INSTITUTO SUPERIOR DE TECNOLOGIAS AVANÇADAS DE LISBOA

Mestrado em Informática

Dissertação para obtenção do Grau de Mestre em

Informática

A Gestão de Risco de Fornecedores na Garantia da Continuidade e Qualidade dos Processos das Organizações

Em Infraestruturas de Serviços Críticos

Marta Raquel Rosa Romão

Presidente: Professor Doutor Paulo André Reis Duarte Branco

Arguente: Professora Doutora Carla Sofia Rocha da Silva

Orientador: Professor Doutor Pedro Ramos dos Santos Brandão

Lisboa

Julho, 2025

ISTEC Lisboa

Instituto Superior de Tecnologias Avançadas de Lisboa

Campus Académico do Lumiar, Lisboa

Dissertação

Mestrado em Informática

Por Marta Raquel Rosa Romão

Dissertação de Mestrado apresentada para cumprimento dos requisitos necessários à obtenção do grau de mestre em Informática, realizada sob a orientação científica do Professor Doutor Pedro Ramos dos Santos Brandão.

Lisboa, 2025

Dedicatória

Aos meus pais, por me terem ensinado que a educação é o alicerce de todas as conquistas.

Ao meu marido, por ser o meu porto seguro em todas as etapas desta jornada.

Ao meu filho, Salvador, fonte inesgotável de inspiração, alegria e motivação.

Que este trabalho seja um exemplo do valor do esforço e da perseverança.

Índice

Índice de Figuras

Índice de Tabelas

Índice de Abreviaturas e Acrónimos

[1] Admin – Administrador

[2] ANACOM – Autoridade Nacional de Comunicações

[3] API - Application Programming Interface

[4] ASF - Autoridade de Supervisão de Seguros e Fundos de Pensões

[5] AWS - Amazon Web Services

[6] Botnet - Robot Network

[7] CCM - Cloud Controls Matrix

[8] CE – Comissão Europeia

[9] CIS – Critical Security Controls

[10] CISO - Chief Information Security Officer

[11] CNCS - Centro Nacional de Cibersegurança

[12] CNPD - Comissão Nacional de Proteção de Dados

[13] CSA - Cloud Security Alliance

[14] CSIRT - Computer Security Incident Response Teams

[15] CVEs - Common Vulnerabilities and Exposures

[16] DKIM - Domain Keys Identified Mail

[17] DLP - Data Loss Prevention

[18] DMARC - Domain-based Message Authentication, Reporting & Conformance

[19] DNS - Domain Name System

[20] DORA - Digital Operational Resilience Act

[21] DoS - Denial of Service

[22] DPIA - Data Protection Impact Assessment

[23] DSRM - Design Science Research Methodology

[24] ENISA - Agência da União Europeia para a Cibersegurança

[25] ERSE – Entidade Reguladora dos Serviços Energéticos

[26] EU-CyCLONe - European Cyber Crisis Liaison Organisation Network

[27] HTTPS - Hypertext Transfer Protocol Secure

[28] IDS – Intrusion Detection System

[29] InfoSec – Information Security

[30] IP - Internet Protocol

[31] IPS – Intrusion Prevention System

[32] ISO 27002 – International Organization for Standardization 27002

[33] ISO 31000 – International Organization for Standardization 31000

[34] ISO/IEC 27000 – International Organization for Standardization/International Electrotechnical Commission 27000

[35] ISPs – Internet Service Providers

[36] KPI – Key Performance Indicator

[37] KRI – Key Risk Indicator

[38] NDAs - Non-Disclosure Agreements

[39] NIS – Network and Information Systems

[40] NIS 2 - Network and Information Systems Directive 2

[41] NIST - National Institute of Standards and Technology

[42] NIST- CSF - National Institute of Standards and Technology – Cybersecurity Framework

[43] NIST SP 800-30 - National Institute of Standards and Technology Special Publication 800-30

[44] PME – Pequenas e Médias Empresas

[45] QNRCS - Quadro Nacional de Referência para a Cibersegurança

[46] RGPD - Regulamento Geral sobre a Proteção de Dados

[47] RPO - Recovery Point Objective

[48] RTO – Recovery Time Objective

[49] SC – Supply Chain

[50] SCM – Supply Chain Management

[51] SFTP - Secure File Transfer Protocol

[52] SIEM - Security Information and Event Management

[53] SLAs – Service Level Agreements

[54] SOPs – Standard Operating Procedures

[55] SPAM - Sending and Posting Advertisement in Mass

[56] SPF - Sender Policy Framework

[57] SQL - Structured Query Language

[58] SSO - Single Sign-On

[59] STAR - Security Trust & Assurance Registry

[60] TIC - Tecnologias da Informação e Comunicação

[61] TLS - Transport Layer Security

[62] UE – União Europeia

[63] VPN - Virtual Private Network

[64] WAFs - Web Application Firewalls

Resumo

Os sistemas de informação são cada vez mais um elemento fundamental da vida coletiva incluindo o Estado e de todas as organizações porque todos sem exceção tratam de dados.

Contudo, com a crescente externalização de serviços críticos e a integração de fornecedores em processos estratégicos das organizações surgem novos desafios no que respeita à salvaguarda da sua continuidade operacional, da segurança da informação e da garantia da qualidade dos serviços prestados.

Assim, partindo de uma abordagem sistemática baseada em práticas de gestão de risco reconhecidas, propõe-se um modelo para a gestão do ciclo de vida dos fornecedores assente em processos e subprocessos que contribuem decisivamente para a resiliência digital da organização e da sua cadeia de fornecimento garantindo a continuidade e qualidade dos processos organizacionais num contexto de ameaças crescentes e de alta complexidade tecnológica.

Palavras-chave: segurança de informação, gestão de risco, fornecedores, cadeia de fornecimento e continuidade de negócio.

Abstract

Information systems are an increasingly fundamental element of collective life, including the state, and of all organizations, because all of them, without exception, deal with data.

However, with the growing outsourcing of critical services and the integration of suppliers into organizations' strategic processes, new challenges have arisen about safeguarding their operational continuity, information security and guaranteeing the quality of the services provided.

Thus, using a systematic approach based on recognized risk management practices, we propose a model for supplier lifecycle management based on processes and sub-processes that make a decisive contribution to the digital resilience of the organization and its supply chain, guaranteeing the continuity and quality of organizational processes in a context of growing threats and high technological complexity.

Keywords: information security, risk management, suppliers, supply chain and business continuity.

1 Introdução

Este trabalho desenvolvido no âmbito da cibersegurança, tem como principal objetivo fornecer uma compreensão abrangente sobre a temática da gestão de risco de fornecedores na garantia da continuidade e qualidade dos processos das organizações, classificadas como Infraestruturas de Serviços Críticos, e propor a criação de uma abordagem por processo, através da criação de um modelo organizacional, como uma das abordagens possíveis a implementar num processo de gestão de risco de fornecedores nas organizações.

1.1 Objetivos Principais

a) Contextualizar a importância da gestão de risco de fornecedores destacando o impacto do risco no desempenho do normal funcionamento das organizações;
b) Apresentar as possíveis consequências de uma gestão inadequada do risco dos fornecedores procurando justificar a necessidade de investigação sobre este tema;
c) Estudar o papel crítico da gestão do risco de fornecedores e propor um novo modelo que permita garantir a continuidade e qualidade dos processos organizacionais.

Para atingir estes objetivos, foi definida uma metodologia que se encontra descrita neste capítulo.

2 Metodologia

2.1 *Design Science Research Methodology*

A *Design Science Research Methodology* (DSRM), doravante designada DSRM, é uma metodologia de pesquisa que visa a criação e avaliação de artefactos que podem incluir modelos, métodos e abordagens de modo a contribuir para uma possível solução de um problema identificado dentro de um campo de estudo com particular uso em áreas como a Engenharia, a Ciência da Computação, os Sistemas de Informação e a Cibersegurança onde a inovação e a aplicação prática são essenciais **Error! Reference source not found.**.

A DSRM segue um processo estruturado que é focado na resolução de problemas através da criação de artefactos inovadores e/ou do desenvolvimento de soluções com aplicabilidade prática e impacto real permitindo a sua melhoria contínua através de ciclos de avaliação e desenvolvimento [1] [2].

Em primeiro lugar, será efetuada uma análise exaustiva da literatura para estabelecer o quadro teórico e obter uma compreensão mais profunda dos conceitos relacionados com a gestão de risco de fornecedores.

A metodologia para esta investigação envolverá uma abordagem abrangente à recolha e análise de dados sobre a importância da gestão de risco de fornecedores na garantia da continuidade e qualidade dos processos organizacionais. Para o efeito, será utilizado um método de investigação qualitativo.

2.2 Aplicabilidade da metodologia *Design Science Research Methodology*

Para o desenvolvimento desta dissertação, a metodologia utilizada foi usada para desenvolver um artefacto específico, uma abordagem por processo, que tem por objetivo que qualquer organização classificada como Infraestrutura de Serviços Críticos possa tomar decisões informadas em todas as fases do processo de gestão de risco, de modo a mitigar os riscos relacionados com:

a) A seleção do fornecedor;
b) A contratação do fornecedor;
c) A definição de requisitos de segurança;
d) A monitorização contínua do desempenho do fornecedor;
e) A cessação do contrato.

A Aplicabilidade da metodologia DSRM neste estudo inclui os seguintes elementos:

2.2.1 **Identificação do Problema** - definição do problema, apresentação da sua importância e dos benefícios esperados da solução.

A crescente dependência de fornecedores, parceiros e terceiras partes especialmente na vertente tecnológica, aumenta a vulnerabilidade das organizações a ciberataques e violações de dados. Estudos indicam que falhas na gestão de risco de fornecedores podem levar a interrupções nas operações e comprometer a segurança e qualidade dos dados e sistemas [3].

a) Problema: a ausência de um modelo estruturado e eficaz baseado numa abordagem por processo, que permita às organizações avaliar e gerir os riscos de fornecedores, parceiros e terceiras partes, sem afetar a continuidade e qualidade dos processos organizacionais.
b) Motivação: a importância crítica para as organizações, classificadas como Infraestruturas de Serviços Críticos, em garantir a continuidade de negócio, a proteção de dados pessoais e a segurança dos seus sistemas. Para além disso, a gestão de risco de fornecedores é essencial para mitigar os impactos negativos de possíveis falhas ou ciberataques na cadeia de fornecimento [4].

A importância deste estudo é acentuada pelas exigências regulatórias da União Europeia, que requerem que as organizações implementem medidas robustas de segurança das redes e dos sistemas de informação (Diretiva (UE) n.º 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). Como é o caso da Diretiva NIS que estabelece os requisitos para a segurança das redes e sistemas de informação [5].

2.2.2 **Definição dos Objetivos da Solução** – definição de uma abordagem por processo que possa ser aplicada de forma eficaz em organizações classificadas como Infraestruturas de Serviços Críticos, assegurando a conformidade com as normas e regulamentos em execução na União Europeia.

a) Objetivo: definir uma abordagem por processo para a gestão de risco de fornecedores que seja aplicável a infraestruturas de serviços críticos.
b) Critérios de sucesso: o sucesso da abordagem por processo será medido através de indicadores específicos tais como a (1) redução dos riscos associados a fornecedores, parceiros e terceiras partes através da melhoria da continuidade e qualidade dos processos organizacionais, (2) redução do número de incidentes de cibersegurança desencadeados a partir de fornecedores, parceiros ou terceiras partes da organização.

2.2.3 Desenvolvimento da solução – desenvolver uma abordagem por processo baseada nas melhores práticas e nas *frameworks* de referência na área de cibersegurança para a gestão de risco de fornecedores, com a definição de um modelo estruturado, em consonância com o conhecimento adquirido através de pesquisa empírica.

A abordagem por processo será constituída por quatro subprocessos e respetivas atividades que incluem componentes como os critérios de seleção de fornecedores, os métodos de avaliação de risco e as estratégias de mitigação. O primeiro subprocesso dedicado ao planeamento do processo, o segundo subprocesso dedicado à fase de avaliação e contratualização dos fornecedores, o terceiro subprocesso considerado o subprocesso para a gestão do contrato, e o quarto e último subprocesso será dedicado ao plano de saída e de transição do fornecedor assim como, a análise do seu comportamento ao longo da vigência do contrato com a entidade contratante.

a) Demonstração: Apesar da ausência de um estudo de caso prático para ilustrar a implementação, a dissertação apresenta uma análise teórica detalhada sobre a abordagem por processo, explicando os seus fundamentos e aplicabilidade.

   Esta opção justifica-se por vários motivos: privilegia-se a consolidação de uma base teórica sólida antes da aplicação prática; evita-se a limitação da abordagem a um caso específico, permitindo uma visão mais genérica e aplicável a diferentes organizações e respetivos setores; e reconhecem-se as limitações na partilha de dados por parte das organizações que inviabilizam, no presente momento, a realização de um estudo de caso detalhado.

   Além disso, a dissertação abre caminho para estudos futuros, nos quais a implementação prática poderá ser avaliada em contextos concretos.

2.2.4 Comunicação da Solução – documentar e comunicar os resultados do trabalho de investigação assegurando que as contribuições deste estudo são disseminadas de forma eficaz.

a) Documentar: fundamentar, no âmbito da cibersegurança, o desenvolvimento de uma abordagem por processo através da escrita de um modelo estruturado na vertente da gestão de risco de fornecedores e dirigido a organizações classificadas como Infraestruturas de Serviços Críticos.

Assim sendo, pretende-se com este estudo fornecer uma visão abrangente e aprofundada da importância da gestão de risco de fornecedores na garantia da continuidade e qualidade dos processos organizacionais, contribuindo através da aplicação da DSRM [6] para uma

compreensão holística deste aspeto crítico, a gestão de fornecedores, na gestão organizacional e nos efeitos sistémicos que produz ao longo de toda a sua cadeia.

3 Enquadramento Teórico

Ao longo deste capítulo apresentam-se os principais conceitos e *frameworks* desenvolvidos para a avaliação de risco em sistemas de informação e que serviram de base ao desenvolvimento deste estudo.

3.1 Cibersegurança

Universalmente não há uma definição aceite que reúna as várias dimensões de cibersegurança.

Existem vários autores que definem cibersegurança de forma abrangente, isto é, definem a cibersegurança como forma de assegurar a continuidade da sociedade de informação, protegendo as suas estruturas, a informação, os dispositivos e *software* através de medidas técnicas e não técnicas [7].

Por isso, a discussão sobre cibersegurança sempre foi e estará influenciada pela revolução de informação, pelo que a definição nunca será estática isto porque os aspetos técnicos também estão em constante evolução [7].

Segundo a ISO 27002, a Segurança da Informação é alcançada através da implementação de um conjunto de controlos técnicos e organizacionais, políticas, processos, procedimentos, *hardware* e *software*. Para endereçar os objetivos específicos de segurança e de negócio, as organizações devem definir, implementar, monitorizar, rever e melhorar os vários aspetos mencionados anteriormente [8].

A Segurança da Informação desempenha um papel crucial na proteção dos ativos de informação e das operações das organizações. Se for gerida e implementada corretamente, contribui de forma significativa para a reputação e aumento do valor da organização [9].

Os termos Segurança de Informação (InfoSec) e Cibersegurança são frequentemente confundidos e usados indistintamente [10]. A principal diferença entre Cibersegurança e Segurança de Informação é que a Cibersegurança apenas tem como âmbito de atuação o ciberespaço (informação digital), enquanto a Segurança de Informação tem um âmbito mais geral de atuação, ou seja, a proteção da informação de todos os tipos e em todos os ambientes [11].

O *National Institute of Standards and Technology* (NIST) - agência do Departamento de Comércio dos Estados Unidos, que se dedica ao desenvolvimento de tecnologias, padrões e diretrizes em diversas áreas e é especialmente reconhecida pelas suas contribuições no campo da cibersegurança - define um ciberataque como sendo uma atividade maliciosa, que utiliza o

ciberespaço para atingir um alvo com o intuito de destruir, degradar, paralisar, recolher informação ou controlar com finalidades ilegítimas um sistema de informação [12].

Os ciberataques podem ser realizados por indivíduos ou organizações criminosas utilizando diferentes técnicas. A Agência da União Europeia para a Cibersegurança (ENISA) - criada para promover um elevado nível comum de cibersegurança em toda a União Europeia (UE), ajudando os Estados-Membros, as instituições da UE e outros *stakeholders* a lidar com os desafios da cibersegurança [13] - identificou num relatório publicado em Novembro de 2022, que os *Supply--Chain attacks* foram uma das tipologias de ataque mais exploradas em 2022 [14].

3.2 *Supply Chain Attack* – caraterização e principais vetores de ameaça

Um *supply chain attack* pode ser considerado como um ataque que tem como objetivo comprometer uma qualquer organização através da sua cadeia de fornecedores, com o objetivo de aceder aos seus sistemas e redes corporativos. O principal propósito passa pela obtenção de acesso não autorizado a sistemas e redes corporativas, muitas vezes contornando os mecanismos de defesa diretos da organização-alvo [15] [16]. Este tipo de ataque constitui uma das formas mais sofisticadas e impactantes das ameaças à segurança digital.

A cadeia de fornecedores é uma porta de entrada em qualquer organização, com a particularidade de que é uma porta que não pode ser fechada porque muitas das organizações dependem de terceiras partes para operar e manter a sua atividade e, por conseguinte, é necessário recorrer a modelos para proteger a segurança da informação e para gerir os riscos da organização garantido a continuidade do negócio.

Para concretizar este tipo de ataque existem diferentes formas de o executar. Entre os principais vetores de ataque destacam-se:

3.2.1 Comprometimento de *Software* e Infraestruturas Digitais

Um dos meios possíveis de ataque é o comprometimento do *software* e das redes corporativas. Para isso, uma das abordagens mais recorrentes envolve a manipulação maliciosa de *software* legítimo durante o seu ciclo de desenvolvimento, de distribuição ou atualização. Esta técnica, conhecida como *software supply chain compromise*, é particularmente perigosa, dado que afeta simultaneamente várias entidades dependentes da mesma aplicação ou serviço, pondo em causa a confiança depositada nos fornecedores de *software*.

3.2.2 Técnicas de Engenharia Social: *Phishing* e *Ransomware*

Outro dos meios possíveis é realizar ataques de *phishing* ou *ransomware* explorando dessa forma o fator humano considerado o elo mais fraco da cibersegurança.

O *Phishing* é considerado uma técnica de engenharia social que se traduz numa tentativa fraudulenta de obter informações sensíveis simulando ser uma entidade confiável falsificando identidades ou comunicações com o intuito de ludibriar os utilizadores e induzi--los a fornecer informações sensíveis como credenciais de acesso ou dados financeiros [17]. Este tipo de ataque serve frequentemente de vetor inicial para ataques mais complexos e pode ocorrer através de múltiplos canais – correio eletrónico, mensagens SMS, redes sociais ou chamadas telefónicas.

