Técnicos	Gestor de Projetos	Não cumprir com os requisitos do DL	Atraso no cronograma;Não cumprimento do projeto; Incumprimento de algum dos requisitos que pode levar a sanção impostas pela Lei n.º 46
11	14/12/2021	Falta de comunicação entre as diferentes partes interessadas	4. Riscos de Gestão	Gestor de Projetos	Falta de comunicação entre as diferentes equipas do projeto	Atraso no cronograma; Incumprimento de algum dos requisitos que pode levar a sanção impostas pela Lei n.º 46
12	08/11/2021	Alteração/ Atualização das directrizes do CNCS ou das respetivas autoridades setoriais	2. Riscos Externos	Owner /Cliente	Revisão do CNCS e das autoridades setoriais das diretrizes existentes	Alteração do cronograma
13	08/11/2021	Alteração/Atualização da legislação setorial	2. Riscos Externos	Owner /Cliente	Alteração da legislação por parte das diferentes autoridades setoriais, o que implicaria a alteração dos requisitos	Alteração do cronograma

Tabela 9 - Identificação do Risco,
Fonte: Elaboração Própria

No decorrer desta atividade, foram identificados os seguintes riscos:

- Falta de comprometimento dos recursos da empresa no Projeto;
- Falta de comprometimento das organizações (cliente);
- Falta de liderança de gestão;
- Os recursos da empresa não são qualificados para a função;
- Divergência entre a data de início oficial e a data de início efetiva;
- Atrasos na execução financeira por parte das organizações;
- Não cumprimento das cláusulas dos contratos;
- Saída de recursos humanos chaves durante o seu ciclo de vida;
- Atraso nas atividades e respetiva calendarização;
- Não cumprimento dos entregáveis do Projeto;
- Falta de comunicação entre as diferentes partes interessadas;

- Alteração/ Atualização das diretrizes do CNCS ou das respetivas autoridades setoriais;
- Alteração/Atualização da legislação setorial.

Análise qualitativa dos riscos

Na realização do projeto avançado realizaram-se as reuniões de *kick-off*, onde inicialmente se recolheram os riscos base do projeto. Durante o decorrer do mesmo, foram realizadas, junto das equipas das organizações, várias reuniões de ponto de situação, de onde surgiram algumas questões que obrigaram a gerir o risco das mesmas.

Como referido anteriormente, a metodologia a adotar para o projeto avançado foi a gestão de risco desenvolvido pelo PMI, pelo que, a matriz de probabilidade e impacto adotada foi a mesma descrita na revisão da literatura e representada na Tabela 10.

	Impacto				
Probabilidade	0.05	0.1	0.2	0.4	0.8
0.9	0.05	0.09	0.18	0.36	0.72
0.7	0.04	0.07	0.14	0.28	0.56
0.5	0.03	0.05	0.10	0.20	0.40
0.3	0.02	0.03	0.06	0.12	0.24
0.1	0.01	0.01	0.02	0.04	0.08

Legenda:

	Baixo		Moderado		Alto

Tabela 10 - Matriz de Probabilidade e Impacto do projeto,
Fonte: Adaptado de Peixoto et al. (2014)

Nas reuniões onde se identificavam os diversos riscos referidos acima, e uma vez que se encontravam presentes os gestores de projeto tanto da empresa como da parte do cliente, foi possível realizar a análise de risco, visto que os critérios foram acordados no decorrer da reunião de *kick-off*. Dessa forma, nesta atividade foi considerada:

- Qualificação do Impacto, de acordo com o custo, cronograma, âmbito e qualidade (Tabela 11);Tabela 11
- Nível do Risco;
- A priorização do risco de acordo com o nível de risco calculado.

	Muito baixo 0.05	**Baixo 0.1**	**Moderado 0.2**	**Alto 0.4**	**Muito alto 0.8**
Custo	Aumento insignificante do custo	<5% de aumento de custo	5-10% de aumento de custo	10-20% de aumento de custo	>20% de aumento de custo

Cronograma	Desvio insignificante do cronograma	Desvio total do cronograma <5%	Desvio total do cronograma 5-10%	Desvio total do cronograma 10-20%	Desvio total do cronograma >20%
Âmbito	Diminuição quase impercetível do âmbito	São afetadas áreas de pouca importância do âmbito	São afetadas Áreas importantes do âmbito	Redução do âmbito inaceitável para o cliente	Produto final do projeto inadequado
Qualidade	Degradação quase impercetível da qualidade	São afetadas apenas as aplicações mais exigentes	Redução da qualidade requer a aprovação do cliente	Redução da qualidade inaceitável para o cliente	Projeto e produto final do projeto inutilizável

Tabela 11 - Qualificação do Impacto do Projeto,
Fonte: Elaboração Própria

Assim sendo, e após analise verificou-se que dos 13 riscos identificados apenas quatro se encontravam no nível de risco baixo, quatro localizam-se no nível de risco moderado e os restantes cinco no nível de risco alto. Esta análise é refletida na Tabela 12.

ID do Risco	Data do registo do risco	Descrição do Risco	Impacto	Probabilidade	Nível de Risco
2	08/11/2021	Falta de comprometimento das organizações (cliente)	0,8	0,5	0,40
8	14/12/2021	Saída de recursos humanos chaves durante o seu ciclo de vida	0,8	0,5	0,40
9	14/12/2021	Atraso nas atividades e respetiva calendarização	0,8	0,5	0,40
10	14/12/2021	Não cumprimento dos entregáveis do Projeto	0,8	0,5	0,40
5	14/12/2021	Divergência entre a data de início oficial e a data de início efetiva	0,8	0,3	0,24
11	14/12/2021	Falta de comunicação entre as diferentes partes interessadas	0,4	0,3	0,12
7	14/12/2021	Não cumprimento das cláusulas dos contratos	0,8	0,1	0,08
1	08/11/2021	Falta de comprometimento dos recursos da empresa no Projeto	0,2	0,3	0,06
4	08/11/2021	Os recursos da empresa não são qualificados para a função	0,2	0,3	0,06
3	08/11/2021	Falta de liderança de gestão	0,4	0,1	0,04
6	14/12/2021	Atrasos na execução financeira por parte das organizações	0,2	0,1	0,02
12	08/11/2021	Alteração/ Atualização das directrizes do CNCS ou das respetivas autoridades setoriais	0,1	0,1	0,01
13	08/11/2021	Alteração/Atualização da legislação setorial	0,1	0,1	0,01

Tabela 12 - Riscos ordenados de acordo a sua criticidade,
Fonte: Elaboração Própria

Os riscos altos devem, por sua vez, ser tratados com alguma urgência a fim de serem evitados ou transformados em riscos mais residuais, os riscos moderados requerem uma supervisão periódica por parte do gestor de projeto e, por fim, os riscos baixos requerem apenas monitorização e controlo.

Resposta aos riscos

O Planeamento das Respostas aos Riscos é um processo de desenvolvimento de alternativas, que permite selecionar estratégias e acordar ações para lidar com a exposição geral aos riscos, e também tratar os riscos individuais do projeto.

Devido à baixa maturidade no âmbito da gestão de projetos, a resposta aos riscos foi realizada única e exclusivamente tendo como pressuposto a análise qualitativa. Assim, o plano de resposta aos riscos foi construído de acordo com a Tabela **13**:

Nível de Risco		Respostas
	Baixo	Mitigar/Aceitar
	Moderado	Reduzir/Mitigar
	Alto	Evitar

Tabela 13 - Resposta ao risco,
Fonte: Fonte Própria

Para a realização do plano de resposta ao risco, as atividades descritas, deverão ser adotadas pelo responsável de cada risco. O objetivo das respostas tende em alterar o nível de risco inicial (risco inerente) para um novo nível de risco (risco residual), de forma a beneficiar o desenvolvimento do projeto.

O plano de respostas criado tendo em conta a informação recolhida na fase de identificação e, através da implementação de boas práticas no que diz respeito à gestão de risco. Este encontra-se identificados na Tabela **14**.

ID do Risco	Data do registo do risco	Descrição do Risco	Resposta	Plano de Resposta ao risco
2	08/11/2021	Falta de comprometimento das organizações (cliente)	**Evitar**	Alteração da documentação de modo a cumprir com as novas diretrizes
8	14/12/2021	Saída de recursos humanos chaves durante o seu ciclo de vida	**Evitar**	Estabelecimento dos canais de comunicação no decorrer da reunião de kick-off; Realização e partilha de atas das reuniões;
9	14/12/2021	Atraso nas atividades e respetiva calendarização	**Evitar**	Preparação de toda a burocracia necessária antes da assinatura do contrato
10	14/12/2021	Não cumprimento dos entregáveis do Projeto	**Evitar**	Compreender os motivos do ão cumprimento; Realizar nova calendaização; Alocação/Contratação de mais recursos para o projeto.
5	14/12/2021	Divergência entre a data de início oficial e a data de início efetiva	**Evitar**	Abertura de novos processos de contratação; Formação do recurso
11	14/12/2021	Falta de comunicação entre as diferentes partes interessadas	**Reduzir/Mitigar**	Compreender o motivo dos atrasos; Planeamento detalhado com todas as atividades a desenvolver para o projeto; Evitar colocar recursos sobrelotados em novos projetos;
7	14/12/2021	Não cumprimento das cláusulas dos contratos	**Reduzir/Mitigar**	Implementação de um controlo das clausulas contratuais (checklist)
1	08/11/2021	Falta de comprometimento dos recursos da empresa no Projeto	**Reduzir/Mitigar**	Alteração da documentação de modo a cumprir com as novas legislações
4	08/11/2021	Os recursos da empresa não são qualificados para a função	**Reduzir/Mitigar**	Definição de uma quantidade máxima de projetos alocados, de modo a evitar a sobrecarga; Realização de uma calendarização geral dos recursos
3	08/11/2021	Falta de liderança de gestão	**Mitigar/Aceitar**	Preparação de toda a burocracia necessária antes da emissão da fatura
6	14/12/2021	Atrasos na execução financeira por parte das organizações	**Mitigar/Aceitar**	Beneficios para os recursos pela quantidade de projetos cumpridos; Atribuição de projetos, formação e contratação de mais recursos de forma a evitar sobrecarga
12	08/11/2021	Alteração/ Atualização das directrizes do CNCS ou das respetivas autoridades setoriais	**Mitigar/Aceitar**	Proporcionar melhores condições; Investir na formação dos recursos; Criar uma perspectiva de carreira (real) tendo em conta os objetivos definidos; Em caso de saída atempada, realizar processo de passagem de conhecimento; Documentar conhecimentos desenvolvidos nos projetos e colocar na intranet
13	08/11/2021	Alteração/Atualização da legislação setorial	**Mitigar/Aceitar**	Reuniões de ponto de situação com mais frequência; Reunião de Steering Committee para explicar a situação e expor as necessidades do projeto

Tabela 14 - Plano de Resposta ao Risco,
Fonte: Elaboração Própria

Monitorização e controlo dos riscos

A monitorização dos riscos é um processo de monitorização da implementação dos planos definidos no processo de resposta aos riscos, de acompanhamento dos riscos identificados, identificação e análise dos novos riscos, e avaliação da eficácia do processo de riscos realizados ao longo do projeto. Esse processo utilizou informações geradas durante a execução do projeto, nomeadamente:

- Identificação de novos riscos;
- Eventuais alterações do nível de risco;
- Ajuste das estratégias de resposta aos riscos previamente definidas;
- Análise da eficiência das respostas aos riscos implementadas;
- Identificação e registo de lições aprendidas e boas práticas aplicadas durante a Gestão de Riscos.

Todas estas atividades foram desenvolvidas em reuniões de projeto, quando o desenvolvimento do projeto assim o carecia. A última reunião foi realizada a 9 de agosto de 2022, data da entrega do relatório da análise de risco para cumprimento do requisito do DL 65/2021. É importante relembrar que projeto ainda se encontra em execução, visto que existe a necessidade de entregar o relatório anual referente ao ano de 2022, e a análise de risco é um processo cíclico, pelo que o contrato ainda se encontra em vigor.

3.3.2 Processo para o cumprimento dos requisitos do DL n. º65/2021.

Como mencionado anteriormente, o projeto avançado consiste na criação de processos e procedimentos concretos para o cumprimento dos requisitos estabelecidos pelo Decreto-Lei n.º 65/2021, desse modo, começou-se por identificar quais os requisitos que as organizações em causa devem cumprir. É de notar que os processos foram testados em OES e Administração Pública.

De acordo com o estipulado no DL n.º 65/2021 e representado na Figura 28, a organização deve:

- Designar o ponto de contato permanente - artigo 4.º do DL n.º 65/2021;
- Designar o responsável de segurança - artigo 5.º do DL n.º 65/2021;
- Elaborar e manter atualizado um inventário de todos os ativos essenciais para a prestação do serviço - artigo 6.º do DL n.º 65/2021;
- Elaborar e manter atualizado um plano de segurança, devidamente documentado e assinado pelo Responsável de segurança - artigo 7.º do DL n.º 65/2021;
- Elaborar um relatório anual deve ser assinado pelo Responsável de segurança - artigo 8.º do DL n.º 65/2021;
- Cumprir as medidas técnicas e organizativas de modo a gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam - artigo 9.º do DL n.º 65/2021;

- Realizar uma análise dos riscos em relação a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação que utilizam e, também aos ativos que garantam a prestação do serviço - artigo 10.º do DL n.º 65/2021;
- Notificar o CNCS da ocorrência de incidentes com impacto relevante ou substancial - artigo 11.º do DL n.º 65/2021;

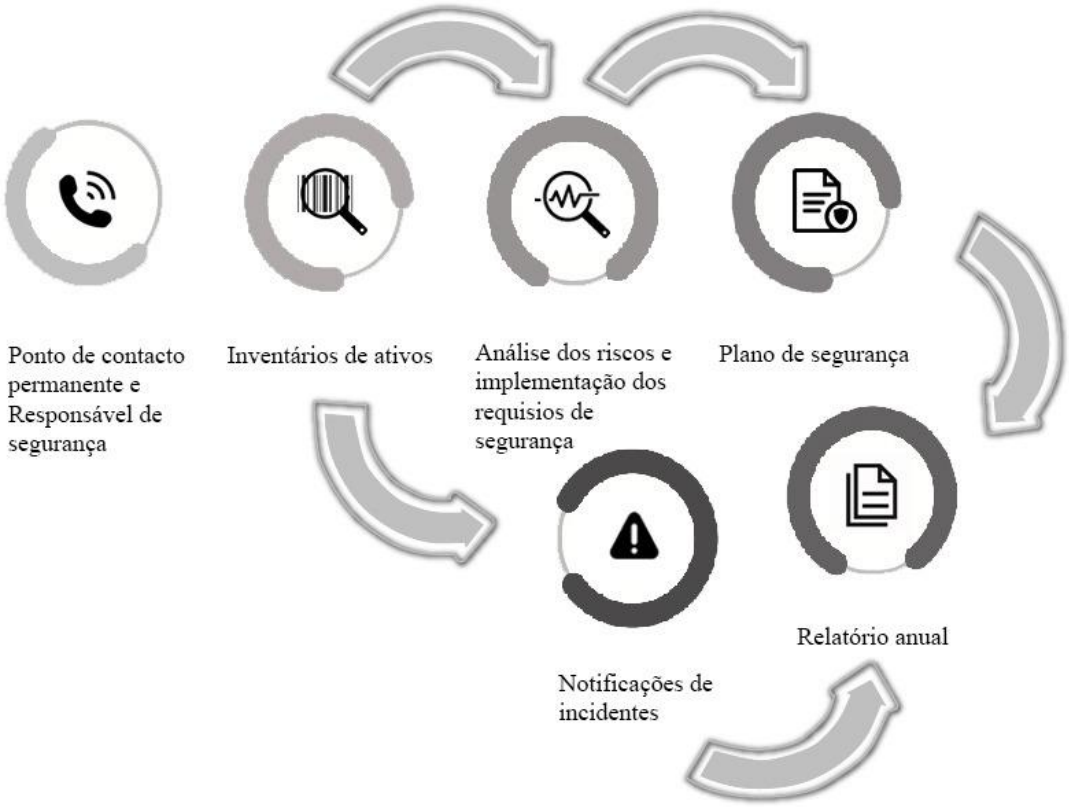


Figura 28 - Obrigações das entidades,
Fonte: Adaptado de Decreto-Lei no 65 (2021); República (2021)

3.3.2.1 Designação do Ponto de Contacto Permanente (PCP) e Responsável de Segurança (RS)

Ponto de Contacto Permanente

A nomeação de um Ponto de Contacto Permanente (PCP) torna-se fundamental para o cumprimento do artigo 4.º, mas sobretudo para que as entidades possam assegurar a função de Ponto de contacto de modo a conferir os fluxos de informação de nível operacional e técnico com o CNCS, nomeadamente:

- A articulação intersectorial, incluindo a eficácia da resposta a incidentes de segurança com impacto a nível dos setores;
- A obtenção de informação operacional e técnica, na sequência de notificação de incidentes com impacto relevante ou substancial submetida pela mesma ou outra entidade;

- A obtenção e atualização de informação de situação integrada no contexto de um incidente com impacto relevante ou substancial;
- A partilha de informação quando estejam ativados planos de emergência de proteção civil diretamente relacionados ou com impacto ao nível da segurança do ciberespaço, bem como de planos no âmbito do planeamento civil de emergência do ciberespaço ou dos planos de segurança das infraestruturas críticas nacionais ou europeias;
- A operacionalização dos procedimentos fixados no âmbito de um plano de emergência de proteção civil quando tenham impacto no funcionamento das redes e sistemas de informação, ou do planeamento civil de emergência do ciberespaço;
- A receção das instruções técnicas emitidas pelo CNCS no âmbito do Regime Jurídico da Segurança do Ciberespaço;
- A operacionalização dos procedimentos fixados no âmbito dos planos de segurança.

A função deve ser assegurada pela entidade com uma disponibilidade contínua de 24 horas por dia e de sete dias por semana, limitada a períodos de ativação, iniciados e terminados mediante comunicação do CNCS.

O PCP poderá ser uma pessoa ou um departamento, interno ou externo através de contratação de serviço externalizado e deverá conhecer os procedimentos e ações a tomar nos vários cenários previstos e categorizados que possam surgir, deverá, também, utilizar os canais apropriados e definidos para este tipo de circunstâncias e deverá ter total disponibilidade total de forma a garantir o suporte, mitigando riscos para a operação e para o negócio.

A indicação do PCP deve ser comunicada ao CNCS:

- no prazo de 20 dias úteis, a contar com o início da atividade da entidade;
- no prazo de 20 dias úteis para as entidades com atividade iniciada antes da entrada em vigor do DL, acrescido de 90 dias relativos ao prazo de produção de efeitos do artigo 4 º do mesmo (6 de dezembro de 2021);
- imediata para qualquer alteração do Ponto de Contacto Permanente da entidade.

Ponto de Contacto Permanente

Nome da entidade	Nome do ponto ou pontos de contacto permanente / serviço disponível ou equipa operacional	Endereço de correio eletrónico principal	Endereço de correio eletrónico alternativo	Número de telefone fixo principal (se aplicável)	Número de telefone móvel principal	Número de telefone fixo alternativo (se aplicável)	Número de telefone móvel alternativo	Outros contactos alternativos	Funções		Comunicação ao CNCS
									Início	Fim	
									dd/mm/aaaa	dd/mm/aaaa	dd/mm/aaaa

Figura 29 - Formulário de Notificação do PCP,
Fonte: Elaboração Própria

Para a realização da comunicação junto do CNCS, e para o cumprimento do requisito, foi criado no âmbito do processo um documento com os requisitos exigidos pelo DL. Este documento será aplicado pelas organizações em estudo. A estrutura do documento é apresentada na Figura 30.

Responsável de Segurança

O Responsável de Segurança (RS) deve ser capaz de traduzir os objetivos da entidade em requisitos de segurança de informação e, também por este motivo deve ser um bom comunicador.

As responsabilidades atribuídas ao RS são:

- Assegurar a definição, implementação e manutenção da estratégia de segurança da informação e cibersegurança de forma holística e estruturada;
- Garantir a conformidade com a legislação e regulamentação aplicável como o Regime Jurídico de Segurança do Ciberespaço e Regulamento Geral de Proteção de Dados;
- Ter conhecimento e garantir implementação de boas práticas de segurança da informação e cibersegurança, como o "Quadro Nacional de Referência para a Cibersegurança (QNRCS)" e "ISO/IEC 27001";
- Definir e identificar requisitos e medidas de segurança da informação e cibersegurança;
- Assegurar o desenvolvimento e implementação de políticas, processos e procedimentos de segurança da informação e cibersegurança;
- Definir e implementar estratégias de avaliação e de resposta aos riscos;
- Acompanhar e avaliar a execução nomeadamente dos processos de Gestão de Alterações e de Gestão de Incidentes;
- Acompanhar auditorias de segurança da informação e cibersegurança e garantir a implementação de ações de melhoria para mitigação do risco;
- Suportar a entidades na estratégia, desempenho e monitorização dos sistemas aplicacionais e infraestrutura;
- Promover ações de sensibilização/consciencialização em cibersegurança junto dos colaboradores da entidade.

O RS tem um papel fulcral na análise e na identificação de medidas adequadas para implementação na entidade. Deve acompanhar todo o processo de implementação, definição de prioridades e atividades de melhoria continua, que garantam que a entidade está preparada em termos de segurança da informação e cibersegurança. Adicionalmente, deve promover processos e procedimentos necessários para ativação do PCP.

A indicação do RS deve ser comunicada ao CNCS:

- no prazo de 20 dias úteis, a contar com o início da atividade da entidade;
- no prazo de 20 dias úteis para as entidades com atividade iniciada antes da entrada em vigor do DL, acrescido de 90 dias relativos ao prazo de produção de efeitos do artigo 4 º do mesmo (6 de dezembro de 2021);
- imediata para qualquer alteração do Ponto de Contacto Permanente da entidade.

De acordo com o CNCS, o RS pode acumular outras funções, se assim fizer sentido para a organização, inclusive a de PCP, desde que estejam asseguradas as funções de ambos.

Tal como para o PCP, a notificação do RS também tem parâmetros que devem ser respeitados. Assim, no âmbito do projeto foi criado um documento de suporte, ilustrado na Figura 30, que facilita às organizações a recolha de informação, a sua manutenção e comunicação da mesma ao CNCS. com o estabelecido foi criado o seguinte documento:

Responsável de Segurança

Nome da entidade	Nome do responsável de segurança	Cargo do responsável de segurança	Endereço de correio eletrónico	Número de telefone fixo (se aplicável)	Número de telefone móvel	Funções		Comunicação ao CNCS
						Inicio	Fim	
						dd/mm/aaaa	dd/mm/aaaa	dd/mm/aaaa

Figura 30 - Formulário de Notificação do RS,
Fonte: Elaboração Própria

Procedimento de identificação do RS e PCP

De forma a permitir que as organizações deem cumprimento à obrigação de identificação/nomeação de um PCP e de RS, ao longo da análise do requisito, foi desenvolvido um procedimento, que sofreu diversas alterações à medida que ia sendo aplicado, com o objetivo de facilitar aos OES e Administração Pública a nomeação dos perfis indicados.

Assim sendo, e em linha com o procedimento ilustrado na Figura 31, a organização deve procurar internamente se possui algum(s) recurso(s) humano(s) interno(s) com os conhecimentos, citados anteriormente, necessários para exercer as responsabilidades de PCP e RS. Caso não possua nenhum recurso com esses conhecimentos deve iniciar, junto do Departamento de Recursos Humanos, a abertura de uma ou duas vagas de contratação para recrutar um recurso com capacidade de assumir as funções. Uma vez selecionados os recursos (internamente ou através de contratação), deve-se perceber se as duas funções irão ser exercidas pelo mesmo recurso. No caso de as funções não serem exercidas pelo mesmo recurso, é necessário verificar, através dos conhecimentos, qual dos recursos melhor se adequa a cada uma das funções. Tendo identificados os recursos devem ser atribuídos as diferentes responsabilidades enumeradas e suportadas pelo documento, em anexo, “Matriz das Responsabilidades”.

Para finalizar, são preenchidos os diferentes formulários de notificação (Figura 29, Figura 30) e deve ser feita a notificação ao CNCS.

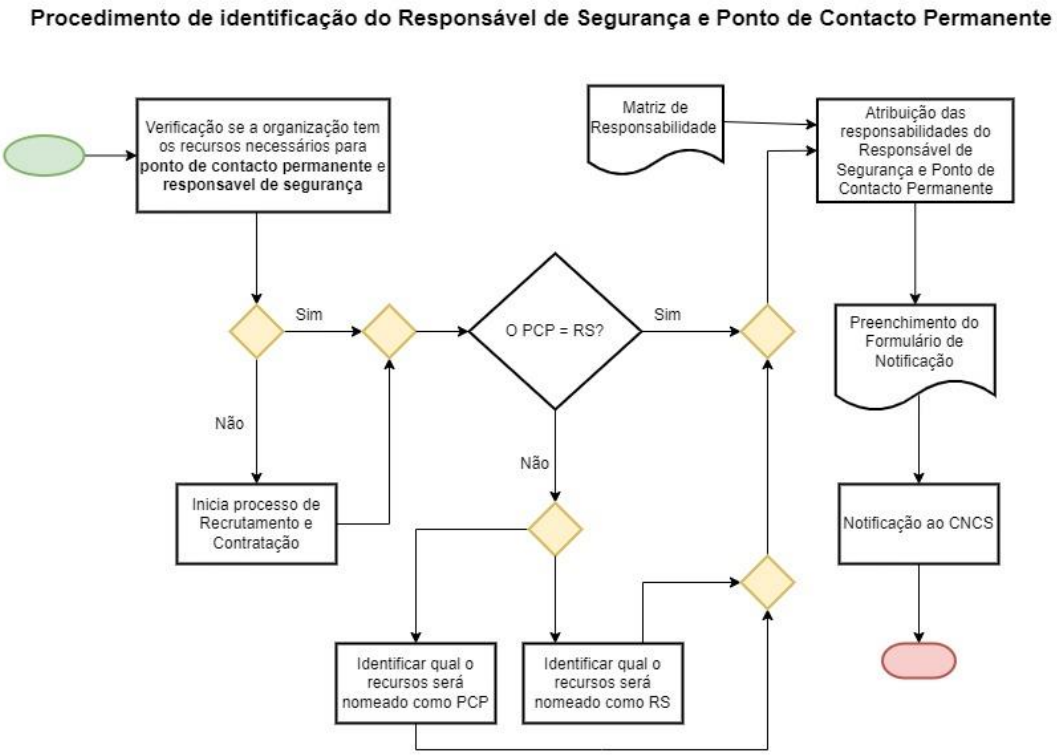


Figura 31 – Fluxograma de identificação do RS e PCP
Fonte: Elaboração Própria

A notificação ao CNCS deve ser realizada de acordo com a Instrução Técnica (República, 2021), por meios eletrónicos para o endereço de correio eletrónico, sri@cncs.gov.pt, estando de igual forma disponível o envio por método criptográfico, com recurso à chave pública de PGP (*Pretty Good Privacy*) associada ao endereço de correio eletrónico referido, publicada no sítio na Internet do CNCS.

Realizada a notificação ao CNCS, o processo de identificação e nomeação dá-se por concluído.

3.3.2.2 Inventário de todos os ativos essenciais

De acordo com o DL 658/2021todos os Ativos devem ser identificados e categorizados sob a forma de inventário. Esse inventário deve ser único, por forma a garantir a existência de um mapeamento estruturado dos Ativos, devendo, adicionalmente, existir uma classificação de cada Ativo de acordo com a sua relevância para a entidade.

Para os Ativos de tipologia “dispositivos físicos, redes e sistemas de informação” foi criado um documento, ilustrado na Figura 32.

Dispositivos Físicos, Redes e Sistemas

N.º Inventário	Nome	Modelo	N.º Série	Tipologia	Localização	Endereço IP	Endereço hardware	Responsável			Classificação
								Nome	Contacto	Departamento	

Figura 32 - Inventário de dispositivos físicos, redes e sistemas de informação
Fonte: Elaboração Própria

Para os Ativos de tipologia "aplicações e plataformas de software que suportam os processos dos serviços críticos", foi criado um documento de suporte com os campos estritamente necessários (em conformidade com as instruções). A estrutura do documento é ilustrada na Figura 33.

Aplicações e plataformas de software que suportam os processos dos serviços críticos

N.º Inventário	Nome do *software*	Versão	Fabricante	Tipologia	Classificação	Responsável			Tipo de Contrato (se aplicável)
						Nome	Contacto	Departamento	

Figura 33 - Inventário de aplicações e plataformas de software que suportam os processos dos serviços críticos
Fonte: Elaboração Própria

A classificação dos Ativos tem como objetivo garantir que todos os Ativos recebem um nível apropriado de proteção em função da sua importância para a entidade, tendo em consideração os requisitos legais, o valor, a criticidade, a sensibilidade para o manuseamento da informação criada, tratada ou armazenada pelo Ativo.

Procedimento de identificação dos Ativos Essenciais

No âmbito do projeto foi, com base nos requisitos, criado um procedimento que engloba a identificação de ativos essenciais. Assim, de acordo com o procedimento ilustrado na Figura 34, numa primeira fase, é importante verificar se a organização responde ao DL como OES ou como Administração Pública, isto porque uma vez que um OES é notificado pelo CNCS é automaticamente indicado qual o serviço prestado pela organização, o que facilita na identificação do serviço essencial. O mesmo não acontece com a Administração Pública, que não é notificada pelo CNCS para o cumprimento do DL.

Sendo que já se verificou se identificou se o procedimento será aplicado a um OES ou Administração Pública, é necessário identificar qual é o serviço crítico/essencial é prestado pela organização em análise.

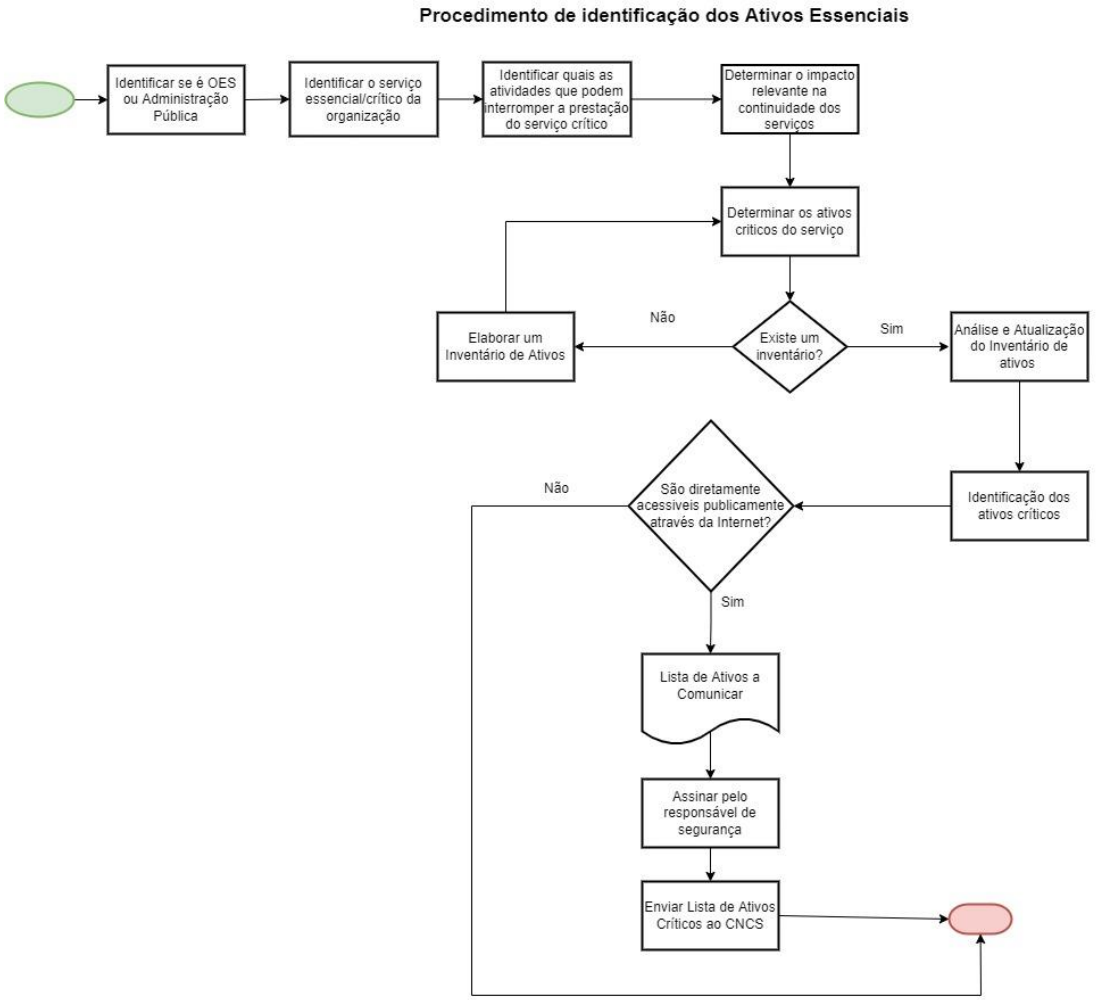
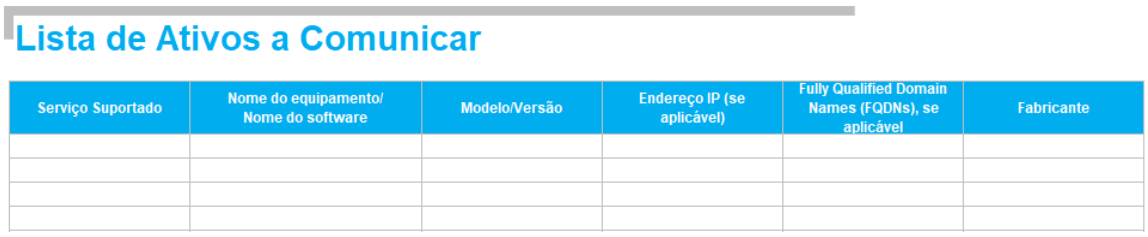


Figura 34 - Fluxograma de identificação dos ativos essenciais,
Fonte: Elaboração Própria

Tendo o serviço essencial/crítico identificado, cabe à organização perceber quais as atividades que podem interromper a prestação do serviço essencial identificado anteriormente. As atividades identificadas devem ser analisadas de acordo com o nível de impacto para a continuidade do negócio.

A partir das atividades com impacto na continuidade dos serviços identificadas, é necessário identificar os ativos críticos das mesmas. Para isso verifica-se se a organização já possui um inventário de ativos. Em caso afirmativo, existe a necessidade de analisar e posteriormente atualizar o mesmo, para que este contenha os campos indicados pelo DL. Em caso negativo, a organização deve criar um inventário de ativos, onde constem não só os ativos críticos, mas também os que suportam a organização.

Visto que a informação requerida para o cumprimento do requisito não é um inventário de ativos, mas sim os ativos críticos, a organização deve sinalizar os ativos críticos e verificar se os mesmos são diretamente acessíveis publicamente através da internet e transpô-los para a lista criada. Num documento de suporte ilustrado na Figura **35**.


Lista de Ativos a Comunicar

Serviço Suportado	Nome do equipamento/ Nome do software	Modelo/Versão	Endereço IP (se aplicável)	Fully Qualified Domain Names (FQDNs), se aplicável	Fabricante

Figura 35 - Formulário de Notificação da Lista de Ativos a comunicar,
Fonte: Elaboração Própria

A lista deve ser assinada pelo RS e posteriormente enviada ao CNCS, juntamente com o Relatório Anual. Tal como o procedimento anteriormente descrito, a notificação ao CNCS deve ser realizada de acordo com a Instrução Técnica (República, 2021). Uma vez feita a notificação, o procedimento é dado como concluído.

A lista deve ser comunicada ao CNCS na sua versão inicial, no prazo de 20 dias úteis a contar do início da atividade da entidade ou numa versão atualizada, anualmente, a ser entregue e conjunto com o relatório anual.

3.3.2.3 Análise de Riscos

Para cumprimento do DL, um dos requisitos é a análise dos riscos e implementação dos requisitos de segurança, para isso usou-se como metodologia a Gestão de Risco de Segurança da Informação descrita na Revisão da Literatura.

Estabelecer o Contexto

A fase Estabelecer o Contexto no processo de gestão de riscos aplicado às organizações foi essencial para o planeamento e implementação do mesmo, uma vez que permitiu compreender os critérios, decisões, recursos e matérias internas e externas relevantes ao propósito da organização, e que poderiam afetar a sua capacidade de alcançar os objetivos definidos.