O *Ransomware* é um tipo de ciberataque em que o atacante infeta os sistemas ou redes da vítima com *software* malicioso, encriptando dados ou bloqueando sistemas com o objetivo de que a vítima pague um resgate em troca do desbloqueio do acesso aos mesmos. Quando integrado num ataque à cadeia de fornecedores, pode propagar-se rapidamente entre diferentes entidades ligadas entre si, amplificando o seu impacto.

3.2.3 Inserção de *Hardware* Malicioso

Por fim, outro dos meios possíveis é através da introdução de *hardware* malicioso ou de componentes de *hardware* adulterados nos sistemas de uma organização de forma deliberada. Estes dispositivos podem incluir, por exemplo, *USB drives* com código malicioso, placas-mãe modificadas ou equipamentos de rede comprometidos.

A complexidade deste vetor reside na dificuldade de deteção e na natureza persistente do acesso que proporciona, muitas vezes atuar abaixo da visibilidade dos mecanismos tradicionais de segurança [18].

4 Evidência empírica sobre ataques à cadeia de fornecedores

O Fórum Económico Mundial de 2025 salientou que 54% das grandes organizações identificam os desafios associados à cadeia de fornecedores como o principal entrave para alcançar a resiliência digital. Esta constatação reflete a crescente complexidade das redes de fornecimento globais, que se tornaram vetores críticos de risco no atual contexto de cibersegurança organizacional [19].

Entre 2021 e 2023, registou-se um aumento de 431% de ataques dirigidos à cadeia de fornecedores, com previsões que indicam a continuidade dessa tendência até ao final de 2025 [20].

Segundo o relatório de 2025 da *SecurityScorecard*, 35,5% das violações de segurança registadas em 2024 estiveram relacionadas com terceiros, nomeadamente através de relações contratuais com fornecedores [21]. Este valor poderá, contudo, ser inferior ao real, tendo em conta que muitos incidentes podem ser incorretamente classificados nas bases de dados institucionais.

Complementarmente, um inquérito publicado pela *SC Media* revelou que 60% das organizações reportaram incidentes de cibersegurança originados por terceiros com acesso privilegiado a sistemas internos, refletindo vulnerabilidades críticas na gestão de identidades e acessos, sobretudo quando se verificam práticas inadequadas de partilha de credenciais e ausência de segregação de privilégios [22].

Por sua vez, um estudo elaborado pela empresa de cibersegurança *BlueVoyant* corrobora esta tendência, indicando que mais de 81% das organizações sofreram impactos negativos provenientes de violações na sua cadeia de fornecedores no último ano, com uma média de 3,7 incidentes por organização [23]. Estes dados demonstram a frequência dos ataques, a sua capacidade de repetição e disseminação transversal.

Quanto à distribuição setorial, os dados disponíveis apontam que os setores mais afetados por incidentes relacionados com terceiros incluem o retalho e a hospitalidade (52,4%), a tecnologia (47,3%) e a energia/*utilities* (46,7%), evidenciando a exposição de domínios que operam com infraestruturas críticas ou serviços essenciais [21].

5 Segurança da informação – os principais pilares

Reconhecida como a base da segurança da informação (Stallings, 2017), a tríade CIA (*Confidentiality, Integrity, Availability*) é constituída por três princípios estruturantes - confidencialidade, integridade e disponibilidade que orientam a definição de políticas, procedimentos e controlos técnicos no domínio da cibersegurança.

A crescente complexidade das ameaças e das exigências regulatórias conduziu à inclusão de mais dois princípios, autenticidade e não-repúdio, os quais reforçam a fiabilidade e a responsabilização no tratamento da informação (ISO/IEC 27002, 2022).

5.1 Confidencialidade

A confidencialidade visa assegurar que a informação é acessível apenas por pessoas, sistemas ou entidades autorizadas, protegendo os dados contra acessos não autorizados[1]. A sua concretização prática no seio das organizações pode incluir mecanismos como controlo de acessos, segregação de funções e/ou encriptação de dados para proteger informações pessoais ou sensíveis. Trata-se de um dos pilares mais críticos da segurança da informação, sobretudo no tratamento de dados pessoais ou sensíveis [24].

5.2 Integridade

A integridade assegura que a informação se mantém correta e completa ao longo do tempo garantindo que os dados não sofrem alterações de forma indevida, isto é, não autorizada, acidental ou maliciosa. Este princípio é essencial para garantir a confiança na informação considerada para a tomada de decisões [26].

Para isso, recorre-se a mecanismos como o uso de assinatura digital para verificar que uma mensagem ou ficheiro não foi modificado, ou o controlo de versões dos ficheiros e/ou as somas de verificação (*checksums*) dos dados antes da sua partilha ou armazenamento. Se ao recalcular aquando do seu recebimento ou da sua recuperação o valor obtido for o mesmo, considera-se que as informações não sofreram alterações e, por conseguinte, não estão corrompidas.

A integridade envolve a manutenção da consistência, exatidão e fiabilidade dos dados durante todo o seu ciclo de vida[2].

5.3 Disponibilidade

A disponibilidade refere-se à garantia de que os utilizadores autorizados devem poder aceder aos dados e aos sistemas de informação quando necessário[3]. A indisponibilidade de sistemas críticos pode ter consequências severas podendo comprometer a continuidade operacional, sendo por isso necessário a implementação de planos de recuperação, redundância de sistemas e proteção contra ataques DoS (*Denial of Service*) **Error! Reference source not found.**.

[1] *"Confidentiality ensures that sensitive information is accessed only by an authorized person and kept away from those not authorized to possess them."* ***Error! Reference source not found.***.
[2] *"Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire lifecycle."* [26].
[3] *"Availability ensures that authorized users have access to information and associated assets when required."****Error! Reference source not found.***.

5.4 Autenticidade

A autenticidade refere-se à verificação da identidade dos utilizadores, dos sistemas ou dados, garantindo que estes não foram adulterados ou falsificados e que se mantêm genuínos[4]. A autenticidade garante assim que as identidades das partes envolvidas numa comunicação ou transação sejam verificadas. Este princípio é importante para prevenir acessos não autorizados e garantir que a origem da informação é confiável [27]. A autenticidade pode ser assegurada através de mecanismos de autenticação multifator, certificados digitais, e/ou protocolos criptográficos.

5.5 Não-repúdio

O princípio de não-repúdio permite assegurar que nenhuma parte envolvida na realização de uma ação possa negar a sua autoria ou responsabilidade e, desse modo, garantir a responsabilização das partes envolvidas e a integridade das comunicações e dos registos.

Para isso, recorre-se a mecanismos como as assinaturas digitais, os registos de *logs* e/ou os protocolos de comunicação seguros. O não-repúdio fornece a prova da origem e da entrega dos dados, garantindo que o remetente não pode negar o facto de ter realizado a ação[5].

6 Contexto legal e regulamentação nacional

6.1 Conformidade e Segurança

Por definição, "estar em conformidade é quando a organização cumpre os requisitos mínimos de regulamentos específicos num determinado momento." [31]

As atividades de conformidade ocorrem num momento específico e têm como objetivo verificar se os controlos e os procedimentos definidos e documentados pela organização estão devidamente implementados e em conformidade legal no momento em que essa verificação ocorre. Essa verificação deve ser efetuada por uma equipa interna ou por uma entidade externa como as entidades auditoras ou reguladoras. Uma vez cumpridos os requisitos, considera-se que a conformidade foi atingida.

[4] *"Authenticity assures that users can verify the origin of information and that it has not been falsified."* [29].
[5] "*Non- repudiation provides proof of the origin and delivery of data, ensuring that the sender cannot deny having sent the message." [30].*

Por contraponto, a segurança da informação é "uma atividade contínua, isto é, uma atividade que ocorre continuamente e não uma atividade que ocorre num determinado momento." [31]

Nesse sentido, a segurança da informação por se tratar de um processo contínuo exige uma contínua monitorização, uma revisão periódica dos seus processos, políticas e normas e melhorias contínuas que espelhem a adaptação da organização às mudanças de contexto e às novas ameaças.

6.2 Infraestruturas Críticas

O aumento do cibercrime de forma generalizada e em particular na UE, levou ao surgimento do decreto-lei 46/2018 [32] onde é definido o Regime Jurídico da Segurança do Ciberespaço que mais tarde é regulamentado pelo decreto-lei 65/2021 [33] como forma de enfrentar esta ameaça e poder inverter esta tendência, obrigando as organizações a cumprir requisitos no que à segurança e à utilização do ciberespaço diz respeito.

A Comissão Europeia (CE) define Infraestruturas Críticas como ativos ou sistemas essenciais à manutenção das funções vitais da sociedade, cujo qualquer dano causado sobre o funcionamento das mesmas, terá um impacto significativamente negativo para a segurança da UE e sobre o bem-estar dos seus cidadãos [34].

O NIST [35], apresenta uma visão mais ampla, definindo estas infraestruturas como sendo ativos físicos ou virtuais de importância vital para os Estados Unidos, cuja incapacitação ou destruição se traduz num impacto debilitante para o país, na segurança económica, na saúde pública interna ou em qualquer combinação destas áreas.

Uma das suas publicações é o *NIST Cybersecurity Framework* (NCF) [36] que tem como principais objetivos apoiar as organizações responsáveis por infraestruturas críticas [37] a gerir o risco neste campo e a definir e implementar uma gestão de risco prudente e adequada à criticidade destas infraestruturas. Esta *framework* foi elaborada em 2013, publicada em 2014, revista e atualizada em 2018 com novas medidas e controlos para enfrentar as ameaças associadas a novas tecnologias.

O Estado português, através da Lei 46/2018 [32] define uma infraestrutura crítica como sendo a componente, sistema ou parte deste, situado em território nacional, que é essencial para a manutenção de funções vitais para a sociedade, saúde, segurança e o bem-estar económico ou social, cuja perturbação ou destruição teria um impacto significativo, dada a impossibilidade de continuar a assegurar essas funções.

6.3 Serviços Essenciais

O Decreto-Lei n.º 65/2021, publicado a 30 de julho de 2021, alterou e alargou o regime de segurança das redes e sistemas de informação, alinhando-o com a Diretiva (UE) 2016/1148 (Diretiva NIS) e alargando o espectro de setores considerados fundamentais para o funcionamento da economia [33]. Adicionalmente ao setor energético, ao setor dos transportes, ao setor do fornecimento e distribuição de água potável, e ao setor da banca foi incluído o setor da saúde abrangendo os prestadores de cuidados de saúde, incluindo hospitais e outras instituições de saúde; o setor das infraestruturas digitais, incluindo os fornecedores de serviços digitais, como os motores de pesquisa, serviços de computação em nuvem e plataformas de comércio eletrónico; as infraestruturas do mercado financeiro, incluindo instituições financeiras que desempenham um papel crítico na economia e, por último, a administração pública que inclui entidades governamentais e serviços públicos que gerem dados sensíveis e operam serviços essenciais.

A classificação dos serviços como essenciais permite associar esses mesmos serviços a operadores e organizações com responsabilidade sobre os mesmos, tendo estes operadores o dever de zelar pela segurança das infraestruturas que suportam o funcionamento destes mesmos serviços.

A CE consciente da necessidade de proteger as infraestruturas críticas europeias, aprovou a 8 de dezembro de 2008 a diretiva 2008/114/CE [38] relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção.

6.4 Operadores de Serviços Essenciais

No que respeita a Operadores de Serviços Essenciais, segundo o decreto-lei 46/2018 [32] trata-se de uma entidade pública ou privada que presta um serviço essencial, enquadrada nos setores supramencionados, suportados em infraestruturas que dependem destas para funcionarem. Anualmente, é atualizado pelo Centro Nacional de Cibersegurança (CNCS) a lista dos operadores considerados como operadores de serviços essenciais.

Quanto aos Prestadores de Serviços Digitais, segundo o decreto-lei 46/2018 [32], é uma pessoa coletiva que presta um serviço digital, a saber, serviço de *e-commerce* ou serviço de computação em nuvem.

O Decreto-Lei n.º 65/2021, por sua vez, veio expandir o âmbito dos operadores de infraestruturas críticas passando a incluir os setores adicionais mencionados acima. Este decreto-lei adapta o ordenamento jurídico português às exigências da Diretiva NIS e reforça a segurança das redes e sistemas de informação em setores críticos [33].

7 Risco – Um conceito amplo

A definição de risco é abrangente e pode variar conforme o contexto referindo-se geralmente como sendo a possibilidade de ocorrência de um evento ou condição que possa provocar um impacto positivo ou negativo nos objetos medindo-se em termos de probabilidade e impacto.

Segundo a ISO 31000 [39], o risco é definido como o "efeito da incerteza nos objetivos" que pode provocar efeitos positivos e negativos designados respetivamente como oportunidades e ameaças.

Segundo a ISO/IEC 27000 [27], o risco é definido como a "potencial ocorrência de um evento que pode causar danos ou perda".

Segundo o NIST SP 800-30 [40], o risco é "uma função da probabilidade de um determinado evento ameaçador ocorrer e do impacto adverso que o evento teria sobre a organização".

Ambas as definições têm na componente do risco, a noção de probabilidade, de impacto e de incerteza.

O apetite ao risco por sua vez, está associado a uma pré-disposição em assumir determinados riscos, independentemente da capacidade de suportar o seu impacto, caso o valor definido como sendo o limite para o apetite seja ultrapassado.

7.1 Risco na Gestão de Fornecedores

Na gestão de risco de fornecedores, o risco envolve a avaliação da probabilidade de ameaças no campo da cibersegurança e o impacto potencial que estas podem ter sobre a integridade, disponibilidade e confidencialidade dos dados e sistemas de informação. Uma gestão eficaz do risco de fornecedores deve incluir:

a) A identificação e avaliação dos riscos associados aos fornecedores e às suas cadeias de fornecimento;
b) A implementação de medidas e controlos com o objetivo de reduzir a probabilidade e de atenuar os impactos dos riscos,
c) O acompanhamento e a monitorização contínua dos riscos e da medição da eficácia dos controlos implementados.

8 Gestão de Risco de Fornecedores

No contexto atual em que as infraestruturas de serviços críticos atuam num ambiente global, interdependente e interconectado prevê-se que as organizações dependam gradualmente de mais fornecedores, parceiros e terceiras partes para fornecerem bens e serviços essenciais à sua operação.

Consequentemente, tende-se a prever que o aumento gradual da dependência de mais fornecedores, introduza um aumento significativo do risco, uma vez que qualquer perturbação ou interrupção na cadeia de fornecimento pode causar efeitos na capacidade de resposta da organização. Em simultâneo, pelo facto de as organizações atuarem num ambiente global e de interconexão entre si, também os seus fornecedores, parceiros e terceiras partes, podem sofrer com os efeitos em cadeia na sua capacidade de resposta.

A gestão de risco de fornecedores é um componente crítico para garantir a continuidade e a qualidade dos processos nas organizações enfrentando desafios significativos na avaliação e mitigação de riscos associados aos seus fornecedores [41]. Este processo tem um impacto direto na capacidade de uma qualquer organização conseguir salvaguardar a fiabilidade, a consistência e a qualidade da sua cadeia de fornecimento, pelo que é essencial gerir proactivamente os potenciais riscos que possam surgir.

Por definição, a gestão de risco de fornecedores é o processo de determinação dos potenciais riscos associados a um determinado fornecedor e a adoção de medidas adequadas para minimizar o impacto desses riscos na organização.

Consiste na implementação de estratégias para gerir os riscos diários e excecionais ao longo da cadeia de fornecedores com base na avaliação contínua dos riscos, com o objetivo de reduzir as vulnerabilidades como eventos de roubos, extravios e acidentes e garantir a continuidade do negócio. Uma boa gestão de riscos ajuda não só a minimizar os eventos com efeitos negativos associados a esta atividade, mas também a identificar os riscos positivos para catapultar novas oportunidades.

Supply Chain Management (SCM) [42] é um meio importante para aprimorar os fluxos de produtos, serviços e informações, proporcionando custos reduzidos e entregas mais ágeis e confiáveis, a fim de agregar valor para o cliente final e criar vantagens comerciais competitivas a longo prazo. Constata-se que as vulnerabilidades da *Supply Chain* (SC) estão ligadas aos riscos, no sentido de que algo é passível de ser perdido ou danificado [43].

A gestão de riscos – que contempla a avaliação do risco – combina cultura, sistemas e processos empreendidos por uma organização para coordenar a identificação e a gestão do risco, sendo que uma correta gestão de riscos prevenirá danos ou reduzirá o efeito dos riscos [44].

A gestão de riscos é uma área em acelerado desenvolvimento, envolvendo diferentes pontos de vista sobre o seu conceito e conteúdo, sobre como deve ser realizada e com que objetivo. Porém, houve necessidade de normas para estabelecer concordância em relação a terminologias, processo de implementação, estrutura e objetivos [45]. Posto isso, torna-se importante que após a fase de identificação e recolha de informação, os responsáveis pela gestão de risco tenham instrumentos que os auxiliem a agrupar o risco em categorias e nível de criticidade, e com base na sua classificação terem uma visão holística e integrada dos riscos existentes e com base nisso, definirem a priorização do seu tratamento, aceitação ou mitigação [46].

Este processo requer por parte das organizações um conhecimento abrangente do contexto interno e externo dos seus fornecedores, exige o envolvimento da organização no sentido de desenvolver estratégias de mitigação para os riscos identificados, a definição e apresentação de planos de contingência e a implementação de métricas de desempenho que permitam acompanhar e monitorizar o desempenho dos fornecedores. Por conseguinte, este processo enfatiza a necessidade de as organizações gerirem proactivamente os riscos dos fornecedores para salvaguardar a continuidade e a qualidade dos seus processos.

No contexto atual, as organizações estão gradualmente mais dependentes de fornecedores externos para a prestação dos seus serviços, o que as torna por sua vez vulneráveis e expostas a um conjunto de riscos nos quais se inclui as interrupções na cadeia de fornecimento, a instabilidade financeira, as preocupações éticas e de reputação da marca. Por isso, a compreensão do contexto tende a ser decisiva para as organizações mitigarem os riscos e garantirem a continuidade e qualidade dos seus processos.

9 Modelos e Standards de Segurança – Uma perspetiva abrangente

9.1 *National Institute of Standards and Technology - Cybersecurity framework*

O quadro de cibersegurança do *National Institute of Standards and Technology* (NIST-CSF) foi criado em resposta ao *Cybersecurity Basics 47* da Ordem Executiva Presidencial dos EUA 13636, cujo objetivo era reforçar a segurança das infraestruturas críticas do país. Embora se destine a infraestruturas críticas foi também adotado por muitas empresas privadas.

O seu objetivo consiste na definição de um conjunto padronizado de princípios, objetivos e terminologias, com vista ao reforço da segurança da informação e ao aprimoramento da capacidade organizacional de resposta, mitigação e remediação face a potenciais incidentes de cibersegurança. A adoção de uma abordagem comum proporciona às equipas de segurança da informação uma base mais sólida e coerente para a tomada de decisões estratégicas. Assim, organizações que implementem metodologias alinhadas com este referencial, independentemente do setor de atividade, conseguem estruturar de forma eficaz os seus processos de prevenção e mitigação de ameaças.

O NIST-CSF foi introduzido pela primeira vez em 2014, atualizado para a versão 1.1 em 2018 e, posteriormente, para a versão 2.0 em fevereiro de 2024. Esta última versão marca uma evolução significativa na abordagem da gestão de risco em vários sectores oferecendo um conjunto universal de orientações para ajudar as organizações a mitigar os riscos no quadro da cibersegurança [49].

A NIST CSF assenta em três tipos de componentes: os componentes que compõem a sua estrutura, as camadas de implementação e os perfis [50]. Assim, com a introdução de uma sexta função essencial, “Governar”, a sua estrutura passou a organizar-se em seis funções principais: Governar, Identificar, Proteger, Detetar, Responder e Recuperar, sendo as últimas cinco as suas funções originais, expandindo assim o seu total para 6 funções.

Cada uma destas funções agrega um conjunto de atividades específicas, classificadas em categorias e subcategorias, que visam mitigar os riscos associados à cibersegurança. Estas categorias incluem descrições detalhadas das melhores práticas, orientações para resposta a incidentes e mecanismos de recuperação eficaz perante eventos de segurança.

9.1.1 As Seis Principais Funções - NIST CSF

O NIST-CSF apresenta uma abordagem para a gestão de risco que contém seis funções principais: Governar, Identificar, Proteger, Detetar, Responder e Recuperar.

Figura 1 - As seis funções principais da NIST-CSF. [51]

Cada função compreende várias categorias, 22 no total, que por sua vez incluem 106 subcategorias que permitem mapear requisitos e controlos a serem cumpridos, bem como referências informativas. Cabe a cada organização adaptar a sua estrutura à estrutura proposta pela *framework* decidindo quais as funções, categorias e subcategorias que irá cumprir.

A **função 'Governar'**, que engloba elementos anteriormente incluídos na função 'Identificar' na versão 1.1, destaca-se agora como uma categoria distinta, realçando o seu papel essencial na supervisão estratégica, como mostra a Figura 1 [49].

Esta evolução pretende promover um maior envolvimento institucional, fortalecendo o sentido de responsabilidade organizacional relativamente à gestão de risco. Além disso, a formalização desta função pode criar uma oportunidade estratégica para mobilizar apoio institucional e justificar a necessidade de maior investimento no reforço das defesas da organização contra crescimento das ciberameaças [49].

Nesta função enquadram-se as categorias relacionadas com o (1) contexto organizacional, com a (2) estratégia da gestão de risco, com a (3) gestão de risco da cadeia de fornecedores, com os (4) papéis, responsabilidades e autoridades, com as (5) políticas, processos e procedimentos e por fim, com a (6) supervisão.

A categoria **Contexto Organizacional** (GV.OC) centra-se na importância de a organização compreender profundamente o seu enquadramento estratégico, operacional e regulatório, de

modo a integrar eficazmente a gestão de risco nas suas práticas de *governance*. Esta compreensão deve refletir-se na identificação clara da missão institucional, nos objetivos estratégicos e nos fatores internos e externos que influenciam o seu funcionamento [51].

Um dos principais objetivos desta categoria é assegurar que as partes interessadas – internas (como diretores, gestores, colaboradores e equipas técnicas) e externas (fornecedores, parceiros, clientes e entidades reguladoras) – sejam devidamente identificadas, e que as suas necessidades, requisitos e expectativas relativamente à segurança da informação sejam compreendidas e consideradas. Isso implica também o reconhecimento de que diferentes partes interessadas podem ter níveis distintos de tolerância ao risco, o que deve ser tido em conta na formulação das políticas e estratégias de cibersegurança.

Além disso, o contexto organizacional deve incorporar fatores como a estrutura e a cultura organizacional, a maturidade digital, os recursos disponíveis (tecnológicos, humanos e financeiros) e as exigências legais e regulamentares aplicáveis ao setor de atividade. A análise desse contexto permite alinhar a cibersegurança com os objetivos de negócio, identificar dependências críticas, avaliar o impacto de potenciais ameaças e garantir que as decisões relacionadas com o risco estão enraizadas numa perspetiva holística e realista.

A categoria **Estratégia de Gestão de Riscos** (GV.RM) estabelece a necessidade de definir, documentar e comunicar uma estratégia clara de gestão de riscos de cibersegurança que seja coerente com os objetivos da organização e com o seu contexto operacional. Esta estratégia deve incluir elementos como prioridades, restrições, tolerância ao risco e suposições-chave, funcionando como uma orientação para a tomada de decisão em matéria de segurança da informação.

A estratégia de gestão de risco deve refletir a realidade dinâmica do ambiente organizacional e tecnológico, incorporando análises atualizadas sobre ameaças emergentes, vulnerabilidades sistémicas, dependências tecnológicas e tendências regulatórias. Um dos pilares centrais desta categoria é a definição da tolerância ao risco, que consiste em determinar os níveis aceitáveis de exposição a ciberameaças, com base no apetite ao risco da organização e no potencial impacto para a sua operação, reputação e conformidade legal.

Além disso, a estratégia de gestão de risco deve ser formalmente aprovada pela gestão de topo e disseminada por toda a organização, promovendo o alinhamento transversal das atividades de cibersegurança com os objetivos de negócio. Esta abordagem possibilita que todos os níveis da organização compreendam o seu papel na mitigação do risco e atuem de forma coordenada.

A categoria **Gestão de Risco da cadeia de fornecedores** (GV.SC) aborda a necessidade da organização estabelecer uma abordagem estruturada e proativa para a gestão dos riscos de cibersegurança associados à cadeia de fornecedores. Esta categoria reconhece que as organizações dependem fortemente de fornecedores, prestadores de serviços, parceiros tecnológicos e outros terceiros que podem introduzir vulnerabilidades significativas nos seus ecossistemas digitais.

O objetivo central desta categoria é assegurar que a gestão de risco da cadeia de fornecedores seja integrada na estratégia global da organização. Para tal, é essencial identificar os elementos críticos da cadeia de valor digital, compreender as interdependências técnicas e contratuais, e avaliar continuamente os riscos decorrentes dessas relações.

As práticas recomendadas incluem a definição de critérios para a seleção e monitorização de fornecedores, a inclusão de cláusulas de cibersegurança nos contratos, e a realização de avaliações regulares para verificar o cumprimento dos requisitos estabelecidos. As organizações devem igualmente garantir que os fornecedores adotam padrões de segurança equivalentes aos seus e que os respetivos planos de resposta e recuperação a incidentes incluem cenários que envolvam terceiros.

Além disso, é fundamental estabelecer e manter canais de comunicação eficazes com os fornecedores, de modo a promover o diálogo e a partilha de informação sobre ameaças, vulnerabilidades e incidentes que possam afetar a segurança e a continuidade dos serviços prestados.

A categoria **Funções, Responsabilidades e Autoridades** (GV.RR) tem como principal propósito garantir que toda a estrutura interna da organização compreende o seu papel na proteção dos ativos digitais e na gestão do risco.

Uma governação eficaz da segurança da informação exige que as responsabilidades estejam formalmente atribuídas, com linhas de *report* estabelecidas, mecanismos de supervisão apropriados e critérios de responsabilização mensuráveis. Para isso, pressupõem-se a designação explícita de responsáveis por áreas críticas, como a gestão de incidentes, a conformidade regulatória, a proteção de dados, a continuidade operacional e a articulação com entidades externas.

Para além da definição estrutural, esta categoria recomenda a incorporação das responsabilidades em descrições de funções, contratos, acordos de nível de serviço (SLAs) e procedimentos operacionais padrão (SOPs). Esta integração assegura o alinhamento da cibersegurança com os processos de gestão de desempenho, auditoria e avaliação de risco.

Adicionalmente, é necessário a atribuição e o reconhecimento da autoridade adequada a cada um dos responsáveis permitindo a tomada de decisões eficazes e oportunas, especialmente em cenários de resposta a incidentes.

Por fim, a existência de papéis bem definidos reforça a cultura de responsabilização e conformidade, contribuindo para uma governação mais robusta e para a eficácia do sistema de gestão de segurança de informação da organização.

A categoria **Políticas, Processos e Procedimentos** (GV.PO) enfatiza a necessidade da organização desenvolver, implementar, comunicar e manter políticas, processos e procedimentos formais constituindo a base normativa e operacional sobre a qual assentam as práticas de segurança da informação.

As políticas devem refletir os objetivos estratégicos da organização e devem estar alinhadas com o seu contexto organizacional e com os requisitos legais, regulamentares e contratuais aplicáveis. Além disso, devem cobrir áreas essenciais como o controlo de acessos, a proteção de dados, a resposta a incidentes, a gestão de vulnerabilidades, a continuidade de operações, o uso aceitável de recursos tecnológicos e a interação com terceiros.

É fundamental que estas políticas sejam acompanhadas por processos e procedimentos operacionais que traduzam os princípios normativos em ações concretas, práticas e auditáveis. Estes processos devem estar bem documentados, ser consistentes com a arquitetura de controlo interno e adaptáveis à evolução do ambiente tecnológico e de ameaças.

A eficácia das políticas e dos procedimentos depende também da sua comunicação clara a todos os níveis da organização e da sua integração nos processos de formação, sensibilização e gestão de desempenho. Devem ser estabelecidos mecanismos para garantir a conformidade, tais como auditorias internas, avaliações periódicas e sanções em caso de incumprimento.

Por fim, esta categoria destaca a importância da revisão contínua e atualização das mesmas, de forma a incorporar as mudanças de contexto operacional, novas ameaças, lições aprendidas de incidentes e alterações legislativas ou regulamentares.

A categoria **Supervisão** (GV.OV) tem como objetivo principal assegurar o acompanhamento contínuo da estratégia, das políticas e das práticas de cibersegurança adotadas pela organização, garantindo que a governação em matéria de cibersegurança seja eficaz, transparente e alinhada com os objetivos estratégicos. Simultaneamente, visa assegurar a conformidade com os requisitos legais, regulamentares e normativos aplicáveis.

Esta categoria exige que a organização estabeleça mecanismos formais de acompanhamento e avaliação sistemática das atividades relacionadas com a gestão de risco. A supervisão deve ser conduzida por órgãos de governação competentes — como conselhos de administração, comités de risco ou comissões de auditoria — que detenham autoridade e independência suficientes para monitorizar a eficácia dos controlos, exigir accountability e promover a melhoria contínua.

Um aspeto crítico da supervisão consiste na adoção de uma abordagem baseada em evidência e apoiada por indicadores-chave de desempenho (KPIs) e de risco (KRIs), que forneçam à liderança informação relevante para suportar as suas decisões estratégicas. Adicionalmente, possibilita a identificação de deficiências e oportunidades de melhoria e contribui para reforçar a confiança das partes interessadas na capacidade da organização em gerir de forma responsável e eficaz os riscos associados ao ambiente digital.

A **função** '**Identificar**', visa promover uma compreensão aprofundada do contexto organizacional em matéria de segurança da informação, através da gestão eficaz de ativos, riscos e interdependências críticas. A organização pode centrar e priorizar os seus esforços de acordo com a sua estratégia de gestão de risco e as suas necessidades. A gestão de ativos (ID.AM), a avaliação de risco (ID.RA) e a melhoria (ID.IM) são as categorias de resultados que se enquadram nesta função.

A **Gestão de Ativos** (ID.AM) tem como principal objetivo garantir que a organização identifica, prioriza e gere adequadamente os seus ativos físicos e lógicos considerados essenciais à continuidade dos serviços críticos. Neste âmbito, a organização deve ser capaz de reconhecer dados pessoais, dispositivos, sistemas e infraestruturas relevantes, bem como estabelecer uma hierarquia de importância com base na sua criticidade e no perfil de risco institucional. De modo que esta gestão deve ser efetuada de acordo com a respetiva importância para os objetivos da organização e a abordagem da organização à gestão do risco.

A operacionalização desta categoria implica, entre outras ações, a manutenção de um inventário de ativos, a identificação de plataformas de *software* e aplicações em uso, o mapeamento dos fluxos de comunicação e dados, e o registo contínuo de sistemas de informação externos. Adicionalmente, exige-se a definição de responsabilidades em matéria de segurança da informação, tanto ao nível interno como nas relações com fornecedores, parceiros e clientes.

A **Avaliação de Risco** (ID.RA) implica que a organização compreenda de forma clara os riscos associados à segurança da informação no que diz respeito às suas operações, reputação, ativos e pessoas. Este entendimento deve assentar numa análise sistemática das vulnerabilidades dos ativos, complementada pela recolha de informação sobre ameaças emergentes em fontes

externas. Adicionalmente, exige-se a identificação dos vetores de ataque (internos ou externos), a análise dos impactos potenciais e da probabilidade de ocorrência, e a priorização das respostas aos riscos identificados com base numa avaliação integrada.

A categoria **Melhoria** (ID.IM) defende a identificação contínua de melhorias através de avaliações, testes e exercícios de segurança e revisões de processos operacionais, frequentemente em colaboração com entidades externas. Além disso, sublinha a importância da gestão proactiva dos planos de resposta a incidentes e de outras contingências operacionais que envolvam a cibersegurança [49].

A função '**Proteger**' estabelece as salvaguardas adequadas para garantir a prestação segura de serviços críticos e assegurar a proteção dos ativos de informação. Esta função visa implementar controlos técnicos e organizacionais que reduzam a probabilidade e o impacto de incidentes de cibersegurança, através de uma abordagem abrangente que contempla cinco categorias distintas: Gestão de Identidade, Autenticação e Controlo de Acessos (PR.AA), Consciencialização e Formação (PR.AT), Segurança de Dados (PR.DS), Segurança da Plataforma (PR.PS) e Resiliência da infraestrutura tecnológica (PR.IR).

A categoria **Gestão de Identidade, Autenticação e Controlo de Acessos** (PR.AC) estabelece que apenas utilizadores, processos e dispositivos devidamente autorizados devem ter acesso a ativos físicos e lógicos, de acordo com o risco associado ao acesso não autorizado. Para esse efeito, a organização deve implementar mecanismos para a emissão, gestão, verificação, revogação e auditoria de credenciais.

Deve ainda controlar o acesso físico aos ativos, gerir acessos remotos e garantir que as permissões de contas privilegiadas respeitam o princípio do menor privilégio - determina que um utilizador, sistema ou aplicação deve ter apenas os direitos e permissões mínimos necessários para executar as suas ações - e a separação de funções.

A integridade da rede deve ser assegurada através de segmentação, utilização de *software* de segurança e execução regular de cópias de segurança. A autenticação proporcional ao risco, a associação de identidades a credenciais únicas e a rastreabilidade das interações são igualmente exigidas.

No âmbito da **Consciencialização e Formação** (PR.AT), a organização deve garantir que todos os intervenientes, incluindo gestores de topo, colaboradores, fornecedores e parceiros, estão cientes das suas responsabilidades em matéria de segurança da informação. A formação e a consciencialização devem abranger todos os utilizadores, assegurando que compreendem e cumprem as políticas e procedimentos estabelecidos na organização.

A categoria **Segurança de Dados** (PR.DS) estabelece que os dados devem ser geridos em conformidade com a estratégia de risco da organização, de modo a garantir a sua confidencialidade, integridade e disponibilidade. Tal implica proteger os dados armazenados e em trânsito contra acessos indevidos, gerir adequadamente os processos de modificação e eliminação de dados, assegurar capacidade de armazenamento suficiente e implementar planos de recuperação para perdas de dados.

Adicionalmente, a organização deve garantir a separação dos ambientes de desenvolvimento e testes dos ambientes de produção.

A categoria de **Segurança da Plataforma** (PR.PS) centra-se na gestão de *hardware*, *software* e serviço, e abrange a aplicação de práticas de gestão de configuração, medidas preventivas contra *softwar*e não autorizado e a integração de práticas de desenvolvimento de *software* seguro. O objetivo é manter a integridade, a confidencialidade e a disponibilidade das plataformas virtuais e físicas [49].

A **Resiliência da Infraestrutura Tecnológica** (PR.IR), privilegia a implementação de controlos com o propósito de mitigar riscos associados ao acesso lógico não autorizado, à utilização indevida de recursos e a ameaças de origem ambiental, procurando assim manter o cumprimento dos princípios da segurança da informação em linha com a estratégia de gestão de risco. Paralelamente, são estabelecidas medidas específicas de resiliência operacional que visam assegurar a continuidade das atividades críticas, mesmo em caso de eventos adversos [49].

A função '**Detetar**' estabelece os mecanismos necessários para monitorizar sistemas, ativos e redes, de forma a permitir uma resposta célere e eficaz a potenciais incidentes. A deteção atempada de ameaças reduz significativamente o tempo de exposição a riscos e contribui para a minimização do impacto de ataques. Esta função organiza-se em duas categorias principais: Monitorização Contínua (DE.CM) e Análise de Eventos Adversos (DE.AE).

A categoria **Monitorização Contínua** (DE.CM) estabelece a necessidade de monitorização permanente de sistemas e redes, com o objetivo de identificar e registar eventos de segurança em tempo útil. Esta monitorização deve abranger a atividade de utilizadores, tráfego de rede, acesso a dados, comunicações internas e externas, e a integridade de *software* e *hardware*. A deteção de acessos não autorizados, o controlo de dispositivos móveis e a supervisão de sistemas críticos são medidas prioritárias neste domínio. A informação recolhida deverá alimentar mecanismos automatizados de alerta, capazes de desencadear respostas imediatas.

Por sua vez, a categoria **Análise de Eventos Adversos** (DE.AE), visa assegurar que a organização possui a capacidade de reconhecer e interpretar atividades maliciosas ou anómalas

que ocorram nos seus sistemas de informação. Para tal, é fundamental a manutenção de um quadro de referência baseado no comportamento esperado dos utilizadores e sistemas, sustentado na análise das operações de rede e nos respetivos fluxos de dados.

Adicionalmente, os eventos de segurança detetados devem ser analisados de forma sistemática, com o objetivo de identificar possíveis alvos e vetores de ataque utilizados. A compreensão do seu impacto é fundamental para que a organização avalie a gravidade das ocorrências e priorize ações de resposta adequadas.

Por fim, é imperativo que existam critérios bem definidos para a geração de alertas de incidentes, garantindo que os mesmos são acionados com base em limites pré-estabelecidos, evitando tanto a subavaliação como o excesso de falsos positivos.