Numa das organizações em estudo, as responsabilidades foram divididas por três órgãos de acordo com as respetivas funções. Esta divisão é apresentada na Tabela 15.

Funções	Responsável	Responsabilidades

GT - Gestão de Topo	Chefia da organização responsável pelas decisões superiores - **Comissão Executiva**	- Analisar e aprovar todas as decisões tomadas no processo de gestão dos riscos; - Delegar funções dentro da organização no que diz respeito ao processo de gestão de risco.
GR - Gestor de Risco	Responsável intermédio que gere o risco na organização de forma transversal - **Gestão de Risco Empresarial**	- Controlar processo de gestão dos riscos da organização; - Assegurar que a recolha de toda a informação necessária para a identificação do risco é realizada; - Assegurar que toda a informação necessária para a análise é recolhida; - Assegurar a realização da análise dos riscos; - Assegurar que as opções escolhidas para tratar os riscos são as mais corretas; - Assegurar que o processo de gestão dos riscos se mantém compatível com a política, objetivos e com os demais requisitos legais e regulatórios aplicáveis à organização; - Assegurar que o *framework* interno da gestão de risco é comunicada a todos os colaboradores com funções relevantes para a sua aplicação.
DR - Dono do Risco	Pessoa ou organização contratante que gere diretamente cada um dos ativos sujeitos ao processo de gestão de risco - **Diretor dos Sistemas de Informação; Responsável do *Help Desk* (telemóveis e controlo de acessos físicos, UPS e Geradores, cablagem)**	- Gerir ativos ou sistemas de informação e os seus respetivos riscos e participar no processo de gestão dos riscos; - Assegurar que o risco é reportado ao Gestor do Risco; - Assegurar que o risco é identificado, analisado, avaliado e tratado; - Assegurar que as opções de tratamento são cumpridas; - Assegurar que as atividades de controlo estão implementadas de forma a mitigar os riscos.

Tabela 15 - Funções e Responsabilidades,
Fonte: Elaboração Própria

A matriz RACI ou matriz de responsabilidades permite que os envolvidos tenham conhecimento das suas responsabilidades no ciclo de vida de um projeto ou processo. O resultado desta matriz é apresentado na Tabela 16.

Os tipos de participação RACI utilizados foram:

- **R(esponsible):** Responsável pela execução da tarefa. Parte interessada responsável, operacionalmente, pela satisfação da atividade e pela criação do resultado pretendido;
- **A(ccountable):** Responsável pelo sucesso da tarefa. Como princípio, o Accountable é único. Parte interessada responsável que poderá ter atividades operacionais na execução da tarefa. O Accountable recebe sempre informação apropriada para supervisionar a tarefa;
- **C(onsulted):** Fornece informação para a tarefa. Parte interessada que fornece informação para a execução da atividade;
- **I(nformed):** Recebe informação da tarefa. Parte interessada que é informada do cumprimento e entregas da tarefa.

Atividades	**Responsável**	**Ações**
Identificação/Revisão e caracterização dos riscos	GT	A
	DR	R
	GR	C
Identificação dos controlos existentes	DR	R / A
	GR	C
Avaliação dos riscos	GT	I
	DR	C
	GR	R
Tratamentos dos riscos avaliados	GT	C / A
	DR	R
	GR	I
Monitorização das ações de mitigação	GT	I / A
	GR	R
	DR	C
Comunicação dos riscos	GR	R
	GT	I
	DR	C
Reporte do sistema de gestão de risco	GR	R
	DR	I
	GT	I

Tabela 16 - Matriz RACI,
Fonte: Elaboração Própria

Levantamento do Risco

Como mencionado na anteriormente, o processo de levantamento de riscos é composto pelas atividades:

- identificação de riscos;
- análise de riscos;
- avaliação de riscos.

Identificação dos Riscos

Para que a identificação dos riscos fosse suficiente e adequada numa primeira instância, visto que as organizações no âmbito do estudo não apresentavam um histórico de realização de gestão de risco na segurança da informação, a abordagem foi realizada de forma metódica e organizada, a fim de garantir que todas as atividades relevantes sejam listadas e todos os riscos delas decorrentes identificados.

Os riscos identificados no decorrer desta atividade foram:

- **Resultados adversos dos avanços tecnológicos:** Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, entre outras, em resultado de avanços tecnológicos.
- **Rutura de infraestruturas de informação crítica:** Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, entre outras, resultantes da deterioração, sobrecarga ou encerramento de infraestruturas físicas e/ou digitais críticas para a organização ou de serviços dos quais esta depende de forma sistêmica, nomeadamente internet, *cloud*, antenas de comunicações, satélites.
- **Desigualdade digital:** Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, entre outras, em resultado da dificuldade, por parte da organização, de acesso a redes digitais e tecnologias críticas, por limitações no investimento, dificuldades na contratação e/ou retenção de técnicos especializados e/ou outras restrições governamentais.
- **Concentração do poder digital:** Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, entre outras, em resultado de uma elevada concentração de ativos tecnológicos e capacidades técnicas fora da organização e/ou de conhecimentos digitais críticos por um reduzido número de indivíduos na organização.
- **Falha das medidas de cibersegurança:** Risco de perturbações económicas e perdas financeiras para a organização, podendo mesmo condicionar a sua imagem ou a continuidade do negócio, decorrentes de infraestruturas e/ou medidas de segurança

cibernética na organização insuficientes, desatualizadas ou inexistentes, devido a cibercrimes cada vez mais sofisticados e frequentes.

- **Segurança da informação e privacidade:** Risco de perda de confidencialidade, integridade e disponibilidade dos sistemas de informação, decorrente de uma inexistente ou inadequada definição de políticas e medidas de segurança da informação e privacidade dos dados, podendo resultar em danos financeiros, de imagem ou de continuidade de negócio para a organização.
- **Falha da governação tecnológica:** Falta de estrutura e/ou regulamentação definida e inexistência ou falha dos canais de comunicação, para o uso de redes digitais e tecnologia, potenciando a existência de infraestruturas, protocolos, e interfaces incompatíveis, condicionando o eficiente desempenho da organização.
- **Falha na plataforma tecnológica:** Risco de incapacidade ou dificuldade na resposta às necessidades do negócio, devido a inexistência ou desalinhamento do planeamento estratégico das Tecnologias de Informação (equipamentos, infraestruturas, software), face a estratégia da organização, ou em resultado de falhas técnicas das mesmas.

Identificação dos Ativos

Para o processo de gestão de risco, a identificação dos ativos foi realizada por base no Procedimento do Inventário de todos os ativos essenciais criado no âmbito do projeto e apresentado anteriormente.

Identificação das ameaças e das vulnerabilidades

Uma vez que cada vulnerabilidade tem uma ou mais ameaças associadas que exploram o ativo através dela, as mesmas foram relacionadas. O objetivo desta associação foi facilitar a correta identificação das ameaças para cada ativo tendo em conta as vulnerabilidades que cada um deles apresenta.

A relação foi criada tendo por base as tabelas dos Anexos da ISO/IEC 27005 e o tipo de ameaças, contidas no DL, nomeadamente:

- Falha de sistema;
- Fenómeno natural;
- Erro humano;
- Ataque malicioso;
- Falha no fornecimento de bens ou serviços por terceiro.

Esta relação pode ser vista na tabela em apêndice.

Identificação dos controlos existentes

Visto que a organização se encontra em processo de implementação de normativos de segurança da informação, foram identificados documentos que possam dar, inicialmente, resposta aos riscos identificados. Entre os documentos identificados encontra-se o:

- Manual de Utilização de Sistemas de Informação;
- Procedimento de Autenticação;
- Procedimento de Acesso ao Edifício e às Instalações;
- Política de Segurança da Informação;
- Plano de Segurança;
- Plano de Manutenção;
- Plano de Segurança (Cibersegurança);
- Plano Anual de Formação;
- Plano de Atividades e Orçamento
- Procedimento Encriptação de Drives;
- Rotinas de manutenção dos AVAC registadas;
- Serviço de limpeza e manutenção das instalações;
- Política de Salvaguarda de Informação PC;
- Processo para Receção Emails Suspeitos;
- Procedimento de Controlo de Documentos e Registos;
- Recrutamento e Seleção;
- Contrato de Trabalho;
- Acordo Coletivo de Trabalho;
- IT Gestão de Desktop;
- Contratos de Aquisição e Manutenção;
- Regulamento de Atribuição e Utilização de Dispositivos Móveis;
- Manuel de Gestão do Risco Empresarial;
- Descritivos de Funções;
- Manual do Sistema de Gestão.

Os documentos acima apresentados serão analisados e adaptados tendo em conta a realidade atual das organizações para uma posterior certificação no âmbito da ISO/IEC 27001.

Análise e Avaliação do Risco

Numa primeira fase, a avaliação foi realizada globalmente baseando-se nos riscos, independentemente de estes conterem ativos, ameaças e vulnerabilidades diferentes.

Após o cálculo do valor dos riscos, e em prol da melhoria contínua, a análise deverá ser detalhada por tipo de ativo, ameaças e vulnerabilidades, a fim de permitir uma avaliação com maior rigor no

que diz respeito aos seus planos de ação. A análise de avaliação de risco é feita num documento de suporte criado para o efeito. Este documento, ilustrado na Figura 36, permite registar as diferentes fases da gestão de risco, estando destacado a atividade de identificação do risco e a análise do risco. A análise do risco foi realizada tendo por base o tipo de impacto que cada um dos riscos pode provocar na organização. No que diz respeito ao cálculo do nível de risco atual, este foi calculado tendo em conta a multiplicação dos valores atribuídos ao impacto e a probabilidade de um determinado risco ocorrer.

Identificação do Risco					Análise do Risco				
ID do Risco	Registado por:	Nome do Risco	Descrição do Risco	Controlos Implementados	Tipo de impacto	Impacto	Probabilidade	Nível de Risco Atual (Inerente)	
								Quantitativa	Qualitativa
1	Gestor de Risco	Resultados adversos dos avanços tecnológicos	Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, etc., em resultado de avanços tecnológicos.	- Manual de Utilização de Sistemas de Informação - Procedimento de Autenticação; - Procedimento de Acesso ao Edifício e às Instalações;	Perdas de produtividade	4	2	8	Médio
2	Gestor de Risco	Rutura de infraestruturas de informação crítica	Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, etc., resultantes da deterioração, sobrecarga ou encerramento de infraestruturas físicas e/ou digitais críticas para a organização ou de serviços dos quais esta depende de forma sistémica, nomeadamente internet, cloud, antenas de comunicações, satélites; etc.	- Política de Segurança da Informação - Plano Anual de Formação	Perdas de produtividade	3	3	9	Médio
3	Gestor de Risco	Desigualdade digital	Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, etc., em resultado da dificuldade, por parte da organização, de acesso a redes digitais e tecnologias críticas, por limitações no investimento, dificuldades na contratação e/ou retenção de técnicos especializados e/ou outras restrições governamentais.	- Política de Segurança da Informação - Plano Anual de Formação - Plano de Segurança (Cibersegurança) - Processo para Receção Emails Suspeitos	Perdas de produtividade	4	3	12	Alto
4	Gestor de Risco	Concentração do poder digital	Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, etc., em resultado de uma elevada concentração de ativos tecnológicos e capacidades técnicas fora da organização e/ou de conhecimentos digitais críticos por um reduzido número de indivíduos na organização.	- Manual de Utilização de Sistemas de Informação - Política de Segurança da Informação - Procedimento de Autenticação;	Perdas de produtividade	4	3	12	Alto
5	Gestor de Risco	Falha das medidas de ciber segurança	Risco de perturbações económicas e perdas financeiras para a organização, podendo mesmo condicionar a sua imagem ou a continuidade do negócio, decorrentes de infraestruturas e/ou medidas de segurança cibernética na organização insuficientes, desatualizadas ou inexistentes, devido a cibercrimes cada vez mais sofisticados e frequentes.	- Política de Segurança da Informação - Plano Anual de Formação	Perdas de produtividade	3	3	9	Médio
6	Gestor de Risco	Segurança da informação e privacidade	Risco de perda de confidencialidade, integridade e disponibilidade dos sistemas de informação, decorrente de uma inexistente ou inadequada definição de políticas e medidas de segurança da informação e privacidade dos dados, podendo resultar em danos financeiros, de imagem ou de continuidade de negócio para a organização.		Perdas de produtividade	3	3	9	Médio
7	Gestor de Risco	Falha da governação tecnológica	Falta de estrutura e/ou regulamentação definida e inexistência ou falha dos canais de comunicação, para o uso de redes digitais e tecnologia, potenciando a existência de infraestruturas, protocolos, e interfaces incompatíveis, condicionando o eficiente desempenho da organização.	- Política de Segurança da Informação - Plano Anual de Formação - Plano de Segurança (Cibersegurança) - Processo para Receção Emails Suspeitos	Perdas de produtividade	3	2	6	Médio
8	Gestor de Risco	Falha na plataforma tecnológica	Risco de incapacidade ou dificuldade na resposta às necessidades do negócio, devido a inexistência ou desalinhamento do planeamento estratégico das Tecnologias de Informação (equipamentos, infraestruturas, software), face a estratégia da organização, ou em resultado de falhas técnicas das mesmas.	- Política de Segurança da Informação - Plano de Segurança (Cibersegurança)	Perdas de produtividade	3	3	9	Médio

Figura 36 - Análise e Avaliação do Risco,
Fonte: Elaboração Própria

Tratamento do Risco

Na realização do tratamento, dado a definição do tipo de tratamento de "Reduzir, implementou-se essa opção para todos os riscos que necessitam de tratamento, de modo a diminuir o valor do risco residual. Tendo por base as boas práticas da cibersegurança, uma avaliação de conformidade com os controlos do QNRCS e da ISO/IEC 27001, foram identificadas as seguintes linhas de ação:

- Ações periódicas de atualização de sistemas aplicacionais e infraestrutura;
- Acompanhamento regular das evoluções tecnológicas disponível no mercado;
- Criação de SOC (*Security Operations Center*);
- Realização regular de testes de vulnerabilidades e intrusão;
- Garantir sistemas de alta disponibilidade;
- Garantir o bom funcionamento do site *disaster recovery* com testes periódicos;
- Criação de um plano de continuidade de negócio;
- Garantir a existência de equipamentos de reserva;

- Planos de formação;
- Aprovação dos Planos de Atividade e Orçamento;
- Política de contratação;
- Revisão periódica de políticas e procedimentos, com base na metodologia ITIL (*Information Tecnology Infraestructure Library*);
- Implementação da certificação ISO 27001;
- Revisão regular da Política de Segurança da Informação.

Com a implementação das medidas acima identificadas espera-se uma redução dos níveis de risco. A redução esperada é apresentada na Figura 37.

Identificação do Risco **Tratamento do Risco**

ID do Risco	Registado por:	Nome do Risco	Descrição do Risco	Tratamento	Plano de ação	Risco Residual	
						Quantitativa	Qualitativa
1	Gestor de Risco	Resultados adversos dos avanços tecnológicos	Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, etc., em resultado de avanços tecnológicos.	Reduzir	- Ações periodicas de atualização de sistemas aplicacionais e infraestrutura; - Acompanhamento regular das evoluções tecnológicas disponíveis no mercado.	3	Baixo
2	Gestor de Risco	Ruptura de infraestruturas de informação crítica	Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, etc., resultantes da deterioração, sobrecarga ou encerramento de infraestruturas físicas e/ou digitais críticas para a organização ou de serviços dos quais esta depende de forma sistémica, nomeadamente internet, cloud, antenas de comunicações, satélites, etc.	Reduzir	- Garantir sistemas de alta disponibilidade; - Garantir o bom funcionamento do site disaster recovery com testes periódicos; - Criação de plano de continuidade de negócio; - Garantir existência de equipamentos de reserva.	4	Baixo
3	Gestor de Risco	Desigualdade digital	Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, etc., em resultado da dificuldade, por parte da organização, de acesso a redes digitais e tecnologias críticas, por limitações no investimento, dificuldades na contratação e/ou retenção de técnicos especializados e/ou outras restrições governamentais.	Reduzir	- Planos de formação; - Aprovação dos PAO; - Política de contratação	6	Médio
4	Gestor de Risco	Concentração do poder digital	Consequências adversas para a organização, a nível estratégico, de imagem, de negócio, de segurança da informação, etc., em resultado de uma elevada concentração de ativos tecnológicos e capacidades técnicas fora da organização e/ou de conhecimentos digitais críticos por um reduzido número de indivíduos na organização.	Reduzir	- Planos de formação; - Aprovação dos PAO; - Política de contratação	6	Médio
5	Gestor de Risco	Falha das medidas de ciber segurança	Risco de perturbações económicas e perdas financeiras para a organização, podendo mesmo condicionar a sua imagem ou a continuidade do negócio, decorrentes de infraestruturas e/ou medidas de segurança cibernética na organização insuficientes, desatualizadas ou inexistentes, devido a cibercrimes cada vez mais sofisticados e frequentes.	Reduzir	- Criação de SOC; - Realização regular de testes de vulnerabilidade e intrusão.	4	Baixo
6	Gestor de Risco	Segurança da informação e privacidade	Risco de perda de confidencialidade, integridade e disponibilidade dos sistemas de informação, decorrente de uma inexistente ou inadequada definição de políticas e medidas de segurança da informação e privacidade dos dados, podendo resultar em danos financeiros, de imagem ou de continuidade de negócio para a organização.	Reduzir	- Revisão regular da Política da Segurança de Informação; - Implementação da certificação ISO 27001.	4	Baixo
7	Gestor de Risco	Falha da governação tecnológica	Falta de estrutura e/ou regulamentação definida e inexistência ou falha dos canais de comunicação, para o uso de redes digitais e tecnologia, potenciando a existência de infraestruturas, protocolos, e interfaces incompatíveis, condicionando o eficiente desempenho da organização.	Reduzir	- Revisão periódica de políticas e procedimentos, com base na metodologia ITIL; - Implementação da certificação ISO 27001.	4	Baixo
8	Gestor de Risco	Falha na plataforma tecnológica	Risco de incapacidade ou dificuldade na resposta às necessidades do negócio, devido a inexistência ou desalinhamento do planeamento estratégico das Tecnologias de Informação (equipamentos, infraestruturas, software), face a estratégia da organização, ou em resultado de falhas técnicas das mesmas.	Reduzir	- Revisão regular da Política da Segurança de Informação; - Criação de plano de continuidade de negócio.	4	Baixo

Figura 37 - Tratamento do risco,
Fonte: Elaboração Própria

3.3.2.4 Plano de Segurança

O Plano de segurança é um documento estruturado que deve descrever como uma entidade aborda todas as suas necessidades de segurança de informação e cibersegurança. Trata-se de um documento dinâmico e que acompanha a evolução da própria entidade, pelo que precisa de revisto e melhorado, de forma periódica. A alteração do Plano de segurança depende essencialmente das necessidades da entidade, das suas necessidades de segurança e dos resultados da gestão de risco. O Plano de segurança dever ser assinado pelo RS. O Plano de segurança é interno à organização, pelo que não necessita de ser comunicado ao CNCS.