A função '**Responder**' centra-se na capacidade de a organização reagir adequadamente a incidentes de cibersegurança detetados, mitigando o impacto desses eventos, restabelecendo com celeridade o normal funcionamento das operações e adotando medidas preventivas que evitem a sua recorrência. Esta função está estruturada em quatro categorias: Gestão de Incidentes (RS.MA), Análise de Incidentes (RS.AN), Comunicação e Notificação de Resposta a Incidentes (RS.CO) e Mitigação de Incidentes (RS.MI).

A Gestão de Incidentes (RS.MA) refere-se ao processo que abrange as várias fases de resposta a incidentes incluindo, quando necessário, a coordenação com entidades externas relevantes, bem como a ativação de mecanismos de recuperação para restabelecer a normalidade operacional.

A **Análise de Incidentes** (RS.AN) visa compreender as causas, os impactos e os vetores de ataque. Esta análise deve basear-se em evidências recolhidas de forma forense e ser conduzida por equipas com competências técnicas adequadas. A organização deve voluntariamente informar sobre os incidentes às partes interessadas.

A categoria **Comunicação e Notificação de Resposta a Incidentes** (RS.CO) destaca a importância da gestão eficaz da informação durante e após o incidente. Isto inclui a coordenação interna, bem como a comunicação com entidades externas, como autoridades competentes, parceiros e o público, quando necessário. Os papéis e canais de comunicação devem estar definidos previamente, respeitando os requisitos legais e regulamentares.

A categoria **Mitigação de Incidentes** (RS.MI) refere-se à implementação de medidas para conter o incidente, limitar a sua propagação e minimizar os seus efeitos. Isto pode incluir o

isolamento de sistemas comprometidos, a remoção de *software* malicioso ou a revogação de acessos indevidos.

A função '**Recuperar**' pretende assegurar que a organização restaura as capacidades e serviços afetados por um incidente de cibersegurança de forma eficaz e sustentada. Esta função é crucial para garantir a resiliência organizacional e a continuidade das operações após um evento disruptivo. Estrutura-se em duas categorias: Plano de Recuperação de Incidentes (RC.RP) e Comunicação de Recuperação de Incidentes (RC.CO).

A categoria **Plano de Recuperação de Incidentes** (RC.RP) estabelece que a organização deve desenvolver, manter e implementar procedimentos e processos formais destinados à recuperação de ativos e serviços críticos na sequência de um incidente de cibersegurança.

Estes planos de recuperação devem estar alinhados com os objetivos estratégicos da organização e ser suficientemente robustos para garantir o restabelecimento das operações com o mínimo de disrupção possível. Durante e após a ocorrência de um incidente, a organização deve seguir rigorosamente os procedimentos definidos, assegurando que as atividades de recuperação são conduzidas de forma coordenada, eficiente e em conformidade com os requisitos previamente estabelecidos.

A categoria **Comunicação de Recuperação de Incidentes** (RC.CO), destaca a importância de uma coordenação eficaz das atividades de comunicação durante e após a fase de recuperação de um incidente de cibersegurança. Esta coordenação deve envolver tanto os intervenientes internos como externos, incluindo centros operacionais, prestadores de serviços de internet (ISPs), equipas de resposta a incidentes e eventuais vítimas ou outras partes impactadas.

A organização deve assegurar a gestão adequada das relações institucionais após a ocorrência de um incidente, promovendo uma comunicação clara, oportuna e transparente. Esta comunicação é essencial não apenas para facilitar as ações de recuperação, mas também para contribuir para a reparação da reputação institucional. Além disso, é fundamental que todas as partes interessadas, internas ou externas, sejam devidamente notificadas sobre o progresso e as ações implementadas no âmbito da recuperação, em conformidade com os requisitos legais, contratuais e *governance*.

9.2 Diretiva NIS 2

A Diretiva NIS 2 [47], ou diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, entrou em vigor a 16 de Janeiro de 2023 e é aplicada a todos os Estados-Membros da União

Europeia. A adoção desta diretiva visa reforçar a segurança das redes e sistemas de informação em toda a União Europeia, substituindo a anterior Diretiva NIS [48] (Diretiva (UE) 2016/1148).

O artigo 42 da Diretiva, estabeleceu que os Estados-Membros da União Europeia deveriam transpor a Diretiva para a legislação nacional garantindo que as suas disposições fossem efetivamente aplicadas a partir de 17 de Outubro de 2024 nomeadamente, a designação das autoridades competentes, a implementação de medidas e a criação dos mecanismos necessários para assegurar a conformidade com os requisitos da Diretiva.

Apesar de aprovada em Conselho de Ministros, a proposta de Decreto-lei não foi promulgada devido à caducidade da autorização legislativa, resultante da crise política de março de 2025 que impediu a promulgação final.

9.2.1 Disposições da Diretiva NIS 2 sobre a Gestão de Risco de Fornecedores

A Diretiva NIS2 veio introduzir disposições especificas para a gestão de risco de fornecedores refletindo a importância crescente de assegurar que os riscos associados a fornecedores, parceiros e terceiras partes, sejam adequadamente geridos colmatando as deficiências da NIS [48] e contribuindo como meio de defesa para o aumento do cibercrime através da cadeia de fornecedores.

Podemos considerar como principais objetivos da Diretiva NIS 2 [47]:

a) A adoção de uma estratégia de segurança comum a toda a UE, onde prevaleça a cooperação, partilha de conhecimento e união para enfrentar a ameaça crescente do cibercrime.
b) O incremento da resiliência e robustez através da definição de um conjunto de medidas a implementar no campo da cibersegurança e dirigidas a entidades e organizações públicas e privadas que operam em setores fundamentais no espaço europeu.
c) O alargamento da Diretiva NIS [48] a mais setores de atividade, independentemente da dimensão organizacional, passando a existir uma distinção entre entidades essenciais e entidades importantes, embora não tenha expressão as diferenças entre ambas no que respeita a requisitos de segurança;
d) A criação de uma base de dados europeia para o registo de vulnerabilidades sob a gestão da ENISA [13].
e) Uma maior responsabilização para entidades não sediadas na União Europeia, mas que operam no espaço europeu em setores de atividade abrangidos pela diretiva;

f) O reconhecimento e a valorização da área de cibersegurança dentro das organizações através da responsabilização dos Conselhos de Administração quando ocorrem incidentes de segurança ou registo de não-conformidades associados à inexistência ou à falta de apropriação na criação de controlos que sejam efetivos no cumprimento dos requisitos de segurança.

As principais disposições relacionadas com a Gestão de Risco de Fornecedores que a NIS 2 [47] introduziu envolvem:

1. A adoção de uma abordagem baseado no risco para a segurança das redes e sistemas de informação incluindo a avaliação e a gestão de risco de fornecedores, parceiros e terceiras partes;
2. A garantia de que as medidas de segurança devem ser implementadas ao longo de toda a cadeia de fornecedores e ao longo também de todo o ciclo de vida dos produtos e serviços utilizados;

a) A inclusão dos Fornecedores de Serviços Digitais e outros prestadores críticos nas avaliações de risco das organizações;
b) A garantia de que os contratos com fornecedores incluam requisitos de segurança adequados, conforme especificado na diretiva;
c) As entidades devem notificar as autoridades competentes sobre os incidentes de segurança que afetem as suas redes e sistemas de informação, incluindo os incidentes relacionados com a cadeia de fornecedores;
d) O incentivo à cooperação e à partilha de informações sobre os incidentes de segurança entre entidades e fornecedores como medida de mitigação dos riscos e de resposta a ameaças;
e) As autoridades competentes nos Estados-Membros devem supervisionar, a conformidade das entidades públicas e privadas, com os requisitos da NIS 2 [47] incluindo a gestão de riscos de fornecedores. Em caso de incumprimento podem ser impostas sanções.

Assim, para garantir a conformidade com a Diretiva NIS 2 [47], as entidades devem integrar a gestão de risco de fornecedores nas suas estratégias de cibersegurança, realizando avaliações de risco, estabelecendo requisitos de segurança nos contratos com os seus fornecedores e assegurar a cooperação efetiva em caso de incidentes de segurança.

9.2.2 Proposta de Lei para a Transposição Nacional da Diretiva NIS 2

9.2.2.1 Expansão do Âmbito de Aplicação

A Diretiva NIS [48] baseia a sua abordagem na identificação de operadores de serviços essenciais por setor, ao passo que a Diretiva NIS 2 [47] e consequentemente a sua proposta de Lei vêm adotar uma abordagem baseada no risco e na dimensão das organizações.

Conforme o artigo 2º da Diretiva NIS 2 [47], a mesma é aplicável a entidades que "prestem serviços essenciais à economia e à sociedade", utilizando critérios objetivos como o volume de negócios, o número de trabalhadores e a natureza dos serviços prestados. Assim, deve ser considerado como critérios de inclusão que as entidades tenham um número de trabalhadores superior a 50, um volume de negócios anual superior a 10 milhões de euros e a natureza das atividades prestadas.

A proposta de transposição propõe que as entidades sejam classificadas como entidades essenciais – incluem operadores de infraestruturas críticas em setores como a energia, a saúde, os transportes, a banca e o abastecimento de águas, e as entidades importantes – incluem entidades tecnológicas, de fabrico, de prestação de serviços digitais e outras que tenham relevância económica ou social. Esta diferenciação consagrada no artigo 3.º da Diretiva traduz-se numa abordagem proporcional, com diferentes níveis de obrigações consoante o impacto potencial das entidades.

Para além dos fundamentos operacionais, importa destacar os fundamentos jurídicos e políticos subjacentes à adoção deste novo modelo normativo.

Em primeiro lugar, a harmonização das regras a nível europeu constitui um objetivo explícito da Diretiva, nos termos do artigo 4.º, promovendo uma uniformização dos requisitos de segurança e supervisão aplicáveis aos operadores críticos em todos os Estados-Membros.

Em segundo lugar, a NIS 2 [47] visa reduzir a fragmentação regulatória que caracterizava o regime anterior, eliminando as disparidades significativas nas obrigações impostas e nos modelos de fiscalização nacionais, o que se afigurava prejudicial à coesão do mercado digital europeu.

Em terceiro lugar, esta reforma normativa contribui para uma maior eficácia na proteção do mercado interno, assegurando que a resiliência digital das infraestruturas críticas não constitui uma barreira à livre circulação de bens, serviços e dados na União Europeia.

Em suma, a proposta de Lei amplia significativamente o âmbito das entidades sujeitas à nova Diretiva.

9.2.2.2 Exigências ao nível da Gestão de Risco

A proposta impõe um quadro normativo mais robusto para a gestão de risco em cibersegurança. O artigo 21º da NIS 2 [47] impõe que as entidades adotem medidas técnicas e organizativas adequadas para gerir os riscos colocados à segurança das suas redes e sistemas segundo o princípio orientador da proporcionalidade, que refere a adaptação das medidas à dimensão e criticidade da entidade.

A proposta de Lei concretiza estas exigências, impondo obrigações como:

- Avaliação e gestão de risco;
- Segurança na cadeia de fornecimento e em relações contratuais com terceiros;
- Políticas de criptografia e controlo de acessos;
- Elaboração de planos de continuidade e recuperação de incidentes;
- Formação contínua em cibersegurança.

Estes requisitos representam um reforço significativo face à legislação anterior.

De salientar, a responsabilização dos órgãos de administração (*accountability*), os quais, segundo a diretiva, devem supervisionar e aprovar as medidas de gestão de riscos podendo ser responsabilizados em caso de incumprimento.

Para dar cumprimento a este novo quadro normativo, as entidades abrangidas deverão investir periodicamente em auditorias de cibersegurança, implementar programas de capacitação interna e procurar certificações reconhecidas internacionalmente, como a ISO/IEC 27001, que fornece um referencial estruturado para a gestão da segurança da informação.

Estas obrigações técnicas e organizativas, implicam também um potencial aumento dos custos com o *compliance*. Tal incremento será particularmente sensível no caso das pequenas e médias empresas (PME) que, ao serem enquadradas como “entidades importantes”, poderão enfrentar dificuldades na alocação de recursos humanos e financeiros adequados ao cumprimento das novas exigências.

9.2.2.3 Mecanismos de Notificação de Incidentes

O regime de notificação de incidentes é clarificado e endurecido, visando reforçar a resposta coordenada a nível nacional e europeu. Assim, a proposta reforça os deveres de notificação de incidentes, impondo prazos mais apertados:

- Notificação inicial no prazo de 24 horas após a deteção do incidente;
- Relatório intercalar em 72 horas;
- Relatório final até 1 mês após a notificação inicial.

Estes prazos estão previstos no artigo 23.º da diretiva, que visa garantir a resposta rápida e coordenada aos incidentes. A notificação deve incluir o tipo de incidente, o seu impacto previsto ou real, e as medidas de resposta adotadas. Há ainda disposições para evitar duplicidade de notificações quando também estejam em causa dados pessoais, promovendo a articulação entre o CNCS, a Comissão Nacional de Proteção de Dados (CNPD) e outras entidades reguladoras setoriais.

9.2.2.4 Estrutura Institucional e Supervisão

A proposta reforça de forma substancial a arquitetura institucional no domínio da cibersegurança, estabelecendo um modelo de *governance* multinível que visa garantir a eficácia da supervisão, a especialização técnica e a articulação entre os diferentes atores do sistema.

Ao abrigo do artigo 8.º da Diretiva, o CNCS é designado como autoridade nacional competente. Esta entidade assume um papel central na operacionalização da Estratégia Nacional de Cibersegurança, sendo-lhe atribuídas competências em matéria de supervisão, aplicação de sanções administrativas, avaliação de conformidade das entidades abrangidas e cooperação internacional com organismos europeus, como a *European Cyber Crisis Liaison Organisation Network* (EU-CyCLONe) - é uma rede de cooperação para as autoridades nacionais dos Estados--Membros responsáveis pela gestão de crises no quadro da cibersegurança que foi formalizada em 16 de janeiro de 2023, quando o artigo 16.º da NIS 2 [47] entrou em vigor - para a resposta a incidentes de grande escala, e a ENISA [13] no desenvolvimento de capacidades e políticas comuns.

Complementarmente, a proposta de Lei atribui competências de supervisão técnica a autoridades setoriais competentes, consoante a natureza do setor regulado. Entre estas destacam--se a Autoridade Nacional de Comunicações (ANACOM) no setor das comunicações eletrónicas, o Banco de Portugal no setor financeiro e bancário, a Entidade Reguladora dos Serviços Energéticos (ERSE) no setor da energia, bem como outras autoridades para os domínios dos transportes, da saúde e da administração pública. Esta estrutura permite assegurar uma supervisão especializada e adaptada aos riscos específicos de cada setor, promovendo uma regulação tecnicamente fundamentada e sensível às características operacionais das entidades visadas.

A eficácia deste modelo institucional assenta, em larga medida, na implementação de mecanismos de articulação interinstitucional, os quais são expressamente contemplados na proposta legislativa. Em primeiro lugar, prevê-se a criação de comissões de coordenação interministeriais, com o objetivo de garantir a coerência das políticas públicas de cibersegurança e facilitar a concertação de decisões estratégicas entre os diferentes ministérios com competências na matéria. Em segundo lugar, reforça-se a rede nacional de CSIRT (*Computer Security Incident Response Teams*), promovendo a partilha de informação operacional, o apoio técnico e a coordenação na resposta a incidentes entre os vários centros de resposta existentes, tanto do setor público como do setor privado.

Estes mecanismos de coordenação assumem particular importância face à crescente complexidade do ecossistema digital e à natureza transetorial dos riscos em cibersegurança.

A abordagem proposta procura responder às exigências da NIS 2 [47] em matéria de interoperabilidade institucional, favorecendo um modelo de *governance* colaborativa, que combine supervisão centralizada com especialização setorial e articulação técnica.

Em síntese, a proposta de Lei materializa uma evolução significativa do modelo de *governance* da cibersegurança em Portugal, reforçando a capacidade institucional, a resposta coordenada a ameaças e a integração do país nos mecanismos europeus de ciberdefesa e resiliência digital.

9.2.2.5 Regime Sancionatório

O diploma introduz um regime sancionatório dissuasor e alinhado com a filosofia do Regulamento Geral sobre a Proteção de Dados (RGPD) [52]. O artigo 34.º da NIS 2 [47] estabelece a imposição de coimas administrativas significativas como forma de garantir a aplicação eficaz do regime jurídico, assegurando a proporcionalidade e a gravidade das sanções face ao incumprimento das obrigações legais.

A proposta prevê um quadro punitivo com escalões diferenciados, prevendo três tipos de contraordenações - muito graves, graves e leves. As contraordenações muito graves que incluem o incumprimento de obrigações como a implementação de medidas de cibersegurança e notificações de incidentes podem auferir:

- Coimas até 10 milhões de euros ou 2% do volume de negócios anual, consoante o que for mais elevado, no caso de entidades classificadas como essenciais;

- Coimas até 7 milhões de euros ou 1,4% do volume de negócios global para entidades classificadas como importantes.

Além das sanções pecuniárias, o diploma prevê outras medidas punitivas complementares como a suspensão temporária das atividades, a responsabilização individual dos gestores em caso de negligência grave ou incumprimento deliberado das obrigações legais, e a divulgação pública das sanções aplicadas com o objetivo de reforçar a transparência e o efeito dissuasor no setor em causa.

Este regime sancionatório visa, em primeiro lugar, proteger o interesse público e a estabilidade dos sistemas críticos, assegurando que as entidades cuja atividade impacta diretamente a economia e a sociedade mantêm níveis adequados de segurança e resiliência digital. Em segundo lugar, pretende-se estimular o cumprimento voluntário das obrigações legais, criando um ambiente regulatório onde as sanções atuam como último recurso, num quadro de corresponsabilização e cultura de segurança.

9.2.2.6 Instrumentos Estratégicos

A proposta contempla três instrumentos-chave para a execução das políticas públicas de cibersegurança, funcionando como elementos de planeamento, orientação e coordenação interinstitucional:

- **a)** Estratégia Nacional de Segurança do Ciberespaço - constitui o principal documento de orientação estratégica da política pública nacional em matéria de cibersegurança. Este instrumento define os objetivos estratégicos de médio e longo prazo, promovendo uma abordagem multissetorial e baseada no risco. A estratégia articula-se em torno de eixos como a capacitação institucional e tecnológica, a cooperação nacional e internacional, a resiliência das infraestruturas críticas, e o reforço da literacia digital e da cultura de segurança.
- **b)** Plano Nacional de Resposta a Incidentes de Grande Escala - é um instrumento operacional de preparação e resposta a cenários de crise no quadro da cibersegurança, nomeadamente em setores críticos. Este plano define os procedimentos de escalonamento, os mecanismos de comunicação entre autoridades competentes e os protocolos de cooperação com os níveis europeu e internacional, em especial com a EU-CyCLONe e as redes de CSIRT nacionais e setoriais.
- **c)** A sua importância reside na capacidade de simular, antecipar e coordenar respostas a incidentes de grande escala, assegurando a continuidade de serviços essenciais e a proteção da ordem pública.Quadro Nacional de Referência para a Cibersegurança (QNRCS) - funciona como um guia normativo que estabelece normas, princípios e boas práticas aplicáveis a entidades públicas e privadas. O CNCS disponibiliza o QNRCS [52] onde são descritas linhas orientadoras e medidas específicas

relacionadas com a gestão de risco com o objetivo de fortalecer a resiliência das infraestruturas críticas, melhorar a resposta a incidentes e garantir a segurança do ciberespaço nacional.

Essas medidas são estruturadas para abordar vários aspetos da cibersegurança, entre eles os relativos à proteção de infraestruturas críticas como:

1. A avaliação contínua dos riscos com o propósito de identificar vulnerabilidades e ameaças nas infraestruturas críticas;
2. O desenvolvimento e a manutenção contínua de planos de continuidade de negócio e recuperação em caso de ataque;
3. A partilha de informações sobre ameaças e vulnerabilidades entre os diferentes *stakeholders*.

9.3 *Cloud Controls Matrix*

A *Cloud Security Alliance* (CSA) [54] surgiu em 2008 enquanto organização mundial sem fins lucrativos totalmente dedicada à vertente *cloud* com o objetivo de definir procedimentos e práticas aplicacionais para os produtos e serviços *cloud* sobretudo para apoiar na gestão de risco associada a esta tipologia de soluções. O aumento de soluções baseadas em *cloud* requer a definição e implementação de mecanismos de segurança que respondam às ameaças a que estas soluções estão expostas, em linha com uma gestão de risco adequada.

Esta *framework* é composta por 197 controlos distribuídos por 17 domínios.

A CSA dispõe de um programa de avaliação e certificação em tecnologias *cloud* para prestadores desta tipologia de serviço denominado *Security Trust & Assurance Registry* (STAR) [55] funcionando em dois níveis distintos:

▪ Nível 1 – Autoavaliação – Neste primeiro nível a organização pode submeter um ou dois questionários de autoavaliação em segurança e privacidade. Para a vertente de segurança os questionários têm por base a *Cloud Controls Matrix* (CCM) que de forma transversal avaliará e documentará todos os controlos de segurança. Para a vertente de privacidade ou proteção de dados, a avaliação é realizada com base no código de conduta do RGPD [56]. Este nível pode ser obtido por organizações que tenham um baixo ou nulo apetite ao risco, por aquelas que procuram oferecer uma maior transparência relativamente aos controlos de segurança que têm implementados e procuram balancear entre a confiança e a transparência nos serviços *cloud* que disponibilizam.

▪ Nível 2 – Certificação – As organizações devem optar por este nível quando se propõem a obter uma certificação de *cloud* ou quando pretendem obter um outro nível de certificação para os seus serviços e tecnologias *cloud*, mas necessitam de ter previamente esta certificação.

9.4 ISO 31000

A norma de gestão de risco recomenda que "as organizações desenvolvam, implementem e melhorem continuamente uma estrutura cujo objetivo é integrar o processo para gerir o risco na governação, estratégia e planeamento, gestão, processos de comunicação, políticas, valores e cultura".

Para uma gestão de risco eficaz toda a infraestrutura deverá desenvolver a sua atividade tendo por base os seguintes princípios orientadores [57]:

a) Uma política eficaz de gestão de risco contribui para que os objetivos da organização sejam atingidos criando e protegendo o valor da organização;

b) A gestão de risco é parte integrante de todos os processos da organização na medida em que deve ocorrer de forma integrada com a responsabilização da gestão, o envolvimento dos decisores em todos os níveis da organização e de todas as partes interessadas. Também é parte da tomada de decisão porque deve definir as medidas a serem tomadas e a sua ordem de atuação de acordo com o seu nível de prioridade;

c) A gestão de risco tem de ser consistente e atempada para gerar resultados eficazes para a organização tendo em consideração e adaptando-se ao seu contexto interno e externo.

d) A gestão de risco é dinâmica e reativa a alterações de contexto, de conhecimento ou de qualquer outra alteração que direta ou indiretamente influencie a organização;

e) A gestão de risco contribui para os processos de melhoria contínua contribuindo para o aumento do nível de maturidade da gestão de risco da organização.

Para que o processo de gestão de risco seja mantido de forma eficaz e eficiente recomenda-se que também sejam identificados os *owners* do risco, que por sua vez são os responsáveis pela gestão do mesmo, e que se avalie continuamente o processo de *report* interno e externo relativo à gestão de risco da organização. Pela sua pertinência, o processo de gestão de risco deve ser integrado na política de gestão de risco, nos restantes processos da organização assim como no seu plano estratégico.

Assim sendo, o processo de gestão de risco compreende várias atividades como demonstra a figura seguinte:

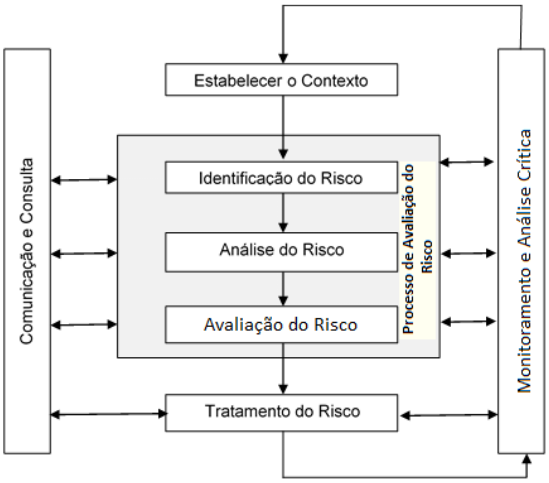

Figura 2 - Diagrama do processo de gestão de risco [58]

9.5 Normativos da Autoridade de Supervisão de Seguros e Fundos de Pensões

No quadro português importa referir, a título de exemplo, o caso das entidades reguladas como empresas de seguros e resseguros que operam em Portugal, as sociedades gestoras de fundos de pensões, as mediadoras de seguros e de resseguros, auditores e atuários vinculados ao setor segurador e de fundos de pensões, outras entidades sujeitas à supervisão da Normativos da Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF), como organismos de investimento coletivo que gerem produtos relacionados com seguros ou pensões e tomadores de seguros, segurados, beneficiários e participantes em fundos de pensões. Na medida em que os normativos afetam os seus direitos ou deveres devem, primeiramente, observar os Normativos da ASF.

Estes normativos, em particular o Regulamento n.º 1/2020-R sobre requisitos de *governance*, estabelecem exigências específicas quanto à identificação e gestão dos riscos operacionais e de segurança, incluindo os riscos decorrentes da terceirização de funções essenciais ou importantes.

9.5.1 Exemplos de Requisitos Relevantes dos Normativos da ASF no Âmbito da Externalização de Funções Críticas ou Importantes

No quadro regulatório definido pela ASF, destacam-se diversos requisitos normativos que visam assegurar uma gestão prudente e segura das atividades externalizadas pelas entidades supervisionadas. Entre os requisitos mais relevantes destacam-se os seguintes:

a) Avaliação prévia dos riscos associados à externalização (artigo 63.º) - previamente à celebração do contrato com o fornecedor, as entidades devem proceder a

uma análise rigorosa dos riscos envolvidos, nomeadamente no que respeita à continuidade operacional e à resiliência em matéria de cibersegurança. Esta avaliação visa garantir que a externalização não compromete a estabilidade, integridade e conformidade das operações, e que os riscos emergentes são devidamente identificados, quantificados e mitigados.

b) Clareza contratual sobre as responsabilidades em matéria de segurança (artigo 66.º) - os contratos celebrados com prestadores de serviços devem conter cláusulas claras e específicas relativamente às obrigações das partes em domínios como a proteção de dados pessoais, a segurança da informação e a privacidade. Além disso, deve ser salvaguardado o direito de acesso, auditoria e fiscalização por parte da ASF, assegurando a rastreabilidade e a responsabilidade em todas as fases da prestação do serviço.

c) Monitorização contínua da função externalizada (artigo 67.º) - é recomendado um mecanismo de monitorização contínua da função ou serviço externalizado, que inclua a avaliação sistemática do desempenho do prestador de serviços, designadamente em relação à eficácia dos controlos de segurança e à conformidade contratual.

d) Elaboração de um plano de saída (artigo 68.º) - as entidades devem dispor de um plano de saída estruturado que preveja medidas concretas que evitem disrupções e assegurem a manutenção dos níveis de serviço essenciais, minimizando riscos para os tomadores de seguros, segurados e terceiras partes.

9.6 *Digital Operational Resilience Act*

Paralelamente, o Regulamento (UE) 2022/2554, *Digital Operational Resilience Act* (DORA), introduz exigências específicas para as instituições financeiras no que respeita à resiliência operacional digital, incluindo disposições claras sobre a gestão de riscos associados a prestadores de serviços TIC (Tecnologias da Informação e Comunicação). O DORA impõe, entre outros aspetos, a classificação e documentação dos fornecedores TIC críticos, a realização de avaliações de risco na fase de planeamento, isto é, antes da contratação, e a existência de estratégias de saída. Este regulamento reforça a necessidade de uma abordagem baseada em processos para a gestão de risco de fornecedores no setor financeiro.

10 A abordagem por processo - uma das abordagens possíveis a implementar na gestão de risco de fornecedores pelas organizações

10.1 Propósito

A crescente complexidade do ecossistema digital tem impulsionado a necessidade de uma abordagem mais robusta à gestão de risco. Por isso, têm sido identificados diferentes fatores como catalisadores desse aumento, contribuindo para uma paisagem digital cada vez mais vulnerável e exigente em termos de resiliência organizacional.

Em primeiro lugar, a aceleração da transformação digital da economia e da sociedade, alavancada pela adoção contínua de novas tecnologias e ferramentas, tem exposto as organizações a uma superfície de ataque significativamente mais alargada. Esta evolução tecnológica, embora essencial à competitividade e à inovação, implica também a integração de sistemas muitas vezes heterogéneos e interconectados, o que aumenta a complexidade da sua proteção.

Paralelamente, observa-se uma crescente sofisticação dos ciberataques, que utilizam técnicas avançadas para contornar mecanismos tradicionais de defesa. Estes ataques não só aumentam em frequência, como também em impacto, afetando setores críticos e comprometendo a confiança nos sistemas digitais.

Acresce a isto a complexidade crescente dos ambientes de armazenamento e transferência de dados, frequentemente distribuídos entre múltiplas infraestruturas, plataformas e jurisdições. Estes contextos exigem elevados níveis de coordenação e monitorização, sob pena de se comprometer a integridade e a confidencialidade dos dados tratados.

A preservação de informação sensível constitui igualmente um dos principais desafios, numa era em que a proteção de dados pessoais e estratégicos é simultaneamente uma exigência legal e

um imperativo ético. A salvaguarda desta informação é particularmente crítica face ao volume crescente de dados partilhados.

A partilha de grandes volumes de dados e a sua transferência transfronteiriça, agravam a exposição das organizações a riscos regulatórios e de soberania digital. Esta realidade impõe a necessidade de mecanismos rigorosos de avaliação e mitigação de risco, garantindo o cumprimento das normas e regulamentos relativos à proteção de dados e à segurança da informação transferida.

Por fim, outro vetor relevante e sobre este recai o propósito da nova abordagem é a crescente dependência de fornecedores, o que introduz riscos adicionais associados à cadeia de fornecimento digital sendo uma das principais portas de entrada para ciberataques nas organizações. A gestão destes riscos torna-se particularmente desafiante quando os controlos de segurança não são uniformemente aplicados ao longo da cadeia.

Ora, estes fatores inter-relacionados desafiam os modelos atuais de *governance* da segurança de informação exigindo novos modelos com uma abordagem integrada, preventiva e colaborativa por parte das organizações.

10.2 Questão e Contributo de Investigação

10.2.1 Questão

A questão que se impõe no seio das organizações é: Qual é que deve ser a abordagem a adotar para a gestão eficaz do risco de fornecedores cumprindo com os requisitos legais aplicáveis?

10.2.2 Contributo de Investigação

O contributo desta dissertação consiste na criação de uma abordagem por processo que possa ser implementada pelas organizações para a gestão de risco de fornecedores salvaguardando que a sua implementação cumpre com os requisitos legais aplicáveis, e que se encontram *compliant* com as boas práticas em cibersegurança.

O segundo propósito da abordagem por processo é que qualquer organização possa tomar decisões informadas em todas as fases de contacto com o fornecedor, de modo a mitigar os riscos associados:

a) À seleção do fornecedor;
b) À contratação do fornecedor;
c) À definição de requisitos de segurança;

d) À monitorização contínua do desempenho do fornecedor;

e) Até ao término do contrato.

A abordagem por processo é constituída por quatro subprocessos que, por sua vez, apresentam um conjunto de atividades que devem ser seguidas e adaptadas pelas organizações de acordo com o seu modelo de governo:

1º Subprocesso - *Planning*

2º Subprocesso - *Onboarding*

3º Subprocesso - *Management*

4º Subprocesso - *Offboarding*

10.3 1º Subprocesso - *Planning*

O 1º subprocesso consiste nas atividades de planeamento que antecedem à formalização da relação contratual entre a organização e o fornecedor, e que devem ser desencadeadas com o objetivo de (1) identificar os requisitos legais e regulamentares aplicáveis à organização no âmbito da cibersegurança, (2) criar políticas, processos e procedimentos com o propósito de documentar a definição e operacionalização da gestão de risco de fornecedores na organização e (3) definir quais os requisitos mínimos que devem ser exigidos aos fornecedores para que o serviço seja prestado num ambiente seguro.

a) A **1ª atividade** consiste na identificação de requisitos legais e regulamentares que sejam aplicáveis à organização no quadro da gestão de risco de fornecedores.

A identificação rigorosa dos requisitos legais, regulamentares e das boas práticas aplicáveis às organizações, no quadro da gestão de risco de fornecedores, constitui o ponto de partida para a adoção desta abordagem. A primeira atividade visa assegurar, desde o momento do planeamento, que a organização compreende as suas obrigações normativas relativas às tecnologias de informação e neste contexto em particular na gestão de fornecedores.

As *frameworks* de cibersegurança assumem um papel central no processo de *due diligence* aplicado à gestão de risco de terceiros, oferecendo uma base estruturada para avaliar a maturidade e a robustez dos controlos de segurança implementados pelos fornecedores. No âmbito das interações com terceiros, uma das questões iniciais e mais relevantes consiste em identificar qual a *framework* de cibersegurança adotada pelo fornecedor, dado que esta escolha constitui um indicador crítico da abordagem sistemática da organização à gestão de riscos de segurança da informação.

A resposta a esta questão permite não apenas aferir a existência de um modelo normativo estruturado, mas também compreender a filosofia subjacente às práticas de segurança do fornecedor. Embora muitas das principais estruturas normativas - como o NIST *Cybersecurity Framework*, a ISO/IEC 27001, o CIS *Controls*, entre outras - partilhem domínios e controlos semelhantes, dada a transversalidade dos princípios fundamentais da cibersegurança, é comum que estas se diferenciem ao nível da granularidade e do âmbito de aplicação.

Neste sentido, a compreensão do setor de atividade em que o fornecedor opera constitui um elemento determinante para avaliar a adequação da *framework* adotada, uma vez que determinados setores podem estar sujeitos a regimes regulatórios específicos que impõem a adoção de determinados referenciais normativos.

A seleção e implementação de uma *framework* coerente com o contexto operacional e regulatório do fornecedor revela-se um indicador de maturidade organizacional e de compromisso com a segurança da cadeia de fornecimento.

Além disso, na fase de planeamento e no contexto desta primeira atividade, é importante clarificar a diferença entre dois conceitos: o conceito de *due diligence* e o conceito de *due care*.

O conceito de *due care* refere-se à adoção de um conjunto de esforços diligentes e proporcionais com vista à proteção dos interesses da organização, assumindo a forma de medidas concretas e sustentadas que visam mitigar riscos previamente identificados. No contexto da gestão de risco de fornecedores, a *due care* implica assegurar que os terceiros desenvolvem, documentam e implementam políticas, normas, requisitos mínimos (*baselines*) e procedimentos de segurança, com o objetivo de garantir a integridade, confidencialidade e disponibilidade dos seus ambientes tecnológicos.

Enquanto a *due diligence* se refere à etapa de análise e investigação preliminar, orientada para a identificação e compreensão dos riscos associados a um determinado fornecedor, antes da formalização contratual. Isto é, a *due care* traduz-se na materialização das ações que resultam dessa avaliação prévia, evidenciando um compromisso efetivo com a mitigação de riscos identificados.

Em termos complementares, a *due diligence* estabelece o quadro de referência para a tomada de decisões informadas, ao passo que a *due care* representa a execução prática das medidas consideradas necessárias para garantir a segurança e a conformidade ao longo da relação contratual, atividade essa que será desenvolvida no segundo subprocesso.

Em síntese, a atividade de identificação de requisitos legais e regulamentares deve resultar num mapeamento claro e documentado das obrigações aplicáveis, constituindo um referencial normativo para as etapas subsequentes do ciclo de vida da gestão de risco de fornecedores.

Este mapeamento deve ser dinâmico, revisto periodicamente à luz da evolução legislativa e do contexto crescente de ameaças no âmbito da cibersegurança, garantindo a conformidade e a eficácia das medidas de segurança adotadas.

b) A **2ª atividade** corresponde à criação ou à revisitação de políticas, processos e procedimentos internos por forma a documentar a definição e operacionalização da gestão de risco de fornecedores.

Assim, a Política de Gestão de Risco de Fornecedores é o documento de caráter normativo que define o posicionamento institucional da organização sobre a Gestão de Risco de Fornecedores que deve ser seguido por toda a organização assim como pelas suas entidades externas.

O documento deve começar por apresentar na sua primeira secção o objetivo, isto é, definir os princípios, responsabilidades e procedimentos para a identificação, avaliação, mitigação e monitorização dos riscos de cibersegurança associados à cadeia de fornecedores, de modo a assegurar a resiliência digital, a proteção dos sistemas e serviços críticos da organização e da sua cadeia de fornecimento.

Na segunda secção, a política deve apresentar a delimitação do seu âmbito com a identificação de todas as partes que tenham direta ou indiretamente interferência sobre os ativos de informação da organização, independentemente do seu modelo contratual ou da sua localização geográfica, tais como, os seus fornecedores de tecnologias de informação e comunicação, os prestadores de serviços (*outsourcing*), os subcontratantes e os parceiros tecnológicos, entre outros.

A terceira secção define os princípios gerais sobre os quais a política assenta:

1. O princípio da proporcionalidade – refere que a resposta ou ação tomada pela organização deve ser adequada e corresponder à magnitude do risco envolvido, o que significa que quanto maior a magnitude do risco, maior o número de recursos e medidas necessárias para a sua mitigação. A criticidade do fornecedor é determinada com base na natureza dos serviços prestados, no grau de dependência tecnológica e na sensibilidade da informação partilhada.