<u>Procedimento de criação de um Plano de Segurança</u>

Para dar cumprimento ao requisito do DL, foi construído um fluxograma, ilustrado na Figura 38, com os diferentes processos a serem seguidos.

A necessidade da criação de um Plano de segurança inicia com a verificação, por parte da organização, da existência de um Política de Segurança. Caso o documento ainda não tenha sido criado, a organização deve proceder à criação do mesmo, caso contrário o documento deve ser revisto e verificar se este se encontra em *compliance* para o mesmo estar adequado à realidade da organização.

É de notar que a Política de Segurança é uma declaração de alto nível de propósito e de intenção de uma entidade em relação à segurança da informação. As políticas devem incluir as linhas orientadoras para uma intenção específica para todas as pessoas, em todos os níveis da entidade. A Política de Segurança da Informação deve ser enquadrada ao nível estratégico da entidade, por forma a garantir o envolvimento e compromisso da gestão de topo, suportando assim a tomada de decisão no respeita às prioridades no âmbito da Segurança da Informação e garantindo os seguintes objetivos:

- Definir a estratégia de Segurança da Informação, alinhada com o Modelo Organizacional da mesma;
- Fomentar uma cultura de segurança para toda entidade;
- Sensibilizar os utilizadores para a importância da Segurança da Informação e para a literacia deste âmbito;
- Promover a Segurança da Informação como um propósito indispensável a alcançar.

Deve, ainda, constar na Política de Segurança da Informação:

- As conformidades legais (nacionais e europeias) aplicáveis à normal operação da entidade;
- As garantias de proteção de propriedade intelectual que necessitam de ser observados e seguidos.

Uma vez terminada a Política de Segurança, surge a necessidade de verificar a existência de documentação com as medidas organizativas, medidas essas necessárias para salvaguardar os ativos físicos e virtuais, bem como a informação de suporte ao negócio ou à atividade, e os dados pessoais. Medidas essas que abranjam áreas importantes como Gestão de Incidentes, Continuidade de Negócio ou Gestão de Recursos Humanos, de forma a garantir que na ocorrência de algum evento disruptivo a entidade está capacitada para dar uma resposta suficiente para salvaguardar a informação e a operação, através de uma abordagem consistente e eficaz.

No caso de as medidas estarem definidas as mesmas devem ser revistas e analisadas se estão em *compliance* com os objetivos da organização, caso contrário deve elaborá-las tendo em conta a descrição de um plano da continuidade do negócio que:

- Defina o propósito, âmbito, papéis, responsabilidades, comprometimento da gestão de topo e coordenação com partes interessadas externas;
- Identifique as funções essenciais ao bom funcionamento da entidade e requisitos de contingência das mesmas;
- Defina prioridades de recuperação, objetivos e métricas;
- Enderece a recuperação total das funções essenciais.

Visto que as medidas estão definidas é necessário realizar o mesmo processo, mas desta vez para a formação de recursos humanos. Neste, devem ser estabelecidos planos de ações de formação em segurança da informação e cibersegurança, bem como definidos os processos e procedimentos necessários para garantir a sua correta implementação. A organização deve criar, disseminar e atualizar:

- Um plano de ações de formação;
- Ações de formação em segurança da informação às partes interessadas relevantes;
- Processos e procedimentos formais que simplifiquem a implementação das ações;
- Medir o sucesso das ações de formação realizadas através de entrevistas aos formandos das mesmas.

O Plano de segurança deve conter ainda a descrição de todas as medidas adotados em matéria de requisitos de segurança e notificação de incidentes. Neste processo é necessário verificar se todas as medidas estão descritas e em *compliance*. Se não estiverem descritas ou em *compliance* é necessário criá-las, com base:

- Num plano de resposta e de recuperação de incidentes que:
    - Contenha um plano de implementação para a capacidade de resposta a incidentes;
    - Descreva a estrutura e organização da resposta inicial;
    - Defina o que são incidentes;
    - Defina os recursos necessários para suportar a resposta a incidentes;
    - Defina os procedimentos de resposta a perdas de informação.
- Disseminar os planos de resposta e recuperação pelas partes relevantes;
- Rever regularmente os planos da continuidade do negócio;
- Efetuar a categorização da posição em termos de funções, âmbito, responsabilidades e risco;
- Executar a triagem na contratação, com base no risco percecionado para a posição;
- Executar a triagem com base no risco percecionado para a posição, de forma regular;

- Implementar processos de atribuição de acessos físicos e lógicos às redes e sistemas de informação e instalações, por exemplo: Gestão de Identidades.
- Em caso de transferência:
    - Efetuar a revisão de acessos físicos e lógicos às redes e sistemas de informação e instalações;
    - Efetuar a confirmação das necessidades operacionais para continuidade dos acessos;
    - Efetuar a atualização de acessos com base nas novas funções.
- Em caso de cessação contratual:
    - Efetuar o cancelamento de acessos às redes e sistemas de informação do ex-colaborador;
    - Recolher todos os ativos relevantes na posse do ex-colaborador;
    - Em caso de não cumprimento das políticas de segurança da informação instituídas, deve acionar o processo de ação disciplinar.

Estando todas as medidas anteriormente mencionadas, definidas, é importante verificar se o PCP e o RS estão definidos e nomeados, caso contrário deve ser seguido o procedimento de designação de PCP e RS.

Realizada a nomeação, a organização já se encontra em condições de criar o Plano de segurança e o RS assinará o mesmo. No apêndice é possível visualizar um exemplo de um Plano de Segurança desenvolvido numa primeira instância para dar cumprimento ao prazo legal (6 de dezembro 2021).

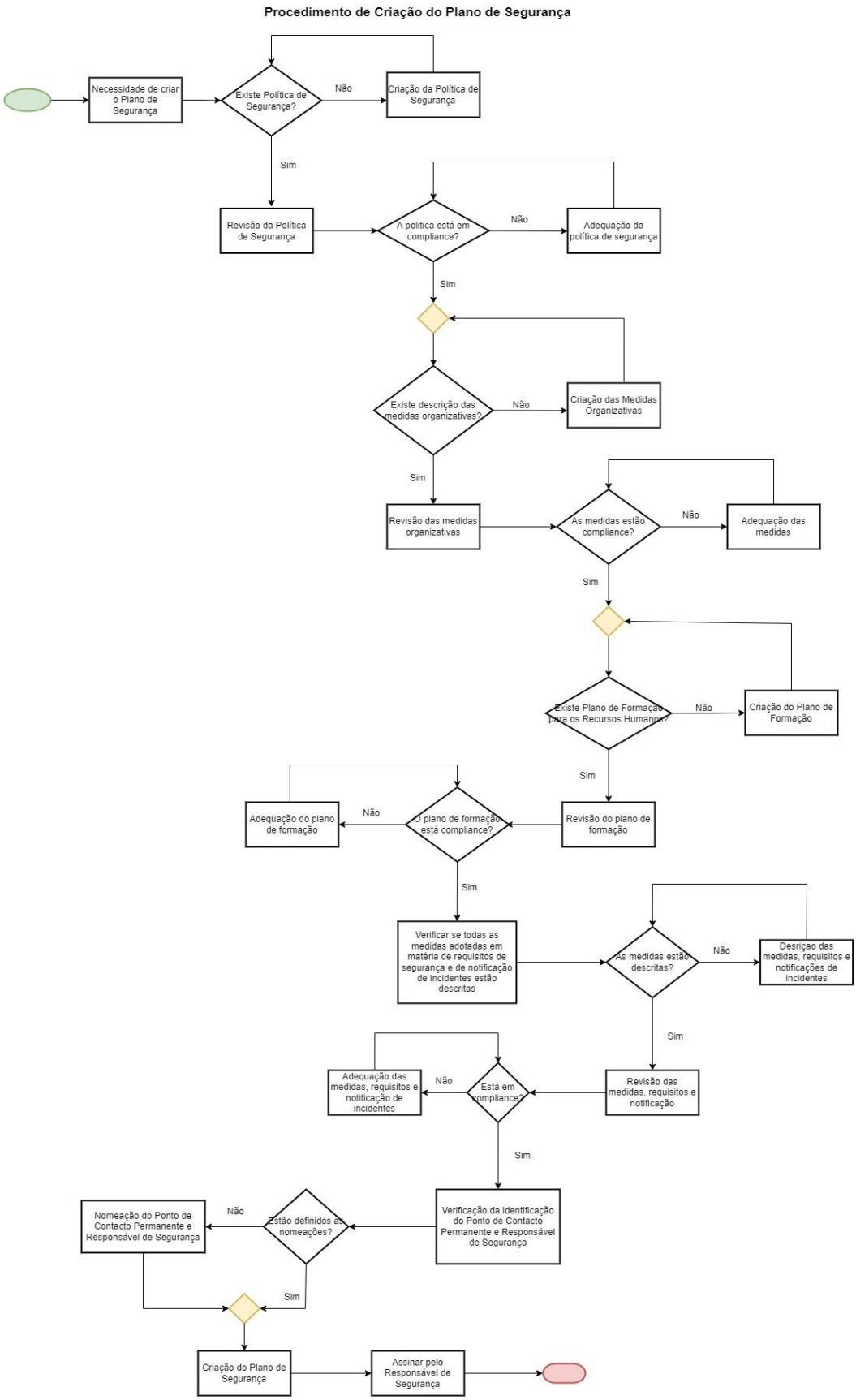


Figura 38 - Fluxograma de Criação de um Plano de Segurança,
Fonte: Elaboração Própria

3.3.2.5 Relatório Anual

É fundamental a realização de avaliações periódicas nas entidades sobre as medidas implementadas, atividades desenvolvidas e problemas encontrados relacionados com a cibersegurança.

Essas avaliações podem ser realizadas sobe a forma de relatórios que descrevem de forma sumária as principais atividades desenvolvidas em matéria de segurança das redes e dos sistemas de informação. Os relatórios também devem incluir informação sobre:

- Estatística trimestral de todos os incidentes, com indicação do número e do tipo dos incidentes;
- Análise agregada dos incidentes de segurança com impacto relevante ou substancial, com informação sobre:
    - Número de utilizadores afetados pela perturbação do serviço;
    - Duração dos incidentes;
    - Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
- Recomendações de atividades, de medidas ou de práticas que promovam a melhoria da segurança das redes e dos sistemas de informação;
- Problemas identificados e medidas implementadas na sequência dos incidentes;
- Qualquer outra informação relevante.

O primeiro relatório anual deveria de ser entregue até 31 de janeiro de 2022, e os subsequentes anuais, até ao último dia útil do mês de janeiro do ano civil seguinte aos quais os mesmos se reportam.

Procedimento de criação de um Relatório Anual

Para a realização do Relatório Anual, as organizações devem verificar se possuem processos implementados internamente que auxiliem na deteção e registo de incidentes, de forma ajudar na recolha das estatísticas trimestrais. No caso de não possuírem esses processos, é aconselhável a sua implementação, permitindo um maior controlo sobre os incidentes de cibersegurança que possam a estar a ocorrer sem ser detetados levando a consequências mais nefastas para a organização.

Uma vez recolhidas as estatísticas trimestrais, existe a necessidade de verificar se a organização em estudo sofreu algum acidente de segurança com impacto relevante ou substancial[8]. Caso a organização tenha sido alvo de um incidente de segurança, deverá realizar uma análise agregada

[8] Para a determinação do impacto de um incidente, utiliza-se as diretrizes constantes na Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016, e sua transposição nacional através da Lei n.º 46/2018, de 13 de agosto

dos incidentes de segurança com a informação descrita acima onde se inclui a análise e resposta ao incidente realizada durante o processo de gestão de incidentes. No caso de a organização não ter sido alvo de um incidente, a organização apenas deve informar que não existem incidentes a reportar no período.

Uma vez tratada a questão dos incidentes, a organização deve recolher as atividades executadas no âmbito da melhoria da segurança de redes (SR) e sistemas de informação (SI) e verificar se o plano de segurança contém medidas adotadas para a melhoria da SR e SI. Estas medidas devem ser compiladas e incluídas no Relatório Anual.

Tendo em conta a informação recolhida, a organização já se encontra em condições de elaborar o relatório anual, para que este seja assinado pelo RS e prontamente enviado ao CNCS, juntamente com a lista de ativos a comunicar. Enviado o relatório o processo do cumprimento do requisito fica terminado.

Em apêndice é possível observar um exemplo de um relatório anual criado para uma das organizações em estudo, desenvolvido com base no fluxograma da Figura **39**.

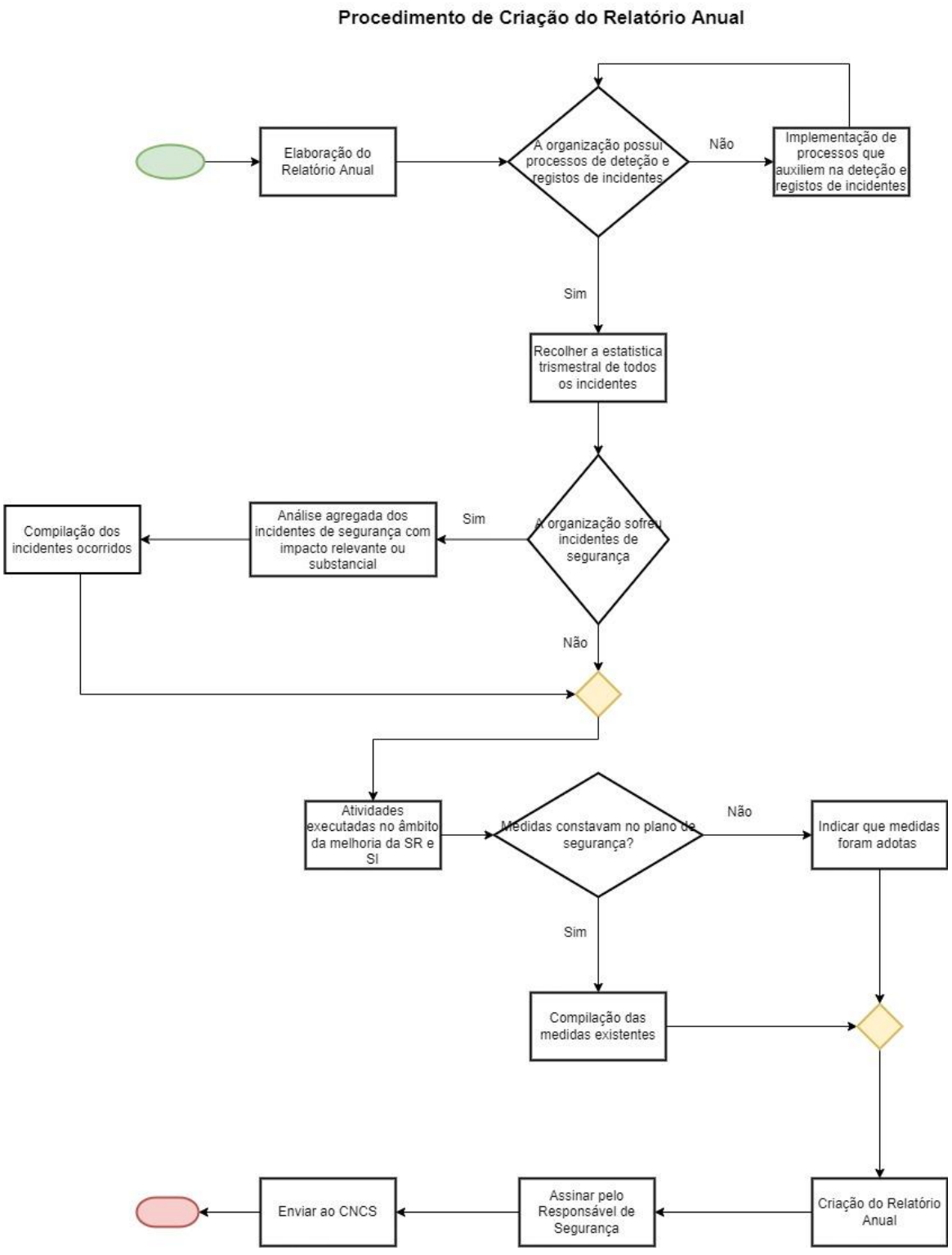


Figura 39 - Fluxograma do Relatório Anual,
Fonte: Elaboração Própria

3.3.2.6 Notificação de incidentes

A gestão de incidentes constitui um ponto fulcral para a cibersegurança das entidades, garantindo a implementação de práticas de segurança através da definição de uma abordagem consistente e eficaz de gestão de incidentes de cibersegurança.

Para minimizar os danos e impactos causados pelos diferentes tipos de incidente[9] de cibersegurança, é necessário identificar, conter, responder e analisar os mesmos. Neste sentido, toda a documentação e controlos implementados relativamente à gestão de incidentes de cibersegurança baseia-se no procedimento esquematizado na Figura 41.

De acordo com o DL, a Administração Pública e os OES devem, perante qualquer incidente detetado ou a estes comunicados pelos seus clientes, utilizadores ou outras entidades, atender aos parâmetros previstos, no RJSC, bem como aos constantes dos normativos complementares setoriais aplicáveis, para classificar os incidentes como tendo impacto relevante ou substancial.

As entidades devem implementar todos os meios e os procedimentos necessários à deteção, à avaliação do impacto e à notificação de incidentes com impacto relevante ou substancial. A fim de determinar a relevância do impacto de um incidente são tidos em conta os seguintes parâmetros:

- O número de utilizadores afetados;
- A duração do incidente;
- A distribuição geográfica, no que se refere à zona afetada pelo incidente.