2. O princípio da responsabilidade – refere que todas as partes envolvidas no processo de gestão de fornecedores devem ter conhecimento das suas responsabilidades, aceitar e cumprir com as mesmas. A responsabilização de todas as partes deve estar formalmente refletida nos contratos celebrados pela organização quando se trata de entidades externas.
3. O princípio da avaliação ao longo do ciclo de vida – a gestão de risco de fornecedores deve ser um exercício contínuo e dinâmico que acompanhe todas as fases da relação contratual e operacional com terceiros. O objetivo da sua revisão é que reflita ao longo do tempo as alterações que ocorrem no contexto tecnológico, organizacional, regulatório e contratual de modo que o nível de risco evolua correlacionado com a natureza dos serviços prestados, o grau de dependência da organização em relação ao fornecedor e ao contexto externo.
4. O princípio da integração – a gestão de risco de fornecedores deve estar integrada no sistema de gestão de risco da organização, em alinhamento com o seu plano estratégico, na medida em que a gestão de terceiros deve ser entendida como uma dimensão transversal do risco da organização na qual se incluam vários domínios da segurança da informação, da continuidade de negócio, da área jurídica, da área financeira, da área de *compliance* e da área de comunicação na vertente reputacional. O principal objetivo desta integração é garantir uma abordagem holística para a identificação, avaliação e tratamento de risco, de modo a evitar silos operacionais contribuindo para a promoção de sinergias entre as várias áreas da organização.
5. O princípio da conformidade – a política de gestão de risco de fornecedores deve cumprir integralmente com as obrigações legais, regulamentares, e normativas, aplicáveis à organização. Este princípio é particularmente importante quando se trata de operadores de serviços críticos por estarem sujeitos a um maior número de obrigações em matéria de cibersegurança ao abrigo da legislação atual.
6. O princípio da transparência – As ações e decisões tomadas ao longo do ciclo de vida da relação contratual com os fornecedores devem ser documentadas e com isso ver reforçada a confiança, a responsabilidade e a capacidade de supervisão na gestão com os fornecedores. Facilita a realização de auditorias internas e externas e contribui ainda para melhorar a prestação de contas da organização aos seus reguladores, acionistas e outras partes interessadas. A ausência de transparência dificulta a deteção de desvios, a identificação de fragilidades ao longo do processo e a sua correção.

7. O princípio da confidencialidade, integridade e disponibilidade – a gestão de risco de fornecedores deve proteger os ativos de informação da organização respeitando os três pilares fundamentais da segurança da informação.

Num cenário em que os fornecedores desempenham um papel cada vez mais relevante na prestação de serviços críticos ou no tratamento de dados sensíveis, torna-se essencial assegurar que a sua atuação não compromete os níveis de segurança exigidos pela organização, especialmente quando têm acesso a infraestruturas, sistemas ou dados relevantes.

A organização deve assegurar que os fornecedores apenas acedem à informação necessária para a prestação de serviços, e que esse acesso é devidamente controlado, monitorizado e revogável.

Para isso, algumas das medidas de proteção contra o acesso não autorizado à informação e que podem ser adotadas pela organização são constituídas por acordos de confidencialidade (NDAs), controlo de acessos baseado em perfis, encriptação de dados em trânsito e em repouso e monitorização de acessos e registo de *logs*.

No que respeita à integridade, podem ser asseguradas algumas medidas de modo a garantir que a informação não é alterada de forma não autorizada ou acidental durante o seu processamento, armazenamento ou transmissão, tais como: o uso de mecanismos de controlo de versões e validação de dados, a utilização de assinaturas digitais e *checksums*, a implementação de um processo de segregação de funções e a monitorização de alterações em sistemas ou ficheiros (*file integrity monitoring*).

Quanto à disponibilidade podem ser adotadas algumas medidas que mitiguem a indisponibilidade de um sistema ou serviço prestado pelo fornecedor não comprometendo a continuidade do serviço e evitando que este comprometimento provoque falhas em cadeia. Para isso, podem ser adotadas medidas como estabelecer acordos de nível de serviço com tempos máximos de resposta e recuperação, testes regulares de recuperação (*disaster recovery*) e continuidade de negócio e planos de contingência e procedimentos de *fallback*.

A quarta secção define as responsabilidades dos diferentes intervenientes da organização.

A gestão de risco de fornecedores exige uma distribuição clara, fundamentada e coesa das responsabilidades dos diferentes intervenientes da organização, de modo a garantir que todas as funções contribuem de forma permanente e coordenada para a identificação, avaliação, mitigação e monitorização dos riscos associados à cadeia de fornecimento.

Assim, a definição da matriz de responsabilidades da organização deve ter como propósitos assegurar que cada função dentro da organização conhece e assume o seu papel na gestão de risco de terceiros, deve também promover a coordenação entre as diferentes linhas de defesa da organização, alinhar a atuação dos diferentes intervenientes com as obrigações regulamentares e as melhores práticas internacionais e por fim, praticar uma cultura organizacional na qual a gestão de risco de fornecedores seja reconhecida como uma responsabilidade transversal e uma prioridade estratégica para a organização.

A título de exemplo, a organização pode recorrer ao modelo das Três Linhas de Defesa (*Three Lines Model* – IIA, 2020) para construir a sua matriz de responsabilidades - a primeira linha de defesa é suportada pelas funções operacionais, a segunda linha de defesa envolve as funções de controlo e supervisão e a terceira linha de defesa é constituída pela auditoria interna e *compliance*. Apresenta-se de seguida, o exemplo de um quadro com as principais responsabilidades atribuídas por função, designada matriz de responsabilidades, dirigida neste caso concreto a operadores de serviços críticos.

Tabela 1 - Matriz de Responsabilidades

Função	Responsabilidade
Conselho de Administração	Aprovação da política e supervisão estratégica do apetite ao risco da organização. Compete-lhe assegurar que os princípios e orientações definidos para a gestão de risco de fornecedores estão alinhados com os objetivos estratégicos da organização e que se encontram refletidos nos mecanismos de *governance*, controlo interno e prestação de contas.
CISO (*Chief Information Security Officer*)	Definição e execução da estratégia de segurança da informação aplicada à gestão de risco de fornecedores através do desenvolvimento de normas e procedimentos técnicos, da identificação e implementação de controlos internos e da promoção de uma cultura de segurança na organização.
Departamento de Compras / *Procurement*	Integração dos requisitos e critérios de cibersegurança nos processos de seleção e contratação de fornecedores em articulação com o CISO e com o departamento jurídico para que seja considerado o perfil de risco do fornecedor, o nível de criticidade e a capacidade de resposta do mesmo aos requisitos de segurança da organização.
Departamento Jurídico	Assegurar a inclusão de cláusulas contratuais adequadas que reflitam os requisitos internos de segurança da informação, de continuidade de negócio e de proteção de dados respeitando as obrigações legais e regulamentares aplicáveis.
Equipas Operacionais	As equipas responsáveis pela execução dos serviços suportados por fornecedores são responsáveis pela implementação efetiva dos controlos de segurança previstos para cada fornecedor, bem como da monitorização contínua da sua performance e do cumprimento dos requisitos definidos. Estas equipas devem colaborar na avaliação de risco, responder a alertas e incidentes, e sustentar os mecanismos de *report* e revisão.
Auditoria Interna / *Compliance*	Assegurar a verificação da conformidade da organização com os princípios e procedimentos estabelecidos na Política e promover a melhoria contínua.

Para organizações com estruturas simplificadas ou para organizações com estruturas setoriais como o caso de hospitais, a matriz de responsabilidades deve ser adaptada partindo de uma perspetiva diferente que pode ser uma perspetiva por processos, por roles ou outra.

Na quinta secção da política pretende-se documentar o ciclo de vida da gestão de risco de fornecedores com a definição das fases que constituem esse ciclo. Este ciclo de vida deve ser revisto periodicamente e articulado com os restantes processos de gestão de risco da organização garantindo uma abordagem coerente e compatível na defesa da sua resiliência digital. Dentro de cada fase deverão ser definidas as atividades e responsabilidades específicas.

A sexta secção deve indicar quais os mecanismos de controlo, avaliação e melhoria contínua a serem implementados pela organização de forma a avaliar a eficácia dos controlos implementados, a adequação das práticas adotadas face à evolução do contexto externo e a avaliação da sua maturidade na gestão de risco da sua cadeia de fornecedores. A política de gestão de risco de fornecedores deve ser revista anualmente ou sempre que ocorram alterações relevantes no contexto interno ou externo.

Por último, na sétima seção deve estar definido quais as medidas corretivas a aplicar em caso de incumprimento da política nos termos da legislação aplicável.

Após a aprovação e publicação interna da Política para que ela seja efetivamente operacionalizada, é fundamental que a organização crie processos e procedimentos que traduzam de um modo prático os princípios e as diretrizes descritos na Política em ações concretas. Assim, sugere-se a criação dos seguintes procedimentos complementares:

1. Procedimento de Seleção e Classificação de Fornecedores;
2. Procedimento de *Due Diligence* de Terceiros;
3. Procedimento de Gestão de Fornecedores ao longo do ciclo de vida;
4. Procedimento de Gestão de Incidentes de Terceiros;
5. Plano de Formação e Sensibilização.

c) A **3ª atividade** é a definição dos requisitos mínimos que são exigidos aos fornecedores para o serviço ser prestado com segurança.

A definição de requisitos mínimos de cibersegurança aplicáveis aos fornecedores da organização constitui uma atividade essencial no processo de gestão de risco de terceiras partes. Estes requisitos funcionam como patamares de segurança obrigatórios que os fornecedores devem cumprir como condição prévia para a formalização do contrato. Com o cumprimento destes requisitos, a organização consegue mitigar riscos provenientes de más práticas, de

vulnerabilidades conhecidas ou de ausência de controlos nos sistemas e processos dos fornecedores.

Os requisitos mínimos são definidos com base em três eixos principais:

1. Descrição da tipologia e natureza dos serviços a contratar – a abordagem baseada na tipologia e natureza dos serviços permite uma aplicação proporcional dos controlos de segurança uma vez que tipologias e naturezas de serviço distintas apresentam níveis de risco distintos, o que por sua vez permite que os mecanismos de controlo sejam orientados de modo eficaz para os níveis de risco mais críticos.

   No caso da contratualização de serviços *Cloud* (IaaS, PaaS e SaaS) implica a externalização total ou parcial de infraestruturas, plataformas ou aplicações com diferentes riscos associados, designadamente os que se relacionam com:

   a) Perda de controlo sobre os ativos de informação – ao externalizar total ou parcialmente a infraestrutura da organização, plataformas ou aplicações, a organização perde capacidade de gestão sobre esses ativos o que limita o seu controlo sobre configurações, atualizações, controlo de acessos, entre outros.
   b) Modelo de *multi-tenancy* - a coexistência de dados e de aplicações provenientes de entidades diferentes num mesmo ambiente provoca riscos associados à segmentação que são particularmente críticos quando se trata de informação sensível, como o comprometimento por *cross-site scripting*, a possibilidade de ataques por via de movimentos laterais ou a exfiltração de dados através de *covert channels*.
   c) Dependência crítica do fornecedor – a organização devido a dificuldades tecnológicas ou operacionais como a migração de serviço ou a portabilidade dos dados pode-se tornar excessivamente dependente de um prestador de serviços.
   d) Acesso não autorizado por terceiros – quando o prestador de serviços transfere para o fornecedor uma parte significativa da responsabilidade pela gestão dos seus serviços *cloud*, os prestadores ao desempenharem essas funções de suporte mantêm frequentemente o acesso privilegiado aos sistemas e dados do cliente com privilégios de administrador e com visibilidade *multi-tenancy*.
   e) Localização e jurisdição dos dados – a localização e jurisdição dos dados constitui uma dimensão crítica na gestão do risco de fornecedores *cloud*, em particular para organizações com obrigações regulatórias reforçadas, ao nível da soberania digital, da proteção legal e do cumprimento do RGPD.

f) *Cloud concentration risk* – a dependência significativa de um número reduzido de grandes fornecedores globais de serviços *cloud*, tais como a *Amazon Web Services* (AWS), o *Microsoft Azure* e *Google Cloud Platform* dá origem ao risco de concentração na *cloud*, o qual representa uma ameaça sistémica com potenciais impactos transversais e simultâneos sobre múltiplas entidades.

Para além do cenário de externalização de serviços *cloud*, é frequente o prestador de serviços ter acesso ou fazer o tratamento de dados pessoais como, por exemplo, o recurso a identificação biométrica, a dados clínicos, informações financeiras, ou outras que contribuam para um agravamento do risco pela natureza dos dados tratados que implique obrigações acrescidas de segurança, controlo e responsabilização, nomeadamente na pseudonimização e encriptação de dados em trânsito e em repouso, no registo e rastreabilidade das operações de tratamento, no controlo de acessos e segregação de funções e na avaliação de impacto sobre a proteção de dados (DPIA) quando aplicável.

A tipologia e a natureza dos serviços a contratar pode também incluir serviços de manutenção remota à infraestrutura interna da organização, serviços de desenvolvimento e/ou integração de *software*, ou outro tipo de serviços no âmbito da cibersegurança.

2. Nível de acesso aos ativos de informação – o tipo de acesso que o fornecedor terá aos ativos de informação da organização constitui o segundo eixo a considerar na definição dos requisitos mínimos.

Destaca-se como mais relevante os seguintes tipos de acesso:

a) Acesso lógico – atribuição de credenciais ao fornecedor que permita aceder remotamente ou localmente aos sistemas da organização através de conta de utilizador, de autenticação via VPN (*Virtual Private Network*) ou de integração via API (*Application Programming Interface*).
b) Acesso com privilégios de administrador – a atribuição de acessos com permissões privilegiadas permite ao fornecedor realizar ações de configuração, de manutenção e de administração nos sistemas operativos, nas bases de dados, nos equipamentos de rede e nas plataformas *cloud*.
c) Acesso físico – a atribuição de acessos presenciais às infraestruturas e instalações da organização, *data centers* ou outros locais onde se encontrem ativos da organização.

d) Acesso indireto – ocorre quando o acesso é concedido a terceiros subcontratados pelo fornecedor que têm acesso aos ativos da organização normalmente sem controlo e monitorização por parte da entidade contratante.

3. Natureza da informação – a natureza da informação que pode ser acedida, editada, partilhada e armazenada pelo fornecedor constitui o terceiro eixo a ser considerado na definição de requisitos mínimos. Este eixo pressupõe que a organização classifique a sua informação de modo que seja previamente analisado o conteúdo da informação, a sua relevância estratégica e o potencial impacto que a consulta, alteração ou destruição da informação poderá ter para a organização.

Assim sendo, a definição de requisitos mínimos deve ter um nível adequado de granularidade e ser ajustado à natureza e criticidade dos serviços prestados, ao nível de acesso que o fornecedor terá aos ativos da organização e à natureza da informação à qual o fornecedor poderá aceder. Esta prática permite harmonizar o número de controlos da organização evitando um subdimensionamento ou o seu contrário dificultando a relação contratual e tornando o processo ineficiente.

10.4 2º Subprocesso - *Onboarding*

No 2º subprocesso, designado *onboarding*, deve-se proceder à fase de avaliação do fornecedor e, em caso de apreciação positiva, o avanço para a contratualização do fornecedor pela organização. Assim:

a) A **1ª atividade** consiste (1) na partilha dos requisitos mínimos de segurança definidos pela organização (previamente definidos no momento do planeamento) junto do fornecedor e (2) na recolha da informação necessária que permita avaliar se esses requisitos estão a ser cumpridos pelo fornecedor e com base nisso aferir qual o seu nível de risco.

A atividade de verificação do cumprimento dos requisitos mínimos de segurança tem por objetivo avaliar a maturidade digital e a capacidade de o fornecedor assegurar a proteção dos ativos de informação da organização sobre os quais passará a ter acesso depois de formalizado a contratualização do serviço.

Esta avaliação pode assumir diferentes formas, consoante o grau de criticidade do serviço e a sensibilidade da informação envolvida, incluindo:

- Questionários de *due diligence* técnica;
- Solicitação de documentação e certificações no âmbito da segurança de informação;

- Entrevistas com responsáveis de cibersegurança do fornecedor;
- Auditorias de segunda parte ou *assessments* remotos.

1. Questionários de *due diligence* técnica

Os questionários de *due diligence* configuram-se como instrumentos estruturados de recolha sistemática de informação, e por isso, permitem obter informação sobre aspetos essenciais relacionados com as políticas e procedimentos de segurança em vigor na entidade externa, a estrutura organizacional dedicada à cibersegurança, a existência de planos de resposta a incidentes e continuidade de negócio, ou a implementação de controlos técnicos fundamentais.

A sua aplicação deve ser criteriosamente adaptada à natureza dos serviços a contratar e ao grau de exposição ao risco, garantindo assim uma avaliação proporcional e eficaz. A análise das respostas deve ser conduzida por profissionais com competências técnicas especializadas, podendo ser complementada por um sistema de pontuação que permita aferir o nível de risco.

2. Solicitação de documentação e certificações

A análise documental permite recolher evidências objetivas sobre a existência e a implementação de práticas adequadas de cibersegurança. Esta etapa centra-se na solicitação de documentação que evidencie o grau de maturidade e conformidade do fornecedor face a normativos, padrões internacionais e boas práticas do setor. Esta atividade deve ser encarada apenas como um indicador.

Entre os documentos mais relevantes e que podem ser incluídos na solicitação de documentação destacam-se os seguintes:

- As políticas internas de segurança da informação, que evidenciem o enquadramento estratégico e os princípios orientadores adotados pelo fornecedor;
- Os relatórios de auditoria externa ou interna, que revelem a periodicidade, abrangência e resultados de avaliações independentes aos controlos de segurança do fornecedor;
- Os certificados de conformidade de certificações reconhecidas internacionalmente, como a ISO/IEC 27001;
- Os resultados de testes de intrusão, mapeamento de vulnerabilidades e exercícios de segurança, que comprovem a execução de medidas preventivas e a identificação ativa de vulnerabilidades nos sistemas.

Os testes de intrusão irão permitir à organização (1) obter uma avaliação técnica da robustez dos sistemas do fornecedor face a ataques reais, isto porque ao simular cenários ofensivos, estes testes confirmam a eficácia dos mecanismos de defesa declarados (*firewalls*, WAFs, IDS/IPS, etc.), (2) revelam falhas que não foram detetadas em auditorias formais ou avaliações documentais e (3) avaliam a resiliência a técnicas comuns de ataque (como o caso de *SQL injection*, *privilege escalation*, *credential stuffing* e *lateral movement*).

Ao exigir a apresentação de resultados recentes de testes de intrusão como parte do processo de *onboarding*, a organização recebe a garantia de que o fornecedor previamente já submeteu os seus ativos a escrutínio técnico independente, e cria um incentivo a que o fornecedor periodicamente teste os seus ativos de modo a identificar e remediar vulnerabilidades detetadas.