De acordo com RJSC os parâmetros previstos para a notificação de incidentes para Administração Pública e OES são:

- **Notificação Inicial -** Deve ser enviada logo que a entidade possa concluir que existe ou possa vir a existir impacto relevante ou substancial e até duas horas após essa verificação;
- **Notificação Fim de Impacto -** Deve ser submetida ao CNCS logo que possível, dentro do prazo máximo de duas horas após a perda de impacto relevante ou substancial;
- **Notificação Final -** Deve ser enviada no prazo de 30 dias úteis a contar do momento em que o incidente deixou de se verificar;
- Nos casos em que o incidente seja resolvido de forma imediata, nas primeiras duas horas após a sua deteção, as entidades podem enviar diretamente a notificação final.

Procedimento de Gestão de Incidentes de Segurança

[9] Um evento com um efeito adverso real na segurança das redes e dos sistemas de informação(Assembleia da República, 2018)

O procedimento de Gestão de Incidentes, representado na Figura 40, inicia quando se deteta um evento de segurança, as áreas envolvidas no processo de resposta a incidentes devem identificar as ações necessárias para iniciar as atividades de triagem e o tratamento do incidente. É importante destacar que a deteção de incidentes pode ocorrer tanto pela equipa de CSIRT (*Computer Security Incident Response Team*), através da deteção de eventos suspeitos pela sua monitorização, quanto por colaboradores, fornecedores ou clientes impactados pelo evento.

Após o processo de deteção a equipa de CSIRT deve realizar a triagem dos eventos efetuando a análise, correlacionando com todas as informações disponíveis nas ferramentas de segurança e caso o resultado da análise seja positivo, deverá classificar, categorizar e registar o incidente. Todos os detalhes do incidente devem ser analisados.

No caso de o incidente decorrer num OES e/ou Administração Pública com um impacto relevante ou substancial, a organização deve realizar a notificação inicial até duas horas após essa verificação, devendo a entidade, sem prejuízo do cumprimento deste prazo, dar prioridade à mitigação e à resolução do incidente. A notificação inicial deve incluir a seguinte informação:

- Ponto de Contacto Permanente;
- Data e hora do início ou, em caso de impossibilidade de o determinar, da deteção do incidente;
- Breve descrição do incidente, incluindo a indicação da categoria da causa raiz e dos efeitos produzidos, de acordo com a taxonomia em anexo e, sempre que possível, o respetivo detalhe;
- Estimativa possível do impacto, considerando:
    - Número de utilizadores afetados pela perturbação do serviço;
    - Duração do incidente;
    - Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço.

Caso o não exista a necessidade de notificar, o CSIRT deve comunicar o incidente a todas as equipas envolvidas no processo, de modo a mitigar e responder ao mesmo. Para responder ao incidente, devem existir procedimentos para o tratamento (*Playbooks*). Estes documentos devem ser elaborados de acordo com as melhores práticas, sendo responsabilidade da equipa encarregada pelo tratamento dos eventos estabelecer e manter atualizados os procedimentos de resposta. O processo de tratamento deve ser definido para que medidas de mitigação, contorno e/ou resolução definitiva sejam estabelecidas.

Para os casos de incidentes que não tenham procedimentos de tratamento previamente definidos ou que a documentação existente se mostre ineficiente insuficiente/desadequada para resolução do caso, a área responsável deve providenciar a elaboração ou atualização do material. Após o

resultado da análise, é definido um plano de resposta. Este plano indicará como conter e erradicar a ameaça, como monitorar a ameaça (para poder verificar se a ameaça foi erradicada) e como coordenar as partes envolvidas para a resolução do incidente. O plano de resposta também deve definir as ações de recuperação a ser tomadas quando a ameaça for corrigida.

Uma vez realizado o processo de resposta ao incidente, existe a necessidade de verificar se o mesmo foi solucionado para assim comunicar às equipas envolvidas, caso contrário deve repetir-se o processo de análise do incidente.

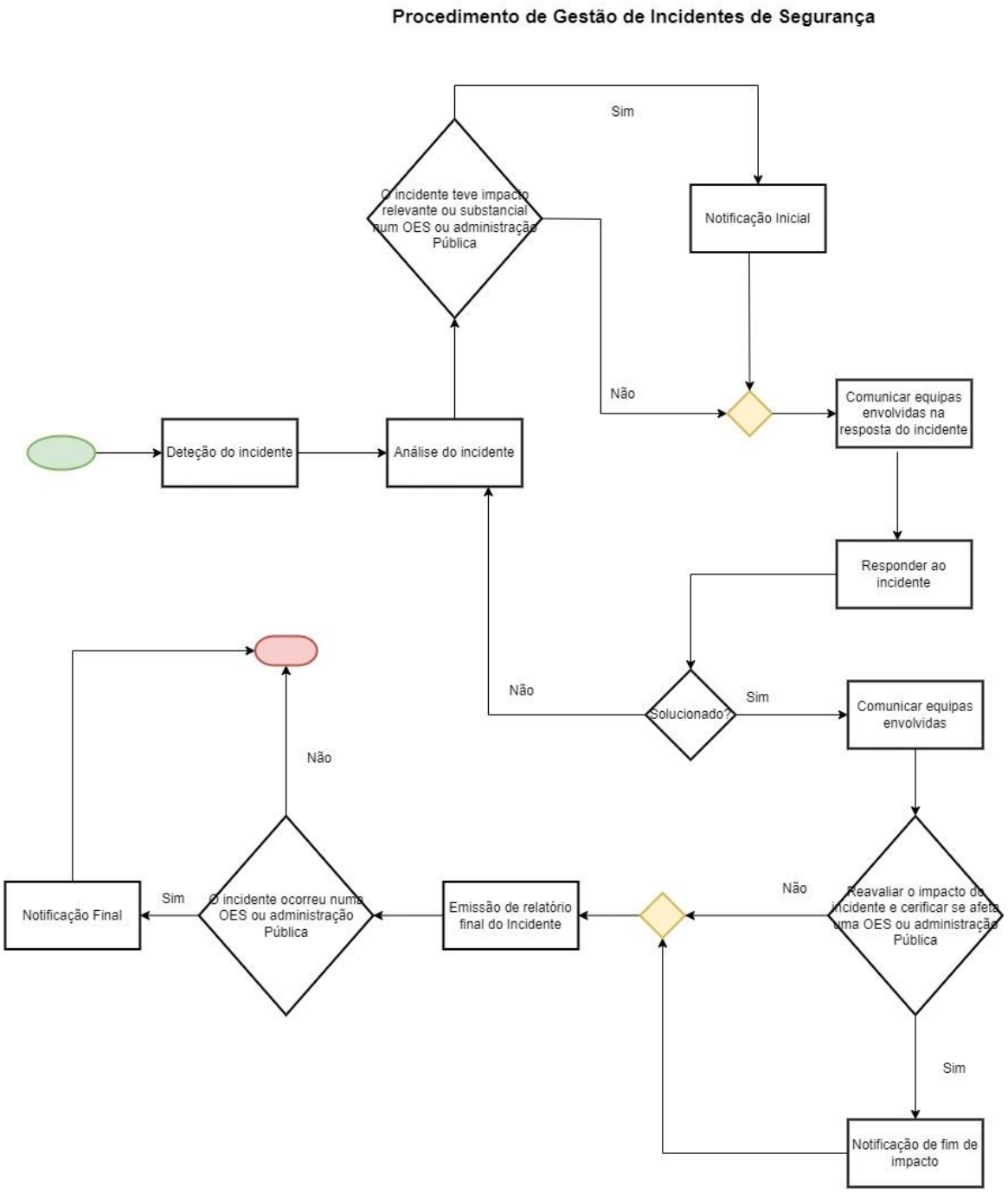


Figura 40 - Fluxograma de Gestão de Incidentes,
Fonte: Elaboração Própria

O incidente deve ser reavaliado ao nível do impacto e certificar se afeta uma OES ou Administração Pública, para assim realizar a Notificação de fim de impacto que deve ser submetida ao CNCS logo que possível e dentro do prazo máximo de duas horas após a perda de impacto relevante ou substancial. A notificação de fim de impacto relevante ou substancial deve incluir a seguinte informação:

- Atualização da informação transmitida na notificação inicial, caso exista;

- Breve descrição das medidas adotadas para a resolução do incidente;
- Descrição da situação do impacto existente no momento da perda de impacto relevante ou substancial, nomeadamente:
    - Número de utilizadores afetados pela perturbação do serviço;
    - Duração do incidente;
    - Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
    - Tempo estimado para a recuperação total dos serviços.

Uma vez notificado ou se o incidente não afetar nenhuma administração pública ou OES, deve ser apresentado, quando aplicável, as recomendações de melhorias para os controlos de segurança existentes e para os procedimentos de monitorização. Quando possível a equipa responsável pela resolução do incidente deve elaborar um relatório de resposta ao incidente, tendo em conta:

- Descrição detalhada do incidente e evidências do mesmo.
- Mecanismos de resposta utilizados;
- Atividades de recuperação utilizadas para restaurar os ambientes / sistemas afetados;
- Lista de lições aprendidas com o incidente e quais iniciativas que a organização pode tomar para mitigar e, possivelmente, eliminar a probabilidade de futuros incidentes.

Se não se tratar de um incidente num OES ou administração Pública o procedimento termina, caso contrário deverá decorrer a Notificação final que deve ser enviada no prazo de 30 dias úteis a contar do momento em que o incidente deixou de se verificar e deve incluir a seguinte informação:

- Data e hora em que o incidente assumiu o impacto relevante ou substancial;
- Data e hora em que o incidente perdeu o impacto relevante ou substancial;
- Impacto do incidente, considerando:
    - Número de utilizadores afetados pela perturbação do serviço;
    - Duração do incidente;
    - Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
    - Descrição do incidente, com indicação da categoria da causa raiz e dos efeitos produzidos, de acordo com a taxonomia definida no artigo 16.º, e o respetivo detalhe.
- Indicação das medidas adotadas para mitigar o incidente;
- Descrição da situação residual do impacto existente à data da notificação final, nomeadamente:
    - Número de utilizadores afetados pela perturbação do serviço;

    - Distribuição geográfica, no que se refere à zona afetada pelo incidente, incluindo a indicação de impacto transfronteiriço;
    - Tempo estimado para a recuperação total dos serviços ainda afetados.
- Indicação, sempre que aplicável, da apresentação de notificação do incidente em causa às autoridades competentes, nomeadamente ao Ministério Público, à ANEPC, à ANACOM, à CNPD e a outras autoridades setoriais, nos termos previstos nas disposições legais e regulamentares aplicáveis;
- Outra informação que a entidade considere relevante.

O envio das notificações de incidentes e de informação adicional, deve ser realizado através do sítio na Internet do CNCS na funcionalidade «Notificação de Incidentes»[10], Figura **41**, mediante o preenchimento do modelo de reporte estabelecido para o efeito, ou via API disponibilizada.

[10] https://www.cncs.gov.pt/pt/notificacao-incidentes/

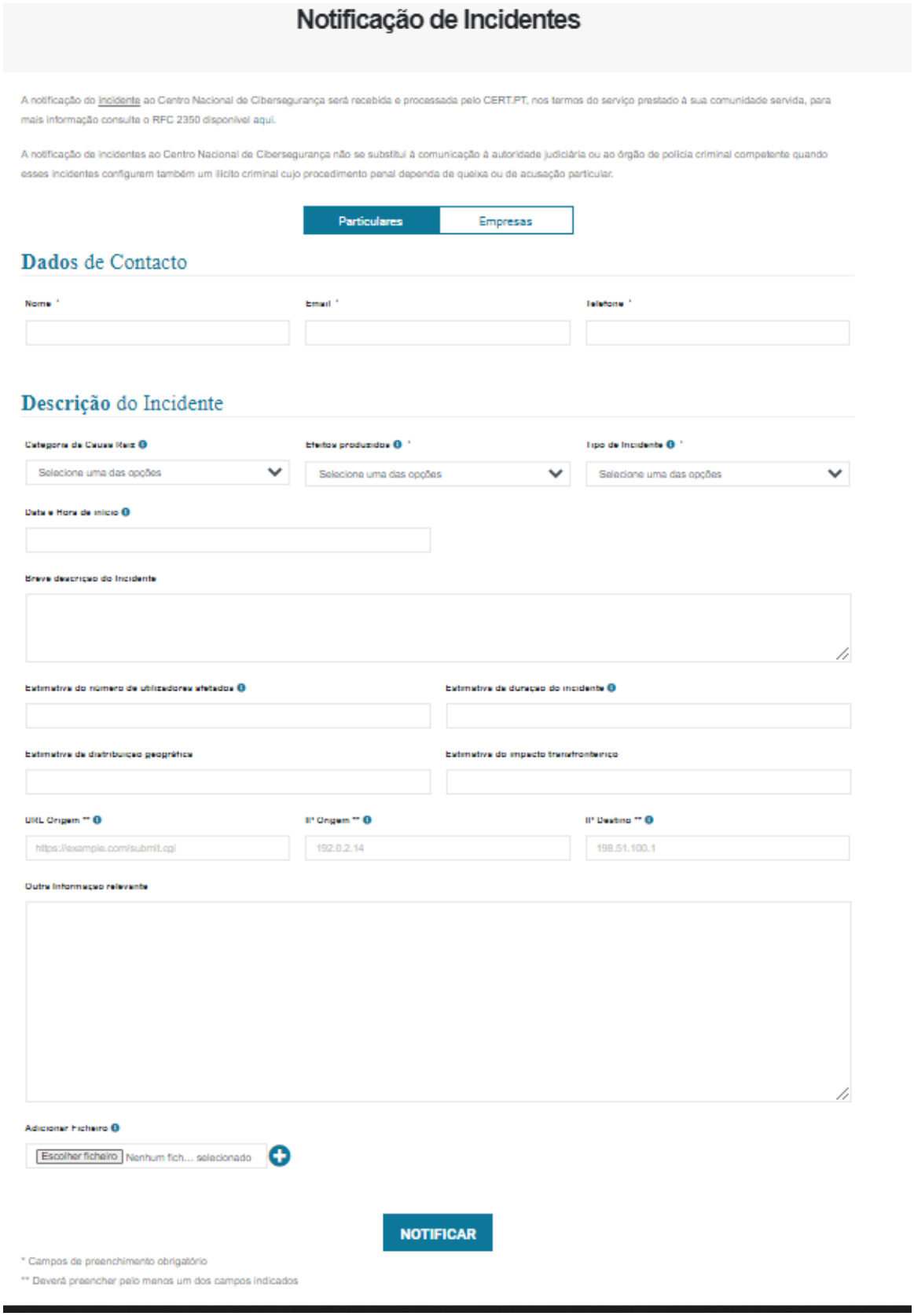


Figura 41 - Notificação de Incidentes,
Fonte: Elaboração Própria

Por fim far-se-á uma conclusão deste trabalho tentando demonstrar o cumprimento dos objetivos e os resultados do projeto.

4. Análise final e discussão dos resultados

O capítulo que se segue centra-se na análise e discussão dos resultados obtidos.

Ao longo da aplicação da metodologia, cuja última reunião com ambas organizações foi realizada no dia 8 de agosto de 2022, foram identificados 13 riscos representados na Tabela 17:

ID do Risco	Descrição do Risco
1	Falta de comprometimento dos recursos da empresa no Projeto
2	Falta de comprometimento das organizações (cliente)
3	Falta de liderança de gestão
4	Os recursos da empresa não são qualificados para a função
5	Divergência entre a data de início oficial e a data de início efetiva
6	Atrasos na execução financeira por parte das organizações
7	Não cumprimento das cláusulas dos contratos
8	Saída de recursos humanos chaves durante o seu ciclo de vida
9	Atraso nas atividades e respetiva calendarização
10	Não cumprimento dos entregáveis do Projeto
11	Falta de comunicação entre as diferentes partes interessadas
12	Alteração/ Atualização das diretrizes do CNCS ou das respetivas autoridades setoriais
13	Alteração/Atualização da legislação setorial

Tabela 17 - Registo dos riscos
Fonte: Elaboração Própria

Os riscos identificados foram qualificados na sua grande maioria como sendo de moderado e alto impacto, o que significa que a maioria dos riscos identificados pode prejudicar o sucesso e o cumprimento dos objetivos inicialmente propostos.

A Tabela 18 identifica a qualificação dos riscos obtida, através dos cálculos de probabilidade e severidade.

	Impacto				
Probabilidade	0.05	0.1	0.2	0.4	0.8
0.9					
0.7					
0.5					R2,R8, R9,10
0.3			R1, R4	R11	R5
0.1					R7

Tabela 18 - Matriz Probabilidade e Impacto
Fonte: Elaboração Própria

Através da consulta da Tabela 18, é facilmente percetível que é necessário colocar em prática os planos de resposta a fim de proceder ao respetivo tratamento de cada um dos riscos. Os riscos identificados que se encontram localizados na zona vermelha da matriz devem ser considerados prioritários, isto é, críticos, e onde é necessário garantir que o gestor de projeto presta a atenção devida a fim de reduzir o seu impacto no projeto.

ID do Risco	**Nível de Risco**	**Mitigar/Aceitar**	**Reduzir/Mitigar**	**Evitar**
1	0,06		**X**	
2	0,40			**X**
3	0,04	**X**		
4	0,06		**X**	
5	0,24			**X**
6	0,02	**X**		
7	0,08		**X**	
8	0,40			**X**
9	0,40			**X**
10	0,40			**X**
11	0,12		**X**	
12	0,01	**X**		

13	0,01	**X**		

Tabela 19 - Identificação do tipo de respostas ao risco delineadas para os riscos do projeto
Fonte: Elaboração Própria

Pela análise da Tabela 19 é possível aferir que a equipa de projeto, apesar de não existir uma cultura de gestão do risco na empresa, está comprometida em evitar e reduzir o risco, investindo no planeamento de respostas de prevenção e mitigação do risco. O plano de aceitação é utilizado em situações que não permitam outro tipo de intervenção, sendo aceitável em quatro riscos (R3, R6, R12, R13), e em caso de os planos de resposta preventivos e/ou de mitigação do risco falharem.

No que diz respeito ao cumprimento dos requisitos do DL n.º 65/2021, os mesmos foram alcançados de acordo com o pretendido e descrito na revisão da literatura. Ambas as organizações do presente estudo alcançaram os requisitos exigidos pelo DL n. º65/2021, na medida em que foram criados os documentos necessários (página 153) e exigidos pela legislação, impedindo assim que estas venham a sofrer coimas instituídas pela Lei n. º46/2018.

5. Conclusão

Neste capítulo são apresentados os principais resultados do projeto avançado, salientando a aplicação da metodologia de gestão de risco em projetos proposta. Por fim, serão referidos temas de trabalhos futuros para os quais este pode servir de base. Abordar-se-ão também algumas limitações à realização deste projeto.

É possível concluir que todos os objetivos propostos na realização do projeto avançado foram alcançados, visto que, apesar da baixa maturidade da empresa onde foi aplicada a metodologia, foram implementadas metodologias de gestão de risco do projeto de modo que o processo de implementação do DL fosse criado e implementado nas organizações em estudo, reduzindo, assim, o risco de coimas decretadas pela legislação, que as organizações correm no caso do não cumprimento dos requisitos estabelecidos pelo DL n.º65/2021.

De forma mais especifica, considerando os objetivos iniciais do projeto, pode-se dizer que:

- Aplicar metodologias de gestão de risco do projeto para criar um processo composto por procedimentos e respetivos documentos de suporte que permitam identificar pontos chave descritos na Lei n.º 46/2018 e no DL n.º 65/2021 – apesar da falta de processos em gestão de projetos, foi aplicada a metodologia de gestão de risco em projetos de modo a mitigar os riscos que pudessem afetar o desenvolvimento e posterior conclusão do projeto;
- Contribuir para o aumento do nível de maturidade das organizações em termos de cibersegurança – através da aplicação dos requisitos impostos pelo DL n. º65/2021, as organizações criam processos e procedimentos internos que auxiliam na resolução de supostos incidentes;
- Reduzir o risco de ataques cibernéticos com as consequências nefastas ao nível do impacto no negócio – com a aplicação do artigo 10.º do DL n.º 65/2021 as organizações vêm-se obrigadas à implementação de uma metodologia de gestão de risco da segurança da informação;
- Simplificar o processo de cumprimento do DL n.º 65/2021 – com o desenho do processo, as organizações têm capacidade de, através do que foi descrito no documento, implementar todos os requisitos legais exigidos;
- Normalizar o processo de implementação dos requisitos definidos pelo DL junto das organizações – uma vez normalizados, os processos estão preparados para serem implementados em qualquer organização da Administração Pública e/ou OES;
- Dar cumprimento por parte da Administração Pública e dos OES, ao DL n.º 65/2021 – o processo foi desenhado tendo em conta os requisitos obrigatórios para esse tipo de organizações;

- Reduzir o risco de coimas decretadas na Lei n.º 46/2018 – uma vez que os requisitos foram todos implementados e as devidas comunicações ao CNCS estabelecidas, as organizações em estudo ficaram livres de coimas associadas.

Com a implementação do processo criado ao longo do projeto avançado, as organizações têm a possibilidade de aumentar o nível de maturidade em termos de cibersegurança, reduzindo o risco de ataques cibernéticos e como tal, o risco geral a que a organização está sujeita ao nível do incumprimento das obrigações legais.

Este projeto pode servir como base de aplicação a outras organizações que pretendam diminuir a exposição ao risco ao nível de segurança informática em operadores de serviços digitais e infraestruturas críticas, ou qualquer organização que sinta necessidade de implementar uma metodologia de gestão de risco em segurança de informação.

Ao nível de limitações podem-se mencionar as seguintes:

- o já referido baixo grau de maturidade da empresa onde foi desenvolvida a metodologia de gestão do risco;
- o facto de a temática da cibersegurança ser um tópico em constante evolução;
- a falta de exemplos na literatura fez com que se tivessem de desenhar "factos à medida" da organização utilizada;
- o tipo de metodologia utilizada não permite a generalização exatamente devido ao facto relacionado com o anteriormente mencionado

5.1 Propostas de trabalhos futuros

Tendo em conta que a empresa em que foi implementada a metodologia de gestão do risco com vista à implementação dos requisitos definidos pela legislação em vigor no que toca à cibersegurança tem características particulares como, por exemplo uma baixa maturidade, seria de todo o interesse replicar o estudo noutro tipo de empresas eventualmente fazendo os ajustes necessários.

No que diz respeito ao desenho do processo de implementação do DL, é proposto que no futuro, a análise de risco seja realizada através de uma ferramenta, como por exemplo o *Monarc*[11], uma vez que a ferramenta utiliza uma metodologia de acordo com a apresentada na revisão da literatura.

[11] https://www.monarc.lu/

Referências Bibliográficas

Alhawari, S., Karadsheh, L., Nehari Talet, A., & Mansour, E. (2012). Knowledge-Based Risk Management framework for Information Technology project. *International Journal of Information Management*, *32*(1), 50–65. https://doi.org/10.1016/j.ijinfomgt.2011.07.002

António Miguel. (2019). *Gestão Moderna de Projetos Melhores Técnicas e Práticas (8ª Edição Atualizada)*.

Assembleia da República. (2018). Lei n.º 46/2018 Regime jurídico da segurança do ciberespaço. *Diário Da República n.º 155/2018, Série I de 2018-08-13*, 4031–4037. https://dre.pt/home/-/dre/116029384/details/maximized

Baskerville, R. L. (1999). Investigating Information Systems with Action Research. *Communications of the Association for Information Systems*, *2*(October). https://doi.org/10.17705/1cais.00219

Beláz, A. (2019). *The changing role of the EU in cybersecurity* (pp. 17–30).

Carayannis, E. G. (2005). *The story of managing projects an interdisciplinary approach. Westport*. Praege.

Centro Nacional de Cibersegurança. (n.d.). *Classificação de Incidentes*.

Chapman, C., & Ward, S. (2003). *Project Risk Management Second Edition*.

Chen, H. L., Chen, W. T., & Lin, Y. L. (2016). Earned value project management: Improving the predictive power of planned value. *International Journal of Project Management*, *34*(1), 22–29. https://doi.org/10.1016/j.ijproman.2015.09.008

CNCS. (2019). *Quadro Nacional de Referência Para a Cibersegurança*.

David Avison, Francis Lau, Michael Myers, and P. A. N. (1999). Action research. To make academic research relevant, researchers should try out their theories with practitiones in real situations and real organizations. *The American Journal of Nursing*, *42*, 94–97. https://doi.org/10.1097/00000446-195112000-00046

Decreto-Lei nº 65. (2021). Presidência do Conselho de Ministros. Resolução do Conselho de Ministros 59/2001. *Diário Da República - I Série-B*, *25*(2), 3179–3182. https://dre.pt/application/conteudo/496727

ENISA. (2017). *ENISA overview of cybersecurity and related terminology Foreword by the Executive Director*. *September*, 1–8.

Europeia, C. (2013). Comunicação Conjunta ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões. Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido. *Comissão Europeia*, 1–23.

EUROPEIA, C. (2017). PROPOSTA DE REGULAMENTO DO PARLAMENTO EUROPEU E

DO CONSELHO RELATIVA À ENISA. *COMISSÃO EUROPEIA*, *0225*.

Europeia, P. E. e o C. da U. (2016). DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO de 6 de julho de 2016. *Official Journal of the European Union*, *2014*(2), 1–30. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016L1148

Feldman, A., & Minstrell, J. (2000). Action Research as a Research Methodology for the Study of the Teaching and Learning of Science. *Handbook of Research Design in Mathematics and Science Education*, 429–445.

Gholamzadeh Chofreh, A., Goni, F. A., Ismail, S., Mohamed Shaharoun, A., Klemeš, J. J., & Zeinalnezhad, M. (2016). A master plan for the implementation of sustainable enterprise resource planning systems (part I): concept and methodology. *Journal of Cleaner Production*, *136*, 176–182. https://doi.org/10.1016/j.jclepro.2016.05.140

Hillson, D. (2002). The risk breakdown structure (RBS) as an aid to effective risk management. *Fifth European Project Management Conference*, *June*, 19–20. http://personal.stthomas.edu/jcpalzer/Bill/ArtSummary-RiskBreakdownStructure.doc

IPMA. (2015). *IPMA Individual Competence Baseline (ICB), Version 4.0*.

ISO/IEC 27000. (2018). Information technology — Security techniques — Information security management systems — Overview and vocabulary. *International Organization for Standardization (ISO)*, *34*(19).

ISO/IEC 27001. (2013). INTERNATIONAL STANDARD ISO / IEC Information technology — Security techniques — Information security management systems — Requirements. *Information Technology — Security Techniques — Information Security Management Systems — Requirements*, *2014*(ISO/IEC 27001:2013), 38.

ISO/IEC 27005. (2018). Information technology — Security techniques — Information security risk management. *International Organization for Standardization (ISO)*, 1–60.

ISO/IEC 27032. (2012). Information technology — Security techniques — Guidelines for cybersecurity. *International Organization for Standardization (ISO)*.

ISO 21500. (2021). Project, programme and portfolio management — Context and concepts. *International Organization for Standardization (ISO)*.

ISO 21502. (2020). Project, programme and portfolio management - Guidance on governance. *International Organization for Standardization (ISO)*. https://www.iso.org/committee/624837.html

ISO 22301. (2019). Security and resilience — Business continuity management systems — Requirements. *International Organization for Standardization (ISO)*.

ISO Guide 73. (2009). Risk management — Vocabulary. *International Organization for Standardization (ISO)*. https://www.iso.org/obp/ui/

Kemmis, S., & McTaggart, R. (1988). The Action Research Planner. *Deakin University*.

Kemmis, S. (1989). Investigácion en la Accion. In *Enciclopedia International de Educación* (pp. 3330–3337).

Kerzner, H. (2009). *Project management: A systems approach to planning, scheduling and controlling. Tenth Edition.*

Keshk, A. M., Maarouf, I., & Annany, Y. (2018). Special studies in management of construction project risks, risk concept, plan building, risk quantitative and qualitative analysis, risk response strategies. *Alexandria Engineering Journal*, *57*(4), 3179–3187. https://doi.org/10.1016/j.aej.2017.12.003

Kwak, Y. H. (2011). A Brief History of Project Management. *The Oxford Handbook of Project Management*, *1916*, 1–10. https://doi.org/10.1093/oxfordhb/9780199563142.003.0002

Latorre, A. (2003). *La investigación-acción*. *1984*, 1–16.

Leiner, B. M., Cerf, V. G., Clark, D. D., Kahn, R. E., Kleinrock, L., Lynch, D. C., Postel, J., Roberts, L. G., & Wolff, S. (2009). A brief history of the internet. *ACM SIGCOMM Computer Communication Review*, *39*(5), 22–31. https://doi.org/10.1145/1629607.1629613

Mehdizadeh, R., Franck, T., Denys, B., & Halidou, N. (2012). Methodology and tools for risk evaluation in construction projects using Risk Breakdown Structure. *European Journal of Environmental and Civil Engineering*, *16*(SUPPL. 1). https://doi.org/10.1080/19648189.2012.681959

Meredith, J. R. e Mantel, Jr, S. (2006). *Project management a managerial approach (6th ed.)*.

Meskendahl, S. (2010). The influence of business strategy on project portfolio management and its success - A conceptual framework. *International Journal of Project Management*, *28*(8), 807–817. https://doi.org/10.1016/j.ijproman.2010.06.007

Morgan, R. P. (2011). Parecer do Comité Económico e Social Europeu sobre a «Proposta de regulamento do Parlamento Europeu e do Conselho relativo à Agência Europeia para a Segurança das Redes e da Informação (ENISA)». *Jornal Oficial Da União Europeia*, 58–63.

Muriana, C., & Vizzini, G. (2017). Project risk management: A deterministic quantitative technique for assessment and mitigation. *International Journal of Project Management*, *35*(3), 320–340. https://doi.org/10.1016/j.ijproman.2017.01.010

NASA. (1969). *Apollo 11 Mission Overview*. https://www.nasa.gov/mission_pages/apollo/missions/apollo11.html

NP ISO 31000:2009. (2013). Gestão de Risco: Princípios e linhas de orientação. *International Organization for Standardization (ISO)*, *2012*, 1–30.

NP ISO 31010. (2009). Risk Management - Risk Assessment Techniques. *International Organization for Standardization (ISO)*.

Peixoto, J., Tereso, A., Fernandes, G., & Almeida, R. (2014). Project Risk Management Methodology: A Case Study of an Electric Energy Organization. *Procedia Technology*, *16*, 1096–1105. https://doi.org/10.1016/j.protcy.2014.10.124

PMI. (2009). Practice Standard for Project Risk Management. In *Project Management Institute, Inc. (PMI)*. https://app.knovel.com/web/toc.v/cid:kpPSPRM002/viewerType:toc/root_slug:practice-standard-project/url_slug:kt00CAWY21

PMI. (2013a). *PMBOK, 5th edition*.

PMI. (2013b). *PROJECT MANAGEMENT INSTITUTE The Standard for Portfolio Management – Third Edition*.

PMI. (2017a). *PMBOK,6th edition*.

PMI. (2017b). PROJECT MANAGEMENT INSTITUTE The Standard for Portfolio Management – Fourth Edition. In *Project Management Institute, Inc.* http://joi.iijournals.com/lookup/doi/10.3905/joi.4.3.57

PMI. (2019). *The Standard For Risk Management in Portfolios, Programs, and Projects*.

Purnus, A., & Bodea, C.-N. (2013). Considerations on Project Quantitative Risk Analysis. *Procedia - Social and Behavioral Sciences*, *74*, 144–153. https://doi.org/10.1016/j.sbspro.2013.03.031

República, D. (2021). *Gabinete Nacional de Segurança*. 19–25.

Robert G. Cooper, Scott J. Edgett, Elko J. Kleinschmidt. (1999). New product portfolio management: practices and performance. *Journal of Product Innovation Management*, *16*(4), 333–351.

Saunders, M., Lewis, P., and Thornhill, A. (2009). Research methods for business students. In *International Journal of the History of Sport* (fifth edit, Vol. 30, Issue 1). https://doi.org/10.1080/09523367.2012.743996

Sêmola, M. (2003). *Gestão da Segurança da Informação. Uma visão Executiva* (Elsevier Editora Ltda. (ed.)).

Seymour, T., & Hussein, S. (2014). The History Of Project Management. *International Journal of Management & Information Systems (IJMIS)*, *18*(4), 233. https://doi.org/10.19030/ijmis.v18i4.8820

Somekh, B. (1995). The contribution of action research to development in social endeavours: a position paper on action research methodology. *British Educational Research Journal*, *21*, 339–355. https://doi.org/10.1080/0141192950210307

Tworek, P. (2012). *PLAN RISK RESPONSE AS A STAGE OF RISK MANAGEMENT IN INVESTMENT PROJECTS IN POLISH AND U.S. CONSTRUCTION - METHODS, RESEARCH*.

União Europeia. (2016). Tratado de Funcionamento da União Europeia. *Jornal Oficial Da União Europeia*, 47–200. https://eur-lex.europa.eu/resource.html?uri=cellar:9e8d52e1-2c70-11e6-b497-01aa75ed71a1.0019.01/DOC_3&format=PDF

van Eck, N. J., & Waltman, L. (2010). Software survey: VOSviewer, a computer program for

bibliometric mapping. *Scientometrics*, *84*(2), 523–538. https://doi.org/10.1007/s11192-009-0146-3

Vitkin, E., Carmeli, B., Greenshpan, O., Baras, D., & Marmor, Y. (2010). MEDAL: Measuring of emergency departments' adaptive load. In *Studies in Health Technology and Informatics* (Vol. 160, Issue PART 1). https://doi.org/10.3233/978-1-60750-588-4-218

Webb, J., Ahmad, A., Maynard, S. B., & Shanks, G. (2014). A situation awareness model for information security risk management. *Computers and Security*, *44*, 1–15. https://doi.org/10.1016/j.cose.2014.04.005

Wheeler, E. (2011). *Security risk management: Building an information security risk management program from the Ground* (Elsevier (ed.)).

Wheelwright, S. C., & Clark, K. B. (1982). *Creating project plans to focus product development*.