Com base nisso, e antes da formalização do contrato, a organização pode impor medidas corretivas obrigatórias, definir cláusulas específicas sobre prazos de mitigação, responsabilidades ou reavaliações periódicas, e estabelecer SLAs específicos com base nas vulnerabilidades detetadas nos testes e no tempo de remediação.

O fornecedor ao se dispor a partilhar os resultados dos seus testes de intrusão, ainda que sob acordo de confidencialidade, demonstra ter um indicador qualitativo de transparência e compromisso com boas práticas de cibersegurança.

Por outro lado, a recusa em disponibilizar os resultados de testes ou a ausência da execução dos mesmos deve ser considerado pela organização como um fator de risco adicional ou até ser impeditivo da celebração do contrato.

Os documentos só deverão ser considerados se o âmbito certificado incluir os serviços a contratar, se o certificado estiver dentro do seu prazo de validade e se o organismo certificador cumprir com os requisitos de independência e imparcialidade.

3. Entrevistas com os responsáveis pela cibersegurança da entidade externa

A realização de entrevistas técnicas com os principais responsáveis pela cibersegurança no fornecedor ou outros elementos relevantes da equipa técnica é particularmente importante, no caso de serviços considerados críticos ou que envolvam o tratamento de dados sensíveis. Estas entrevistas assumem um papel complementar à análise documental, permitindo aprofundar o entendimento e esclarecer aspetos ambíguos ou omissos identificados na fase de análise documental.

Permitem também avaliar o grau de envolvimento da gestão de topo, compreender os mecanismos de aplicabilidade dos controlos e verificar qualitativamente a consistência entre a informação prestada e a realidade operacional.

Este contacto direto permite ainda observar a cultura organizacional do fornecedor que contribuirá posteriormente ao longo da vigência do contrato para uma comunicação mais fluída e articulada entre o fornecedor e a organização, se a mesma estiver em sintonia.

As entrevistas técnicas devem ser planeadas com rigor, conduzidas por profissionais com competências em cibersegurança e orientadas por guiões de avaliação previamente estruturados, que assegurem a comparabilidade das respostas e a objetividade do processo.

4. Auditorias de segunda parte ou *assessments* remotos

A organização pode ainda realizar auditorias de segunda parte, conduzidas diretamente pelas suas equipas ou por entidades por si mandatadas. Estas auditorias podem ser presenciais e ocorrerem nas instalações do fornecedor, embora seja menos frequente, ou remotas. Neste caso, os trabalhos de auditoria realizam-se através de sessões de *walkthrough*, de entrevistas aos *focal points* e à revisão de documentação técnica.

Este tipo de auditoria permite verificar a aplicação prática dos controlos, simular cenários operacionais, e recolher evidências diretas da implementação de medidas de segurança.

Apesar de representar para a organização um esforço financeiro e logístico desencadear, em conjunto, as diferentes formas de avaliação aos fornecedores, deve ser tida em consideração que utilizadas em conjunto, estas diferentes formas potenciam uma tomada de decisão mais informada sobre a continuidade do processo de contratação do fornecedor, e, por conseguinte, permite à organização mitigar riscos desde a fase inicial.

O término da primeira atividade traduz-se na identificação do perfil de risco do fornecedor. Realizada esta primeira atividade da qual resultará uma análise multidimensional que integra o grau de maturidade em cibersegurança, a identificação do perfil de risco do fornecedor deverá ser o elemento decisivo para a tomada de decisão quanto à contratualização da prestação do serviço.

Em caso de adjudicação, e com vista a alinhar o nível de risco do fornecedor com o apetite ao risco da organização, esta poderá adicionalmente impor algumas medidas corretivas previamente à celebração do contrato.

Esta atividade reveste-se de particular relevância num contexto de ameaças crescentes e de dependência tecnológica cada vez mais acentuada, porque funciona como um primeiro filtro de segurança no processo de integração de terceiros no ecossistema digital da organização.

b) A **2ª atividade** consiste na avaliação e tratamento do risco. Com base na avaliação de risco deve ser realizado um alinhamento do processo de homologação de fornecedores com a inclusão, se necessário, de requisitos de segurança específicos, nomeadamente para fornecedores que tenham acesso a ativos críticos da organização.

Concluída a fase de recolha de informação e de análise preliminar para aferir o nível de risco do fornecedor, a organização deve prosseguir com a avaliação formal do risco associado à contratação do fornecedor. O propósito da avaliação de risco é determinar a exposição residual da organização ao risco, tendo em consideração a probabilidade de ocorrência e impacto potencial das ameaças identificadas.

A atividade de avaliação e tratamento do risco deve seguir uma metodologia reconhecida como por exemplo, a ISO/IEC 27005, ou seguir uma metodologia interna desenvolvida pela organização e que tenha em consideração os seguintes elementos:

1. Integração com o processo de homologação de fornecedores

A avaliação de risco deve estar integrada com o processo de homologação de fornecedores, de forma a assegurar que apenas entidades que cumpram determinados níveis de segurança sejam elegíveis para contratação. Desta forma, a homologação passa a depender de critérios económicos, operacionais e de requisitos de cibersegurança.

Esta integração deve materializar-se, designadamente, pela inclusão de controlos obrigatórios no processo de qualificação, nomeadamente para fornecedores que:

- Tenham acesso lógico a sistemas ou redes internas;
- Tratem ou armazenem dados pessoais ou sensíveis;
- Prestem serviços de suporte remoto, desenvolvimento de *softwar*e, operação de infraestruturas críticas ou de *cloud computing*;
- Tenham acesso físico a instalações da organização ou aos seus *data centers*.

2. Estimativa do risco residual

A análise de risco deve resultar na estimativa do risco residual, ou seja, o risco que subsiste após a implementação desses controlos por parte do fornecedor. Esta análise deve ser baseada

numa grelha de criticidade ou matriz de risco previamente definida, que permita distinguir entre fornecedores de risco baixo, moderado ou elevado.

a) Tratamento do risco

Nos casos em que o risco residual seja superior ao nível de tolerância definido pela organização, deve ser elaborado um plano de tratamento do risco, que pode incluir:

- A exigência de medidas de mitigação adicionais;
- A revisão dos níveis de acesso a conceder ao fornecedor;
- A imposição de cláusulas contratuais adicionais em matéria de segurança da informação;
- Ou a recusa da contratação com a recomendação de reavaliar a solução técnica proposta.

A responsabilidade pela definição e validação deste plano deve ser partilhada entre o CISO e a equipa de segurança e risco, as equipas operacionais e o departamento jurídico.

3. Formalização da decisão

A decisão sobre a adjudicação deve estar formalmente documentada e sustentada pela análise de risco realizada, constituindo parte integrante do processo de homologação.

Para fornecedores classificados com criticidade elevada, recomenda-se a aprovação explícita por instâncias superiores (como o Conselho de Administração ou o Comité de Risco da organização).

4. Ciclo de melhoria contínua

Os dados recolhidos durante esta fase devem contribuir para o processo de melhoria contínua, evolução dos critérios de avaliação, dos modelos de risco e das exigências impostas a fornecedores, em linha com a evolução do contexto de ameaças e das exigências regulamentares.

10.5 3º Subprocesso - *Management*

O 3º subprocesso é dirigido à gestão do contrato. Sugere-se que sejam os *contract owners* a assumir as atividades seguintes.

A **1ª atividade** consiste na monitorização e na medição dos requisitos contratualizados através:

1. da monitorização dos acordos de nível de serviço previamente definidos aquando da elaboração do contrato;

2. da gestão de indicadores de desempenho dos fornecedores, bem como da apresentação de evidências como o resultado de testes ativos de cibersegurança;
3. e por fim, a melhoria do processo de gestão de incidentes relacionado com as terceiras partes.

A gestão contratual representa um momento crítico no ciclo de vida da relação com o fornecedor porque permite avaliar o estado de cumprimento dos requisitos de cibersegurança definidos contratualmente. A monitorização sistemática e a medição objetiva do desempenho do fornecedor são fundamentais para garantir a eficácia dos controlos implementados e para mitigar desvios operacionais que possam comprometer a segurança da organização. A periodicidade dos ciclos de monitorização devem ser proporcionais ao grau de criticidade do serviço prestado e à sensibilidade dos ativos de informação em causa.

Os fornecedores com acesso lógico privilegiado, com envolvimento em processos críticos de negócio ou tratamento de dados pessoais ou sensíveis devem ser submetidos a ciclos de monitorização mais frequentes (trimestrais ou semestrais), ao passo que fornecedores de menor risco poderão ser avaliados anualmente.

Esta 1ª atividade desdobra-se em três eixos operacionais:

1. Monitorização dos Acordos de Nível de Serviço

Os Acordos de Nível de Serviço estabelecem métricas formais sobre a qualidade, disponibilidade e segurança dos serviços prestados. Durante a fase contratual, é essencial que as organizações monitorizem periodicamente o cumprimento dos SLAs, sobretudo os que dizem respeito a tempos de resposta a incidentes, disponibilidade de sistemas críticos, tempos de recuperação (RTO - *Recovery Time Objective* e RPO - *Recovery Point Objective*), periodicidade de aplicação de *patches* de segurança, níveis mínimos de encriptação de dados em repouso e em trânsito ou atualização de sistemas.

A monitorização regular dos SLAs deve ser realizada por via de relatórios periódicos fornecidos pelo fornecedor e/ou por mecanismos de verificação independente como *logs*, *dashboards* integrados ou soluções de SIEM (*Security Information and Event Management*).

Quando são detetadas não conformidades com os níveis acordados, devem ser acionados os mecanismos corretivos que se encontram previstos no contrato, sendo que os mais comuns são os planos de remediação, as penalizações financeiras, a reavaliação de risco ou a renegociação de cláusulas contratuais que pode, em situações graves, desencadear a rescisão contratual.

2. Gestão de Indicadores de Desempenho de Cibersegurança

Os KPIs de cibersegurança são métricas operacionais utilizadas para avaliar o desempenho real do fornecedor ao longo do contrato. Ao contrário dos SLAs, que são estipulados *ex ante*, os KPIs podem ser ajustados consoante a evolução do contexto de risco e a maturidade da relação contratual. Assim, a adoção de KPIs direcionados aos fornecedores permite uma monitorização mais granular e baseada em evidência.

Entre os KPIs mais relevantes pode-se incluir os seguintes:

• Cyber Risk Rating: avaliação contínua do perfil de risco do fornecedor, baseada em dados externos e técnicas de *threat intelligence*. A maioria das plataformas apresenta o *Cyber Risk Rating* com uma escala numérica. A título de exemplo:

• A *BitSight* apresenta o *score* do *Cyber Risk Rating* numa escala de 250 a 900 pontos, o que significa que quanto mais alto for o score apresentado, maior é a capacidade da organização de mitigar o risco de exposição a ciberameaças.

• A *SecurityScorecard* apresenta o score do *Cyber Risk Rating* numa escala de A a F, sendo A a representação de risco baixo e F a representação de risco elevado.

• Os *rankings* setoriais permitem comparações do *Cyber Risk Rating* do fornecedor com a média da indústria ou do país.

Esta pontuação de risco é geralmente calculada por plataformas especializadas de *cyber risk intelligence*, como a *BitSight*, a *SecurityScorecard*, a *RiskRecon*, a *UpGuard*, a *Panorays*, entre outras. O cálculo da sua pontuação combina várias dimensões técnicas e comportamentais, a partir da recolha automática de dados externos que contêm designadamente:

a) A avaliação de ativos expostos através da (1) identificação dos domínios, subdomínios, IPs e servidores públicos pertencentes ao fornecedor; (2) da deteção de sistemas obsoletos, expostos, ou mal configurados (caso de servidores com TLS (*Transport Layer Security*)) desatualizado, portas abertas, *headers* inseguros) e (3) da avaliação da higiene de DNS (*Domain Name System*) e dos registos SPF (*Sender Policy Framework*), DKIM (*Domain Keys Identified Mail*), DMARC (*Domain-based Message Authentication, Reporting & Conformance*).
b) A deteção de vulnerabilidades conhecidas a partir da verificação da existência de vulnerabilidades técnicas (CVEs - *Common Vulnerabilities and Exposures*) associadas aos sistemas do fornecedor, e da análise da prontidão na correção de falhas conhecidas.

c) A evidência de comprometimento através da presença do fornecedor em bases de dados de credenciais comprometidas (*Data Breaches*), da inclusão em listas negras (*Blacklists*) ou reputação negativa de IPs; ou da deteção de atividades maliciosas (como *spam* ou *botnets*) originadas a partir da infraestrutura do fornecedor.
d) A resiliência da segurança técnica através da configuração de *firewalls*, *proxies*, *headers* de segurança e certificados digitais; do uso de protocolos seguros (HTTPS - *Hypertext Transfer Protocol Secure* ou SFTP - *Secure File Transfer Protocol*) e da aplicação de medidas de proteção de e-mail e prevenção de *spoofing*.
e) O histórico de incidentes e tempo de resposta através da análise do tempo médio de remediação de vulnerabilidades e do histórico de incidentes reportados publicamente.
f) As avaliações de segurança interna (quando disponíveis) a partir dos resultados de auditorias independentes (por exemplo: SOC 2, ISO 27001).

• Resultados de Testes de Intrusão (*Pentesting*): deverá ser verificada a realização periódica de testes de intrusão por parte do fornecedor e solicitar para além do resultado dos testes, as medidas de remediação adotadas e respetivos planos de ação com indicação do prazo de execução. A organização pode ainda incluir estes relatórios como parte dos indicadores de desempenho avaliados nas revisões contratuais.

• Mapeamento de Vulnerabilidades: a análise contínua destes relatórios irá permitir detetar vulnerabilidades recentemente introduzidas pelo fornecedor em virtude de alterações de configuração, atualizações de *software* ou mudanças na arquitetura tecnológica. Além disso, possibilita avaliar periodicamente a maturidade do fornecedor no que respeita à sua capacidade de remediação.

A organização ao analisar o relatório disponibilizado pelo fornecedor deve incluir, entre outros aspetos: a verificação da severidade e tipo das vulnerabilidades identificadas; a existência de *exploits* conhecidos associados; a eficácia e tempestividade das medidas corretivas implementadas; a atualidade e abrangência do scan realizado e a validação da ferramenta e metodologia utilizadas.

Se se constatar a indicação no relatório da existência de vulnerabilidades críticas não mitigadas ou falhas reincidentes pode constituir fundamento para a aplicação de medidas corretivas, penalizações contratuais ou mesmo a reavaliação do perfil de risco atribuído ao fornecedor. Estas ações, nesta fase, já devem estar previstas nos mecanismos contratuais e por isso, integradas nos processos internos de gestão de terceiros.

• Cumprimento de obrigações de *reporting* e comunicação de incidentes.

A comunicação de incidentes rege-se por mecanismos formais de notificação, previamente acordados entre a organização e o fornecedor em articulação com as restantes normas contratuais, as obrigações legais e regulamentares e a própria política interna de resposta a incidentes.

A frequência e a classificação dos incidentes reportados pelo fornecedor ao longo da relação contratual permitirá à organização identificar padrões de falhas estruturais, potenciais fragilidades nos processos de segurança do fornecedor e, em casos mais graves, risco de comprometer a continuidade de negócio da organização. Contudo, se se verificar a ausência de incidentes, esta não deve ser interpretada como uma ausência total de risco, mas sim avaliada à luz da maturidade do processo de deteção, da transparência do fornecedor, e da robustez dos mecanismos de *report*.

A monitorização contínua dos prazos e canais de *report* acordados deve incluir, entre outros, os seguintes aspetos: o número total de incidentes por período (mensal ou trimestral); a classificação por tipologia e criticidade; os tempos de deteção e resposta; o impacto estimado nos serviços ou dados da organização e as medidas corretivas adotadas e lições aprendidas.

A organização, com esta informação deve alimentar o sistema de KPIs e de KRIs na reavaliação periódica do perfil de risco do fornecedor. Não obstante, os fornecedores com um histórico de incidentes frequentes, não reportados atempadamente ou mal geridos, devem ser objeto de escrutínio acrescido, podendo justificar ações como auditorias extraordinárias, revisão dos SLAs, imposição de medidas compensatórias ou, em última instância, rescisão contratual.

A monitorização do cumprimento destas obrigações permitirá reforçar a confiança na relação contratual e permitir uma resposta coordenada em situações críticas o que reforça positivamente a avaliação quanto à continuidade do contrato celebrado com o fornecedor.

3. Melhoria Contínua do Processo de Gestão de Incidentes com Terceiros

O processo de gestão de incidentes com terceiros deve incluir procedimentos de notificação de incidentes em tempo útil (com prazos máximos definidos contratualmente e canais de contacto preferenciais); exercícios conjuntos de simulação de incidentes; análise pós-incidente com envolvimento do fornecedor e atualização dos planos de resposta e continuidade com base nas lições aprendidas.

Quanto aos procedimentos conjuntos de resposta a incidentes, os planos de resposta da organização devem incorporar fluxos que incluam os fornecedores, especialmente quando estes têm acesso direto a sistemas ou dados críticos. A interoperabilidade dos processos e a partilha de informação devem estar previstas e testadas.

A realização de exercícios conjuntos irá permitir testar a eficácia dos mecanismos de resposta, identificar lacunas e promover o alinhamento entre as partes. Estes exercícios devem ser realizados periodicamente, sobretudo em contratos de serviços críticos.

A análise pós-incidente deve ser realizada após cada incidente no sentido de ser efetuada uma análise estruturada para apurar as causas, impactos e falhas de coordenação, resultando em planos de ação concretos. A partilha desta análise com o fornecedor contribui para uma cultura de melhoria contínua. Com base nos incidentes ocorridos, devem ser avaliadas e, se necessário, revistas as medidas de controlo, os KPIs associados e até as cláusulas contratuais, incorporando as lições aprendidas e dessa forma, reforçando a resiliência de cada uma das organizações.

A **2ª atividade** consiste:

1. **Na gestão do ciclo de vida dos dados que estão sob a gestão de fornecedores (através por exemplo da implementação de ferramentas de *Data Loss Prevention* (DLP))**

A gestão do ciclo de vida dos dados sob a responsabilidade dos terceiros contratados constitui uma dimensão crítica para salvaguarda da confidencialidade, integridade e disponibilidade da informação. Isto verifica-se na externalização de serviços designadamente, quando envolve tratamento ou armazenamento de dados sensíveis ou críticos, que implica a transferência parcial de controlo sobre os dados, aumentando substancialmente a superfície de exposição a riscos operacionais, legais e reputacionais.

A implementação de soluções de DLP junto dos fornecedores ou, em alternativa, a exigência da sua adoção como requisito contratual, deve ser proporcional ao nível de risco identificado, com base na criticidade do serviço prestado e na natureza dos dados envolvidos. Quando a prestação de serviços envolve o tratamento de dados pessoais ou sensíveis, propriedade intelectual ou informação estratégica para a organização, os fornecedores devem ser abrangidos por esta medida.