Winter, Mark and Szczepanek, T. (2008). Projects and programmes as value creation processes: A new perspective and some practical implications. *International Journal of Project Management*, *26*. https://doi.org/10.1016/j.ijproman.2007.08.015

Apêndices

1. Identificação das ameaças e das vulnerabilidades

Tipo Ameaça	Ameaça	Tipo Vulnerabilidade	Vulnerabilidade
Ataque malicioso	Acesso não autorizado a sistemas	Organização	Inexistência de um procedimento formal para o registo e a remoção de utilizadores
		Pessoas	Falta de consciencialização em segurança
			Formação insuficiente em segurança
			Uso incorreto de *software* e *hardware*
		Software	Atribuição indevida de direitos de acesso
			Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
			Listas de *password*s desprotegidas
			Má gestão de *password*s
			Não execução do "*logout*" ao deixar-se uma estação de trabalho sem assistência / controlo
	Alteração do *hardware*	*Hardware*	Armazenamento não protegido
			Falta de cuidado durante o descarte e a destruição
			Falta de uma rotina de substituição periódica
			Inexistência de um controlo eficiente de mudança de configuração

		Manutenção insuficiente/Instalação defeituosa de dispositivos de armazenamento
		Realização não controlada de cópias
		Sensibilidade à humidade, poeira, sujeira
		Sensibilidade à radiação eletromagnética
		Sensibilidade a variações de temperatura
		Sensibilidade a variações de voltagem
Alteração do *software*	*Software*	*Download* e uso não controlado de *software*
		Inexistência de cópias de segurança (“backup”)
Ataque a sistemas (por exemplo, ataque distribuído de negação de serviço)	Organização	Inexistência de política de uso de correspondência eletrónica (*e-mail*)
		Inexistência de procedimentos para a instalação de *software* em sistemas operativos
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Uso incorreto de *software* e *hardware*
	Rede	Conexões de redes públicas desprotegidas
		Transferência de *password*s em claro
	Software	Atribuição indevida de direitos de acesso
		Configuração de parâmetros incorreta

		Download e uso não controlado de *software*
		Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
		Inexistência de um registo de auditoria
		Listas de *password*s desprotegidas
		Má gestão de *password*s
		Procedimentos de teste de *software* insuficientes ou inexistentes
Ato fraudulento (por exemplo, reutilização indevida de credenciais e dados transmitidos, fazer-se passar por uma outra pessoa, intercetação)	Organização	Inexistência de procedimentos para o *report* de fragilidades ligadas à segurança
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
	Rede	Conexões de redes públicas desprotegidas
		Não identificação e não autenticação do emissor e do recetor
		Transferência de *password*s em claro
	Software	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
		Listas de *password*s desprotegidas
		Má gestão de *password*s

Bomba/terrorismo	Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Organização	Inexistência de controlo sobre ativos fora das dependências
		Inexistência de procedimento de monitorização das instalações de processamento de informações
		Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)
		Inexistência de um procedimento formal para o registo e a remoção de utilizadores
		Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros
	Software	Atribuição indevida de direitos de acesso
Chantagem, suborno, agressão ou extorsão a funcionários	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de mecanismos de monitorização
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
		Procedimentos de recrutamento inadequados
		Trabalho não supervisionado de pessoal de limpeza ou de terceirizados
		Uso incorreto de *software* e *hardware*
Ciberespionagem	Rede	Arquitetura insegura da rede

		Transferência de *password*s em claro
Comprometimento dos dados	Organização	Inexistência de um procedimento formal para a supervisão dos registos do SGSI
		Inexistência de um procedimento formal para o controlo da documentação do SGSI
	Software	*Software* amplamente distribuído
		Utilizar programas com um conjunto errado de dados (referentes a um outro período)
Cópia ilegal de *software*	Organização	Inexistência de procedimentos para a instalação de software em sistemas operativos
		Inexistência de uma política formal sobre o uso de dispositivos móveis
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de mecanismos de monitorização
	Software	Documentação inexistente
		Download e uso não controlado de *software*
Crime digital (por exemplo, perseguição no mundo digital)	Organização	Inexistência de procedimentos para o report de fragilidades ligadas à segurança
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança

		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
	Rede	Conexões de redes públicas desprotegidas
		Não identificação e não autenticação do emissor e do recetor
		Transferência de *password*s em claro
	Software	Listas de *password*s desprotegidas
		Má gestão de *password*s
Determinação da localização	*Hardware*	Armazenamento não protegido
		Falta de cuidado durante o descarte e a destruição
	Local ou instalações	Inexistência de mecanismos de proteção física no prédio, portas e janelas
		Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Trabalho não supervisionado de pessoal de limpeza ou de terceirizados
	Rede	Conexões de redes públicas desprotegidas
Engenharia social	Organização	Inexistência de procedimentos para a manipulação de informações classificadas
	Pessoas	Falta de consciencialização em segurança

		Formação insuficiente em segurança
		Inexistência de mecanismos de monitorização
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
		Procedimentos de recrutamento inadequados
		Trabalho não supervisionado de pessoal de limpeza ou de terceirizados
		Uso incorreto de *software* e *hardware*
Entrada de dados falsificados ou corrompidos	*Hardware*	Armazenamento não protegido
		Realização não controlada de cópias
	Organização	Inexistência de um procedimento formal para a supervisão dos registos do SGSI
		Inexistência de um procedimento formal para o controlo da documentação do SGSI
		Inexistência de um processo formal para a autorização das informações disponíveis publicamente
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de mecanismos de monitorização
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens

		Uso incorreto de *software* e *hardware*
	Rede	Arquitetura insegura da rede
		Conexões de redes públicas desprotegidas
		Gestão de rede inadequada (quanto à flexibilidade de roteamento)
		Inexistência de evidências que comprovem o envio ou receção de mensagens
		Junções de cablagem mal feitas
		Linhas de comunicação desprotegidas
		Não identificação e não autenticação do emissor e do recetor
		Ponto único de falha
		Tráfego sensível desprotegido
		Transferência de *password*s em claro
	Software	Configuração de parâmetros incorreta
		Datas incorretas
		Software amplamente distribuído
		Utilizar programas com um conjunto errado de dados (referentes a um outro período)
Escuta não autorizada	Rede	Linhas de comunicação desprotegidas
		Tráfego sensível desprotegido

Forjamento de direitos	Rede	Não identificação e não autenticação do emissor e do recetor
Furto de dispositivos de armazenamento ou documentos	*Hardware*	Armazenamento não protegido
		Falta de cuidado durante o descarte e a destruição
		Realização não controlada de cópias
	Local ou instalações	Inexistência de mecanismos de proteção física no prédio, portas e janelas
	Organização	Inexistência de autorização para as instalações de processamento de informações
		Inexistência de mecanismos estabelecidos para a monitorização de violações da segurança
		Política de mesas e ecrãs limpos ("*clear desk and clear screen*") inexistente ou insuficiente
	Pessoas	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados
Furto de equipamentos	Local ou instalações	Inexistência de mecanismos de proteção física no prédio, portas e janelas
	Organização	Inexistência de controlo sobre ativos fora das dependências
		Inexistência de um processo disciplinar no caso de incidentes relacionados à segurança da informação
		Inexistência de uma política formal sobre o uso de dispositivos móveis
Furto de informação	Organização	Inexistência de política de uso de correspondência eletrónica (e-*mail*)
		Inexistência de relatórios de falha nos arquivos ("*logs*") de auditoria das atividades de administradores e operadores

		Inexistência de um processo formal para a autorização das informações disponíveis publicamente
		Inexistência de uma política formal sobre o uso de dispositivos móveis
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de mecanismos de monitorização
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
	Software	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
Guerra de informação	Organização	Atribuição inadequada das responsabilidades pela segurança da informação
		Cláusulas (relativas à segurança) insuficientes ou inexistentes, em contratos com funcionários
		Inexistência de procedimentos para a manipulação de informações classificadas
		Inexistência de um procedimento formal para a supervisão dos registos do SGSI
		Inexistência de um procedimento formal para o controlo da documentação do SGSI
		Inexistência de um processo formal para a autorização das informações disponíveis publicamente
	Pessoas	Falta de consciencialização em segurança

		Formação insuficiente em segurança
	Software	Inexistência de um registo de auditoria
Intercetação de informações	*Hardware*	Armazenamento não protegido
		Realização não controlada de cópias
	Organização	Inexistência de um procedimento formal para a supervisão dos registos do SGSI
		Inexistência de um procedimento formal para o controlo da documentação do SGSI
		Inexistência de um processo formal para a autorização das informações disponíveis publicamente
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de mecanismos de monitorização
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
		Uso incorreto de *software* e *hardware*
	Rede	Arquitetura insegura da rede
		Conexões de redes públicas desprotegidas
		Gestão de rede inadequada (quanto à flexibilidade de roteamento)

		Inexistência de evidências que comprovem o envio ou receção de mensagens
		Junções de cablagem mal feitas
		Linhas de comunicação desprotegidas
		Não identificação e não autenticação do emissor e do recetor
		Ponto único de falha
		Tráfego sensível desprotegido
		Transferência de *password*s em claro
	Software	Configuração de parâmetros incorreta
		Datas incorretas
		Software amplamente distribuído
		Utilizar programas com um conjunto errado de dados (referentes a um outro período)
Intrusão em sistemas, infiltrações e entradas não autorizadas	Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Organização	Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)
	Rede	Arquitetura insegura da rede
		Transferência de *password*s em claro
	Software	Atribuição indevida de direitos de acesso

		Listas de *password*s desprotegidas
		Má gestão de *password*s
Processamento ilegal de dados	Organização	Cláusulas (relativas à segurança) insuficientes ou inexistentes, em contratos com funcionários
	Pessoas	Inexistência de mecanismos de monitorização
	Software	Serviços desnecessários permanecem habilitados
Recuperação de dispositivos de armazenamento reciclados ou descartados	*Hardware*	Falta de cuidado durante o descarte e a destruição
	Organização	Inexistência de mecanismos estabelecidos para a monitorização de violações da segurança
Sabotagem de sistemas	*Hardware*	Armazenamento não protegido
		Falta de cuidado durante o descarte e a destruição
		Realização não controlada de cópias
	Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Organização	Atribuição inadequada das responsabilidades pela segurança da informação
		Inexistência de auditorias periódicas (supervisão)
		Inexistência de política de uso de correspondência eletrónica (*e-mail*)
		Inexistência de procedimento de monitorização das instalações de processamento de informações

		Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)
		Inexistência de um procedimento formal para a supervisão dos registos do SGSI
		Inexistência de um procedimento formal para o controlo da documentação do SGSI
		Inexistência de um procedimento formal para o registo e a remoção de utilizadores
		Inexistência de um processo formal para a autorização das informações disponíveis publicamente
		Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de mecanismos de monitorização
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
		Procedimentos de recrutamento inadequados
		Uso incorreto de *software* e *hardware*
	Rede	Arquitetura insegura da rede
		Conexões de redes públicas desprotegidas

		Gestão de rede inadequada (quanto à flexibilidade de roteamento)
		Inexistência de evidências que comprovem o envio ou receção de mensagens
		Junções de cablagem mal feitas
		Linhas de comunicação desprotegidas
		Não identificação e não autenticação do emissor e do recetor
		Ponto único de falha
		Tráfego sensível desprotegido
		Transferência de *password*s em claro
	Software	Atribuição indevida de direitos de acesso
		Configuração de parâmetros incorreta
		Destruição ou reutilização de dispositivos de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados
		Documentação inexistente
		Download e uso não controlado de *software*
		Falhas conhecidas no *software*
		Inexistência de cópias de segurança (“*backup*”)
		Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores

		Inexistência de relatórios de gestão
		Inexistência de um controlo eficaz de mudança
		Inexistência de um registo de auditoria
		Listas de *password*s desprotegidas
		Má gestão de *password*s
		Não execução do "*logout*" ao deixar-se uma estação de trabalho sem assistência / controlo
		Procedimentos de teste de *software* insuficientes ou inexistentes
		Serviços desnecessários permanecem habilitados
		Software amplamente distribuído
		Utilizar programas com um conjunto errado de dados (referentes a um outro período)
Spoofing (fazer-se passar por outro)	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de mecanismos de monitorização
	Rede	Arquitetura insegura da rede
		Conexões de redes públicas desprotegidas
		Gestão de rede inadequada (quanto à flexibilidade de roteamento)
		Transferência de *password*s em claro

	Software	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
		Listas de *password*s desprotegidas
		Má gestão de *password*s
Suborno por informação	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de mecanismos de monitorização
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
Uso de cópias de software falsificadas ou ilegais	Organização	Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual
Uso impróprio de recurso computacional	*Hardware*	Armazenamento não protegido
		Falta de cuidado durante o descarte e a destruição
		Realização não controlada de cópias
	Local ou instalações	Inexistência de mecanismos de proteção física no prédio, portas e janelas
	Organização	Ausência das responsabilidades ligadas à segurança da informação nas descrições de cargos e funções
		Ausência de registos nos arquivos de auditoria ("*logs*") de administradores e operadores
		Inexistência de análises críticas periódicas por parte da direção

		Inexistência de autorização para as instalações de processamento de informações
		Inexistência de controlo sobre ativos fora das dependências
		Inexistência de mecanismos estabelecidos para a monitorização de violações da segurança
		Inexistência de política de uso de correspondência eletrónica *(e-mail)*
		Inexistência de procedimentos para a instalação de *software* em sistemas operativos
		Inexistência de procedimentos para a manipulação de informações classificadas
		Inexistência de procedimentos para o *report* de fragilidades ligadas à segurança
		Inexistência de um processo disciplinar no caso de incidentes relacionados à segurança da informação
		Inexistência de uma política formal sobre o uso de dispositivos móveis
		Política de mesas e ecrãs limpos ("*clear desk and clear screen*") inexistente ou insuficiente
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
		Uso incorreto de *software* e *hardware*

	Rede	Conexões de redes públicas desprotegidas
		Junções de cablagem mal feitas
		Ponto único de falha
	Software	Configuração de parâmetros incorreta
		Datas incorretas
		Documentação inexistente
		Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
		Inexistência de relatórios de gestão
		Interface de utilizador complexa
		Listas de *password*s desprotegidas
		Má gestão de *password*s
Uso não autorizado de equipamento	Organização	Inexistência de análises críticas periódicas por parte da direção
		Inexistência de procedimentos para o *report* de fragilidades ligadas à segurança
	Pessoas	Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
	Rede	Conexões de redes públicas desprotegidas
	Software	Inexistência de relatórios de gestão

Utilização de Código malicioso (por exemplo: vírus, *ransomware*, Cavalo de Troia e etc.)	Organização	Inexistência de controlo sobre ativos fora das dependências
		Inexistência de política de uso de correspondência eletrónica (*e-mail*)
		Inexistência de procedimentos para a instalação de *software* em sistemas operativos
		Inexistência de uma política formal sobre o uso de dispositivos móveis
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Uso incorreto de *software* e *hardware*
	Rede	Conexões de redes públicas desprotegidas
		Transferência de *password*s em claro
	Software	Atribuição indevida de direitos de acesso
		Configuração de parâmetros incorreta
		Download e uso não controlado de *software*
		Inexistência de cópias de segurança ("*backup*")
		Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
		Inexistência de um registo de auditoria
		Listas de *password*s desprotegidas
		Má gestão de *password*s

		Procedimentos de teste de *software* insuficientes ou inexistentes
Vasculhar informação de propriedade intelectual	Organização	Inexistência de política de uso de correspondência eletrónica (*e-mail*)
		Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual
		Inexistência de procedimentos para o *report* de fragilidades ligadas à segurança
		Inexistência de relatórios de falha nos arquivos ("*logs*") de auditoria das atividades de administradores e operadores
		Inexistência de um processo formal para a autorização das informações disponíveis publicamente
		Inexistência de uma política formal sobre o uso de dispositivos móveis
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Inexistência de mecanismos de monitorização
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
	Software	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
Violação de dados pessoais	Organização	Inexistência de política de uso de correspondência eletrónica (*e-mail*)
		Inexistência de um processo formal para a autorização das informações disponíveis publicamente

			Inexistência de uma política formal sobre o uso de dispositivos móveis
		Pessoas	Falta de consciencialização em segurança
			Formação insuficiente em segurança
			Inexistência de mecanismos de monitorização
			Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
Erro Humano	Acesso não autorizado a sistemas	Organização	Inexistência de um procedimento formal para o registo e a remoção de utilizadores
		Pessoas	Falta de consciencialização em segurança
			Formação insuficiente em segurança
			Uso incorreto de *software* e *hardware*
		Software	Atribuição indevida de direitos de acesso
			Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
			Listas de *password*s desprotegidas
			Má gestão de *password*s
			Não execução do "*logout*" ao deixar-se uma estação de trabalho sem assistência / controlo
	Alteração do *hardware*	*Hardware*	Armazenamento não protegido
			Falta de uma rotina de substituição periódica

		Inexistência de um controlo eficiente de mudança de configuração
	Pessoas	Trabalho não supervisionado de pessoal de limpeza ou de terceirizados
		Uso incorreto de *software* e *hardware*
Alteração do *software*	Pessoas	Uso incorreto de *software* e *hardware*
	Software	Download e uso não controlado de *software*
		Especificações confusas ou incompletas para os *developers*
		Inexistência de cópias de segurança ("*backup*")
		Inexistência de um controlo eficaz de mudança
		Software novo ou imaturo
Dados de fontes não confiáveis	Organização	Inexistência de um processo formal para a autorização das informações disponíveis publicamente
Defeitos ("*bugs*") no sistema	*Software*	Especificações confusas ou incompletas para os *developers*
		Inexistência de um controlo eficaz de mudança
		Software novo ou imaturo
Divulgação indevida de informação	Organização	Atribuição inadequada das responsabilidades pela segurança da informação
		Ausência das responsabilidades ligadas à segurança da informação nas descrições de cargos e funções
		Cláusulas (relativas à segurança) insuficientes ou inexistentes, em contratos com funcionários

			Inexistência de autorização para as instalações de processamento de informações
			Inexistência de mecanismos estabelecidos para a monitorização de violações da segurança
			Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual
			Inexistência de um processo formal para a autorização das informações disponíveis publicamente
			Política de mesas e ecrãs limpos ("*clear desk and clear screen*") inexistente ou insuficiente
	Processamento ilegal de dados	Organização	Cláusulas (relativas à segurança) insuficientes ou inexistentes, em contratos com funcionários
		Pessoas	Inexistência de mecanismos de monitorização
		Software	Serviços desnecessários permanecem habilitados
	Uso de cópias de *software* falsificadas ou ilegais	Organização	Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual
		Pessoas	Formação insuficiente em segurança
			Inexistência de mecanismos de monitorização
		Software	Documentação inexistente
			Download e uso não controlado de *software*
Falha de sistema	Defeito de equipamento	*Hardware*	Inexistência de um controlo eficiente de mudança de configuração

	Organização	Resposta inadequada do serviço de manutenção
	Pessoas	Uso incorreto de *software* e *hardware*
	Software	Configuração de parâmetros incorreta
Defeito de *software*	*Software*	Especificações confusas ou incompletas para os *developers*
		Inexistência de um controlo eficaz de mudança
		Software novo ou imaturo
Falha de equipamento	Organização	Inexistência de um plano de continuidade
Falha do ar condicionado	*Hardware*	Sensibilidade a variações de voltagem
	Local ou instalações	Fornecimento de energia instável
	Organização	Resposta inadequada do serviço de manutenção
Interseção de comunicação não autorizada	Rede	Linhas de comunicação desprotegidas
		Tráfego sensível desprotegido
Saturação do sistema de informação	Rede	Gestão de rede inadequada (quanto à flexibilidade de roteamento)
Violação das condições de uso do sistema de informação que possibilitam sua manutenção	*Hardware*	Manutenção insuficiente/Instalação defeituosa de dispositivos de armazenamento
	Organização	Inexistência de procedimento de controlo de mudanças
		Resposta inadequada do serviço de manutenção
		Service Level Agreement inexistente ou insuficiente

Falha no fornecimento de bens ou serviços por terceiro	Interrupção do fornecimento de energia	*Hardware*	Sensibilidade a variações de voltagem
		Local ou instalações	Fornecimento de energia instável
	Interrupção do fornecimento do serviço de telecomunicações	Organização	Inexistência de um plano de continuidade
		Rede	Junções de cablagem mal feitas
			Linhas de comunicação desprotegidas
			Ponto único de falha
			Tráfego sensível desprotegido
Fenómeno natural	Fenómeno climático	*Hardware*	Sensibilidade a variações de temperatura
		Local ou instalações	Fornecimento de energia instável
			Inexistência de mecanismos de proteção física no prédio, portas e janelas
			Localização em área suscetível a inundações
			Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Fenómeno sísmico	Local ou instalações	Fornecimento de energia instável
			Inexistência de mecanismos de proteção física no prédio, portas e janelas
			Localização em área suscetível a inundações
			Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Fenómeno vulcânico	Local ou instalações	Fornecimento de energia instável

			Inexistência de mecanismos de proteção física no prédio, portas e janelas
			Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Inundação	Local ou instalações	Localização em área suscetível a inundações
Outros	Abuso de direitos	Organização	Inexistência de auditorias periódicas (supervisão)
			Inexistência de procedimento de monitorização das instalações de processamento de informações
			Inexistência de procedimentos para a identificação, análise e avaliação de riscos
			Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)
			Inexistência de relatórios de falha nos arquivos ("*logs*") de auditoria das atividades de administradores e operadores
			Inexistência de um procedimento formal para o registo e a remoção de utilizadores
			Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros
		Software	Atribuição indevida de direitos de acesso
			Destruição ou reutilização de dispositivos de armazenamento sem a execução dos procedimentos apropriados de remoção dos dados
			Falhas conhecidas no *software*
			Inexistência de um registo de auditoria

		Não execução do "*logout*" ao deixar-se uma estação de trabalho sem assistência / controlo
		Procedimentos de teste de *software* insuficientes ou inexistentes
Acidente grave	*Hardware*	Armazenamento não protegido
		Falta de cuidado durante o descarte e a destruição
		Realização não controlada de cópias
	Local ou instalações	Inexistência de mecanismos de proteção física no prédio, portas e janelas
		Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Organização	Cláusulas (relativas à segurança) insuficientes ou inexistentes, em contratos com funcionários
		Inexistência de análises críticas periódicas por parte da direção
		Inexistência de autorização para as instalações de processamento de informações
		Inexistência de controlo sobre ativos fora das dependências
		Inexistência de mecanismos estabelecidos para a monitorização de violações da segurança
		Inexistência de procedimento de controlo de mudanças
		Inexistência de procedimentos para garantir a conformidade com os direitos de propriedade intelectual

		Inexistência de procedimentos para o *report* de fragilidades ligadas à segurança
		Inexistência de um plano de continuidade
		Inexistência de um procedimento formal para a supervisão dos registos do SGSI
		Inexistência de um procedimento formal para o controlo da documentação do SGSI
		Inexistência de um processo disciplinar no caso de incidentes relacionados à segurança da informação
		Inexistência de uma política formal sobre o uso de dispositivos móveis
	Pessoas	Inexistência de mecanismos de monitorização
		Inexistência de políticas para o uso correto de meios de telecomunicação e de troca de mensagens
		Trabalho não supervisionado de pessoal de limpeza ou de terceirizados
	Rede	Arquitetura insegura da rede
		Conexões de redes públicas desprotegidas
		Junções de cablagem mal feitas
		Linhas de comunicação desprotegidas
		Ponto único de falha
		Tráfego sensível desprotegido

		Transferência de *password*s em claro
	Software	*Download* e uso não controlado de *software*
		Inexistência de cópias de segurança (“*backup*”)
		Software amplamente distribuído
Água	Local ou instalações	Inexistência de mecanismos de proteção física no prédio, portas e janelas
		Localização em área suscetível a inundações
		Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
		Trabalho não supervisionado de pessoal de limpeza ou de terceirizados
Cenários de guerra	Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Organização	Atribuição inadequada das responsabilidades pela segurança da informação
		Cláusulas (relativas à segurança) insuficientes ou inexistentes, em contratos com funcionários
		Inexistência de controlo sobre ativos fora das dependências
		Inexistência de procedimento de monitorização das instalações de processamento de informações

		Inexistência de procedimentos para a manipulação de informações classificadas
		Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)
		Inexistência de um procedimento formal para a supervisão dos registos do SGSI
		Inexistência de um procedimento formal para o controlo da documentação do SGSI
		Inexistência de um procedimento formal para o registo e a remoção de utilizadores
		Inexistência de um processo formal para a autorização das informações disponíveis publicamente
		Provisões (relativas à segurança) insuficientes ou inexistentes, em contratos com clientes e/ou terceiros
	Pessoas	Falta de consciencialização em segurança
		Formação insuficiente em segurança
	Software	Atribuição indevida de direitos de acesso
		Inexistência de um registo de auditoria
Destruição de equipamento ou dispositivos de armazenamento	*Hardware*	Falta de uma rotina de substituição periódica
	Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Pessoas	Procedimentos de recrutamento inadequados

Fogo	*Hardware*	Sensibilidade a variações de temperatura
	Local ou instalações	Fornecimento de energia instável
		Inexistência de mecanismos de proteção física no prédio, portas e janelas
		Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
Impulsos eletromagnéticos	*Hardware*	Sensibilidade à radiação eletromagnética
	Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Organização	Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)
	Software	Atribuição indevida de direitos de acesso
Indisponibilidade de recursos humanos	Pessoas	Ausência de recursos humanos
Poeira, corrosão, congelamento	*Hardware*	Sensibilidade à humidade, poeira, sujeira
Radiação	*Hardware*	Sensibilidade à radiação eletromagnética
	Local ou instalações	Uso inadequado ou sem os cuidados necessários dos mecanismos de controlo do acesso físico a prédios e aposentos
	Organização	Inexistência de processo formal para a análise crítica dos direitos de acesso (supervisão)
	Software	Atribuição indevida de direitos de acesso

Repúdio de ações	Organização	Atribuição inadequada das responsabilidades pela segurança da informação
	Rede	Inexistência de evidências que comprovem o envio ou receção de mensagens
Utilização abusiva	Organização	Inexistência de política de uso de correspondência eletrónica (*e-mail*)
Utilização indevida de privilégios	*Software*	Inexistência de mecanismos de autenticação e identificação como, por exemplo, para a autenticação de utilizadores
		Listas de *password*s desprotegidas
		Má gestão de *password*s

2. Critérios de Análise e Avaliação do Risco

Metodologia da Análise de Risco Utilizada

Qualitativa	Quantitativa
Muito Alto	1
Alto	2
Médio	3
Baixo	4
Muito Baixo	5

Critérios de Probabilidade e Impacto

Critérios de avaliação		
Risco	**Impacto**	**Probabilidade**
Muito Baixo (1)	Consequências a nível departamental sem perdas financeiras para a empresa. Evento que gera impacto sobre uma pessoa ou representa perda de confidencialidade, integridade e disponibilidade que não necessita de intervenção ou paralisação imediata	Improvável que Ocorra (mais de 24 meses)
Baixo (2)	Consequências a nível departamental com possíveis perdas financeiras para a empresa. Evento que gera impacto sobre um pequeno grupo ou representa perda de confidencialidade, integridade e disponibilidade, prejudicando as funções secundárias de trabalho, não sendo o bastante para intervir nas funções principais.	Provavelmente ocorrerá (até 24 meses)
Médio (3)	Consequências moderadas para a empresa com perdas financeiras ou de imagem e reputação associadas. Evento que gera impacto sobre um grupo relevante ou representa perda de confidencialidade, integridade e disponibilidade, prejudicando as funções primárias de trabalho.	Ocorrerá a médio prazo (até 18 meses)
Alto (4)	Fortes consequências para a empresa, com perdas financeiras de imagem e reputação, ou possibilidade de perdas humanas. Evento que gera impacto sobre vários grupos ou representa perda de confidencialidade, integridade e disponibilidade, prejudicando as funções primárias de trabalho de múltiplas áreas da organização	Ocorrerá a curto prazo (até 12 meses)
Muito alto (5)	Perigo de continuidade da empresa com elevadas perdas financeiras, danos para a imagem e reputação ou perdas humanas. Evento que gera impacto em toda a organização ou representa perda de confidencialidade, integridade e disponibilidade,	Ocorrerá a muito curto Prazo (até 6 meses)

	causando prejuízos de forma generalizada, inviabilizando ou proporcionando perceção negativa.	

Critérios para cada nível de impacto para todas as áreas de consequências

Níveis de impacto	Legal ou Regulatório	Financeiro	Serviço a clientes	Reputacional
Muito alto (5)	Impacto legal/regulatório muito alto, com altas coimas associadas, podendo interromper a prestação do serviço.	Quebra operacional significativa, podendo ser total e/ou definitiva.	Impacto interno e externo comprometendo a prestação do serviço ou sistema forçando os colaboradores a não cumprir com as suas funções e responsabilidades	O evento foi publicado por fontes de comunicação social
Alto (4)	Impacto legal/regulatório de alto impacto com coimas associadas.	Quebra operacional parcial com impacto elevado nas operações.	Impacto externo comprometendo a prestação do serviço ou sistema forçando os colaboradores a não cumprir com as suas funções e responsabilidades	O evento foi publicado por pessoas individuais.
Médio (3)	Impacto legal/regulatório de médio impacto.	Quebra operacional parcial com impacto residual nas operações.	Impacto interno comprometendo a prestação do serviço ou sistema forçando os colaboradores a não cumprir parcialmente com as suas funções e responsabilidades	O evento ficou circunscrito internamente na organização.

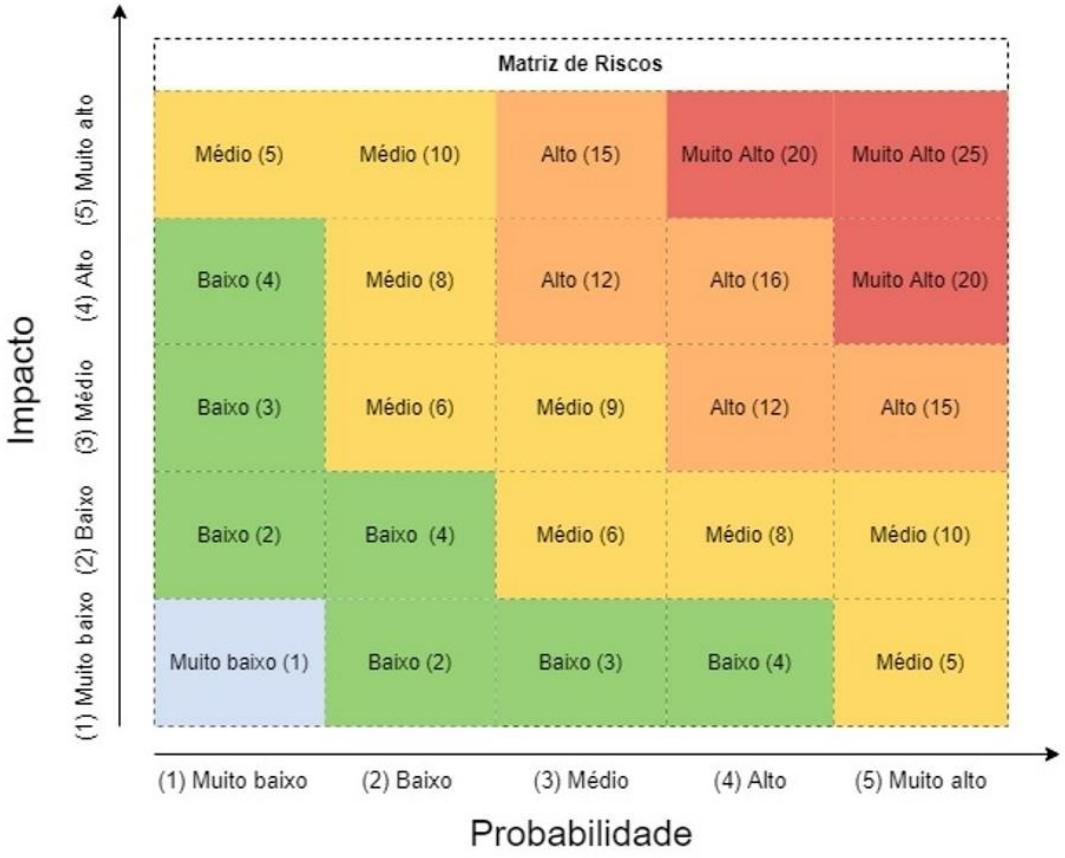
Baixo (2)	Impacto legal/regulatório de baixo impacto.	Quebra operacional parcial com baixo impacto nas operações.	Impacto interno comprometendo a prestação do serviço ou sistema, porém não interrompendo os colaboradores a cumprir com suas funções e responsabilidades	Evento ficou circunscrito internamente no departamento.
Muito baixo (1)	Inspeção com ausência de recomendações do regulador.	Sem impacto operacional/financeiro para a organização.	Impacto interno não comprometendo a prestação do serviço ou sistema, e não interrompendo os colaboradores a cumprir com suas funções e responsabilidades	Evento ficou circunscrito internamente na área afetada.

Determinação do Nível de Risco

Relacionando o potencial impacto dos riscos no negócio e a probabilidade de materialização desses riscos, o nível do risco foi designado numa escala de:

- 1 - Muito Baixo;
- 2 – Baixo;
- 3 – Médio;
- 4 – Alto;
- 5 - Muito Alto;

Assim sendo, a matriz de risco definida para realização da Análise de Risco é:



A matriz de risco permite identificar quais são os riscos que deverão receber mais atenção e quais os prioritários no seu tratamento. A matriz é composta pela dimensão da probabilidade e do impacto, sendo que a relação entre os dois se traduz no valor do risco.

O valor do risco pode variar entre 1 e 25 (quantitativamente) ou entre Muito Baixo e Muito Alto (qualitativamente). Todos os riscos que se situem até ao valor 4 ou Baixo serão riscos aceites, porque a sua probabilidade de ocorrência e o potencial impacto representam consequências muito reduzidas para a organização. Todos os valores que se situarem a partir de 5 ou Médio terão de ser tratados, uma vez que a sua probabilidade de ocorrência e o impacto potencial podem representar consequências negativas relevantes para a organização.

2.1 Exemplo de um Plano de Segurança

Plano de Segurança.pdf

2.2 Exemplo de um Relatório Anual

Relatório Anual.pdf

Anexos

A - Matriz de Responsabilidade do Ponto de Contacto Permanente

As responsabilidades atribuídas ao Ponto de Contacto Permanente são (Decreto-Lei no 65, 2021; República, 2021):

- Assegurar os fluxos de informação de nível operacional e técnico com o Centro Nacional de Cibersegurança;
- A articulação intersectorial, incluindo a eficácia da resposta a incidentes de segurança com impacto a nível dos setores;
- A obtenção de informação operacional e técnica, na sequência de notificação de incidentes com impacto relevante ou substancial submetida pela mesma ou outra entidade;
- A obtenção e atualização de informação de situação integrada no contexto de um incidente com impacto relevante ou substancial;
- A partilha de informação quando estejam ativados planos de emergência de proteção civil diretamente relacionados ou com impacto ao nível da segurança do ciberespaço, bem como de planos no âmbito do planeamento civil de emergência do ciberespaço ou dos planos de segurança das infraestruturas críticas nacionais ou europeias;
- A operacionalização dos procedimentos fixados no âmbito de um plano de emergência de proteção civil quando tenham impacto no funcionamento das redes e sistemas de informação, ou do planeamento civil de emergência do ciberespaço;
- A receção das instruções técnicas emitidas pelo CNCS no âmbito do RJSC;
- A operacionalização dos procedimentos fixados no âmbito dos planos de segurança;
- Disponibilidade contínua de 24 horas por dia e de sete dias por semana;
- Tomar ações nos vários cenários previstos e categorizados que possam surgir.

B - Matriz de Responsabilidade do Responsável de Segurança

As responsabilidades atribuídas ao Responsável de segurança são (Decreto-Lei nº 65, 2021; República, 2021):

- Reportar à gestão de topo;
- Reencaminhar internamente as solicitações das Autoridades;
- Traduzir os objetivos da entidade em requisitos de segurança de informação;
- Assegurar a definição, implementação e manutenção da estratégia de segurança da informação e cibersegurança de forma holística e estruturada;
- Garantir a conformidade com a legislação e regulamentação aplicável como o RJSC e RJSC e RGPD;

- Garantir a implementação de boas práticas de segurança da informação e cibersegurança;
- Definir e identificar requisitos e medidas de segurança da informação e cibersegurança;
- Assegurar o desenvolvimento e implementação de políticas, processos e procedimentos de segurança da informação e cibersegurança;
- Definir e implementar estratégias de avaliação e de resposta aos riscos;
- Acompanhar e avaliar a execução nomeadamente dos processos de Gestão de Alterações e de Gestão de Incidentes;
- Acompanhar auditorias de segurança da informação e cibersegurança e garantir a implementação de ações de melhoria para mitigação do risco;
- Suportar a entidades na estratégia, desempenho e monitorização dos sistemas aplicacionais e infraestrutura;
- Promover ações de sensibilização/consciencialização em cibersegurança junto dos colaboradores da entidade;
- Analisar e identificar medidas adequadas para implementação na entidade;
- Acompanhar todo o processo de implementação,
- Definir prioridades e atividades de melhoria continua, que garantam que a entidade está preparada em termos de segurança da informação e cibersegurança;
- Promover processos e procedimentos necessários para ativação do ponto de contacto permanente;
- Assinar e responsabilidade sobre a elaboração dos Inventários de ativos e Listas de ativos;
- Assinar e responsabilidade sobre a elaboração dos Planos de segurança;
- Assinar e responsabilidade sobre a elaboração dos Relatórios anuais.

C - Taxonomia dos Incidentes

Os incidentes podem ter as seguintes categorias de causas raiz (Centro Nacional de Cibersegurança, n.d.):

- Falha de sistema;
- Fenómeno natural;
- Erro humano;
- Ataque malicioso; e
- Falha no fornecimento de bens ou serviços por terceiro.

Sendo os efeitos produzidos:

Efeitos Produzidos	Tipo de Incidentes
Código Malicioso	Sistema Infetado Distribuição de *Malware*

	Servidor C2
	Configuração de *Malware*
Disponibilidade	Negação de Serviço
	Negação de Serviço Distribuída
	Configuração incorreta
	Sabotagem
	Interrupção
Recolha de Informação	*Scanning*
	Sniffing
	Engenharia Social
Intrusão	Compromisso de Conta Privilegiada
	Compromisso de Conta Não Privilegiada
	Compromisso de Aplicação
	Arrombamento
Tentativa de Intrusão	Exploração de Vulnerabilidade
	Tentativa de *Login*
	Nova assinatura de ataque
Segurança da Informação	Acesso não autorizado
	Modificação não autorizada
	Perda de dados
Fraude	Utilização indevida ou não autorizada de recursos
	Direitos de autor
	Utilização ilegítima de nome de terceiros
	Phishing
Conteúdo Abusivo	*SPAM*
	Discurso Nocivo
	Exploração sexual de menores, racismo e apologia da violência
Vulnerabilidade	Criptografia fraca
	Amplificador DDoS
	Serviços acessíveis potencialmente indesejados
	Revelação de informação
	Sistema vulnerável
Outro	Sem tipo Indeterminado