Na prática, a gestão eficaz deste ciclo de vida exige a proteção da informação em todas as suas fases desde a sua criação ou recolha, passando pela transmissão, processamento e armazenamento, até à sua eliminação segura.

Neste contexto e como medida para mitigar o risco associado é recomendável a implementação de mecanismos como as ferramentas de DLP que permitem detetar e bloquear transferências não autorizadas de informação sensível para fora do perímetro autorizado, incluindo por canais como e-mail, dispositivos de armazenamento removível ou plataformas *cloud*.

Esta ferramenta permite também aplicar políticas automáticas de proteção com base no conteúdo da informação (a título de exemplo, informação relativa aos números de cartões de crédito, dados de saúde ou credenciais), no seu contexto (como é o caso do perfil do utilizador ou da localização geográfica) ou no seu comportamento (por exemplo em caso de atividades anómalas). Pode também monitorizar em tempo real a movimentação de dados, mesmo em ambientes híbridos ou em dispositivos fora da infraestrutura da organização e produzir evidência para fins de auditoria e controlo interno, apoiando a demonstração de *accountability* perante as autoridades reguladoras.

A verificação da eficácia desta solução deve fazer parte das atividades de monitorização contínua, podendo incluir testes técnicos, análise de registos de incidentes e revisões periódicas de configuração e cobertura. Quando se verificar a ausência ou deficiente aplicação desta ferramenta, que se pode traduzir num sinal de maturidade reduzida na gestão da informação, justificar-se-á medidas corretivas ou a reavaliação do risco residual associado ao fornecedor.

2. Na revisão periódica de acessos

A revisão periódica de acessos quando devidamente implementada, assegura que os direitos de acesso concedidos a entidades terceiras nomeadamente fornecedores ou aos seus subcontratantes permanecem alinhados com os princípios do privilégio mínimo, da necessidade de conhecimento e da proporcionalidade face às funções desempenhadas.

Desse modo, permite detetar e corrigir situações de excesso de permissões, contas inativas, contas sem uso, ou acessos que deixaram de ser justificáveis, seja por alterações no âmbito do contrato, na função do utilizador ou outra. Neste caso, esta medida contribui para reduzir a superfície de ataque em caso de comprometimento de credenciais e evita movimentos laterais que possibilitem a escalada de privilégios. De igual forma, assegura a conformidade com obrigações legais e regulamentares.

A implementação desta atividade pressupõe a criação de um processo formal de revisão de acessos que deverá contemplar os seguintes elementos estruturantes:

a) Periodicidade diferenciada consoante o grau de risco

A frequência das revisões deve ser estabelecida com base no nível de criticidade do serviço e da sensibilidade dos sistemas ou dados acedidos. É recomendável que os acessos privilegiados ou *admin* sejam alvo de revisão mensal ou trimestral, os acessos lógicos a informação sensível sejam revistos trimestral a semestral e os acessos físicos sejam alvo de revisão anual, ou aquando da modificação do contrato.

a) Inventário atualizado dos acessos concedidos

É fundamental a existência de um repositório fiável que documente todos os acessos atribuídos a fornecedores, incluindo a sua tipologia (*admin*, privilegiado, lógico ou físico), o sistema de destino, a data de concessão e a entidade que autoriza.

c) Envolvimento das áreas relevantes

A revisão deverá envolver de forma articulada a área ou unidade de negócio que, dentro da organização, identificou a necessidade de recorrer a serviços externos e promoveu a sua aquisição, os administradores de sistemas ou os responsáveis pela gestão de identidades e a função responsável pelo *governance* e supervisão das práticas de segurança da informação, frequentemente atribuída ao CISO.

d) Procedimentos de revogação e remediação

Perante a identificação de acessos indevidos ou não autorizados por parte do fornecedor, devem ser desencadeados os procedimentos formais de revogação de credenciais, acompanhados da notificação das partes interessadas. Sempre que se justifique, deverão igualmente ser adotadas medidas corretivas e reforços adicionais aos controlos de segurança, com vista à mitigação de eventuais impactos e à prevenção de recorrência.

e) Auditoria e registos de conformidade

O processo deverá assegurar a produção de registos formais devidamente estruturados, que permitam a realização de auditorias internas e externas, evidenciando a adoção de medidas de diligência razoável na gestão dos acessos concedidos a entidades terceiras.

No cenário de adoção de arquiteturas em *cloud* e de integrações técnicas avançadas como os interfaces de programação de aplicações (APIs) e o *Single Sign-On* (SSO), a revisão periódica de acessos deve ser adaptada às especificidades das tecnologias envolvidas. Assim, em ambientes *cloud*, é essencial assegurar que as sessões ativas e os *tokens* associados a contas de fornecedores são periodicamente analisados, nomeadamente após alterações contratuais, saídas de colaboradores do lado do fornecedor ou revisão de âmbito do serviço. Os *tokens* com longas durações ou que não têm controlo centralizado representam vetores de risco significativos, sendo, por isso, recomendada a sua rotatividade e expiração controlada.

Adicionalmente, a existência de contas de serviço utilizadas em processos automatizados, designadamente para integração contínua, transferência de dados ou execução de tarefas em segundo plano, requer uma monitorização diferenciada. Estas contas, frequentemente dotadas de

permissões elevadas, devem estar sujeitas a políticas específicas incluindo a revisão periódica dos privilégios atribuídos, a segregação de funções e a restrição do seu uso a finalidades bem delimitadas e justificadas.

Outro aspeto prende-se com a verificação da ausência de credenciais partilhadas entre múltiplos elementos do fornecedor. A utilização de contas comuns compromete a rastreabilidade e a responsabilização individual, dificultando a identificação da origem de potenciais incidentes de segurança. Caso a partilha de credenciais se revele tecnicamente inevitável, devem ser implementados mecanismos de controlo rigoroso, tais como a autenticação multifator, o registo detalhado de atividades (*logging*) e a auditoria periódica dos acessos.

Por fim, neste tipo de contextos tecnológicos, a gestão do ciclo de vida dos acessos por parte dos fornecedores deve integrar-se numa abordagem de *Zero Trust*, em que nenhum acesso é considerado intrinsecamente fiável e todos os pedidos de autenticação e autorização são sujeitos a verificação. Esta orientação reforça a resiliência das organizações perante um ecossistema de fornecedores cada vez mais distribuído, interdependente e tecnologicamente sofisticado.

3. No direito de auditorias periódicas ao fornecedor

A inclusão contratual do direito de realizar auditorias periódicas aos fornecedores permite verificar, de forma sistemática e independente, o cumprimento e eficácia dos controlos internos implementados, o cumprimento das obrigações contratuais e o grau de maturidade atual dos sistemas de gestão de risco do fornecedor.

A previsão deste direito já se deve encontrar formalizada no contrato, conferindo à organização o poder de planear, executar ou delegar auditorias técnicas, documentais ou operacionais, com especial foco nas áreas críticas, como a gestão de acessos, a proteção de dados pessoais, a continuidade de negócio e a resposta a incidentes. A periodicidade das auditorias deve ser proporcional ao grau de criticidade do serviço prestado, podendo variar entre avaliações anuais em fornecedores estratégicos até verificações mais espaçadas em serviços de risco residual.

As auditorias podem assumir diversas modalidades, desde auditorias *in loco*, com observação direta das infraestruturas e entrevistas às equipas técnicas do fornecedor, até auditorias remotas, baseadas na análise de documentação, registos de *logs* e evidências técnicas. Em casos específicos, é admissível a aceitação de auditorias de terceira parte, nomeadamente quando realizadas por entidades independentes certificadas, desde que exista transparência quanto ao âmbito, metodologia e resultados obtidos.

Para além de garantir a visibilidade sobre os controlos efetivamente aplicados, as auditorias periódicas possibilitam a identificação precoce de fragilidades, e com base nesses resultados, permitem identificar planos de melhoria e acompanhar a execução das medidas corretivas.

Importa a organização esclarecer junto do fornecedor que o exercício do direito de auditoria não deve ser entendido como um ato de desconfiança, mas antes como uma componente integrante da gestão responsável dos riscos de terceiros, reforçando a confiança mútua e a transparência entre as partes.

Neste sentido, recomenda-se que a sua execução seja precedida de comunicação formal, definição clara dos objetivos, âmbito e critérios de avaliação, e conduzida de acordo com os princípios da proporcionalidade, da minimização do impacto e da confidencialidade.

O direito de auditoria deve ainda ser complementado por cláusulas contratuais que prevejam sanções em caso de recusa injustificada, bem como mecanismos de resolução de litígios, de forma a garantir a sua eficácia jurídica e operacional.

4. **Caso surjam alterações ao contexto, na fase de monitorização podem também ser equacionadas alterações ao contrato**

Assente numa abordagem dinâmica e adaptativa a gestão de risco de fornecedores, importa reconhecer que o contrato celebrado entre a organização e o prestador de serviços não deve ser entendido como um instrumento estático, mas antes como um instrumento sujeito a revisões sempre que se verifiquem alterações ao contexto do risco. Neste sentido, a fase de monitorização contínua, como sugerido nas atividades anteriores, assume um papel central na verificação da conformidade, mas também o pode fazer na deteção de sinais que justifiquem a revisitação e, se necessário, a renegociação das cláusulas contratuais.

Estas alterações de contexto podem assumir diversas formas, incluindo, mudanças na criticidade do serviço prestado, em resultado da sua maior integração com os processos de negócio da organização. Podem também ser decorrentes de atividades anteriores como as auditorias, os testes de intrusão ou o mapeamento de vulnerabilidades, se os resultados indicarem não conformidades ou identificarem vulnerabilidades que revelem lacunas na proteção dos ativos da organização. Poderá igualmente verificar-se transformações operacionais (como a subcontratação de partes do serviço) ou tecnológicas (como a migração para um novo ambiente *cloud*) no fornecedor assim como, incidentes de segurança com impacto direto ou indireto nos ativos da organização. Por fim, no período de vigência do contrato podem ainda surgir atualizações regulatórias ou normativas no domínio da cibersegurança

Perante tais circunstâncias, a organização deve acionar mecanismos de reavaliação do risco e, sempre que necessário, propor alterações contratuais que restabeleçam o equilíbrio entre o nível de exposição ao risco e os controlos internos em vigor. Estas alterações podem incidir, por exemplo, sobre os requisitos técnicos mínimos, os indicadores de desempenho e segurança, os prazos de resposta a incidentes, os mecanismos de *reporting*, as sanções contratuais, ou a exigência de medidas corretivas vinculativas.

A legitimidade e eficácia desta atividade depende da existência prévia de cláusulas contratuais que prevejam a possibilidade de revisão do contrato em função da evolução do risco, bem como de canais de comunicação estabelecidos entre a organização e o fornecedor.

10.6 4º Subprocesso - *Offboarding*

Por fim, na fase de *offboarding*, como **1ª atividade** deve ser definido e implementado o plano de saída e de transição do fornecedor aquando do término e/ou da transferência do contrato, onde deve ser definido entre outras, as atividades e o respetivo clausulado referente à transferência e à eliminação da informação, à remoção de acessos e à transição para um novo fornecedor ou à reintegração na operação.

A fase de *offboarding* representa a etapa final no ciclo de vida da relação contratual com os fornecedores e assume especial relevância no contexto da gestão de risco de terceiros, sobretudo quando estão em causa ativos de informação críticos ou dados sensíveis sob a sua responsabilidade. O término do contrato independentemente do seu motivo (cessação prevista, rescisão antecipada ou substituição do prestador) implica a adoção de um conjunto estruturado de medidas destinadas à preservação da confidencialidade e à continuidade operacional da organização.

1. Implementação do processo de saída

O primeiro passo consiste na definição de um plano de saída, acordado contratualmente no momento da fase de contratação, mas operacionalizado na fase de *offboarding*. Este plano deve conter uma descrição detalhada das atividades a desenvolver, dos responsáveis pela sua execução, dos prazos e das garantias associadas. A sua formalização deve incluir a identificação clara dos ativos a restituir, eliminar ou transferir; a definição dos procedimentos de descontinuação técnica; o estabelecimento de canais de comunicação entre as partes e as obrigações pós-contratuais, como os acordos de confidencialidade e de não utilização de dados.

Este plano deverá ser acionado de forma tempestiva e coordenada entre as equipas internas da organização (jurídica, segurança da informação, operações e área requisitante) e o fornecedor em questão.

2. Transferência e eliminação de informação

Um dos elementos mais críticos do *offboarding* é a transferência segura ou a eliminação definitiva da informação detida pelo fornecedor. Esta atividade deve obedecer a requisitos normativos e de segurança rigorosos, assegurando desse modo que todos os dados fornecidos ou gerados durante a execução do contrato são devidamente restituídos à organização, em formatos legíveis e interoperáveis. Esta atividade deve também assegurar que a eliminação dos dados é feita com base em práticas seguras (por exemplo, *data wiping* ou *data shredding*), garantindo a impossibilidade de recuperação posterior e de que o fornecedor emita declarações formais de destruição dos dados, com evidências do procedimento adotado, nomeadamente para dados pessoais, sensíveis ou classificados.

Este ponto é particularmente relevante no contexto do cumprimento do RGPD, que impõe à organização a obrigação de garantir que os dados pessoais tratados por terceiros sejam apagados ou devolvidos no fim da relação contratual.

3. Revogação de acessos

Outro eixo fundamental do subprocesso de *offboarding* prende-se com a revogação sistemática de todos os acessos atribuídos ao fornecedor. Esta medida visa mitigar o risco de acessos indevidos após a cessação do contrato, abrangendo todas as contas de utilizador e acessos lógicos a sistemas, redes e aplicações; acessos físicos a instalações, centros de dados e ambientes sensíveis; acessos *admin* com privilégios elevados e *tokens*, certificados digitais, VPNs e integrações automatizadas via API ou SSO.

Em ambientes baseados em serviços *cloud* é recomendável que sejam revistos e desativados *tokens* persistentes e contas de serviço associadas a tarefas automatizadas.

4. Apoio à transição para um novo fornecedor ou reintegração na operação (*insourcing*)

Nos casos em que a cessação contratual implique a migração dos serviços para um novo prestador ou a sua reintegração nos sistemas e equipas internas da organização (*insourcing*), o subprocesso de *offboarding* deve assegurar uma transição estruturada e controlada, de forma a evitar ruturas na continuidade operacional e a preservar a integridade dos ativos e processos

críticos. Para tal, devem ser previstas e implementadas medidas específicas que promovam a transferência, nomeadamente:

- A transferência sistemática de conhecimento, incluindo documentação técnica, parametrizações relevantes, manuais operacionais e inventário atualizado de ativos afetos ao serviço prestado;
- A cooperação técnica entre o fornecedor cessante e o novo prestador de serviços, operacionalizada através de sessões de transferência estruturada de conhecimento (*hand-over*), devidamente calendarizadas e conduzidas sob supervisão das equipas internas competentes;
- A afetação transitória de recursos humanos qualificados por parte do fornecedor cessante, com o objetivo de prestar apoio técnico durante o período de transição, assegurando a continuidade operacional e mitigando eventuais constrangimentos de natureza técnica ou organizacional;
- A definição de obrigações contratuais relativas à continuidade da prestação de serviços mínimos até que o novo modelo esteja integralmente implementado, de forma a assegurar a salvaguarda das funções críticas da organização e a prevenir interrupções operacionais durante o período de transição.

Estas medidas devem constar expressamente no plano de saída e ser suportadas por cláusulas contratuais robustas, permitindo não só a execução eficaz do processo, mas também a responsabilização das partes envolvidas em caso de incumprimento.

5. Verificação de obrigações contratuais e encerramento formal

A fase de *offboarding* deverá culminar com a verificação integral do cumprimento de todas as obrigações contratuais remanescentes, nomeadamente a devolução de ativos físicos, a conclusão de entregas pendentes e a formalização do término da relação contratual. Este encerramento deve ser devidamente documentado através da elaboração de um relatório de fecho, o qual deverá:

- Registar, de forma sistemática, todas as atividades executadas no âmbito do processo de saída do fornecedor;
- Incluir evidência documental como relatórios de destruição de dados, listas de acessos revogados, registos de devolução de equipamentos ou documentação técnica entregue;

- Identificar oportunidades de melhoria com base nas lições aprendidas, contribuindo para o aperfeiçoamento contínuo do subprocesso de *offboarding* e da gestão do ciclo de vida dos fornecedores.

Por último, como **2ª e última atividade**, após a cessação do contrato deve ser efetuada uma análise comportamental e reputacional do fornecedor, de modo a avaliar a sua postura de segurança, o seu histórico de incidentes e também as vulnerabilidades da cadeia de fornecimento.

Após a cessação formal do vínculo contratual, revela-se pertinente a realização de uma avaliação retrospetiva do desempenho do fornecedor ao longo do período de vigência do contrato, com especial foco nos domínios da segurança da informação e da gestão de risco. Esta atividade visa não apenas encerrar de forma informada o ciclo de fornecimento, mas também alimentar os processos de melhoria contínua e os repositórios internos de conhecimento sobre terceiros.

Neste contexto, a análise deve contemplar múltiplas dimensões, nomeadamente:

- A avaliação da maturidade e da consistência na implementação dos controlos acordados, da capacidade de resposta do fornecedor a exigências adicionais ou emergentes, e do grau de alinhamento com os requisitos normativos e contratuais ao longo da prestação do serviço.
- O registo e análise dos eventos de segurança reportados, do cumprimento dos prazos de notificação, da transparência na comunicação com a organização, bem como a eficácia das medidas corretivas aplicadas. Esta dimensão é essencial para avaliar o comportamento sob pressão e a resiliência operacional do fornecedor.
- Identificação de vulnerabilidades resultantes da dependência de subcontratantes ou de infraestruturas partilhadas, bem como o grau de visibilidade e controlo efetivo exercido sobre terceiros por parte do fornecedor principal. Esta análise contribui para uma compreensão mais ampla da exposição sistémica da organização.

Os resultados desta avaliação devem ser integrados na base de dados interna de qualificação e desempenho de fornecedores, podendo condicionar futuras decisões de contratação. Além disso, a sistematização desta prática reforça uma abordagem de gestão de risco baseada na evidência, promove a responsabilização dos fornecedores e contribui para o fortalecimento global de toda a cadeia digital.

11 Conclusão

A revisão exaustiva da literatura e a análise efetuada nesta investigação permitem concluir que a criação da generalidade dos regulamentos surgiu como resposta a falhas ou a incidentes ocorridos, ou a ausências regulatórias em determinados espectros, em vez da sua criação resultar de uma previsão proativa de possíveis erros futuros. Entende-se que a adoção consistente dos princípios fundamentais da segurança da informação assume um papel central na consolidação de uma cultura organizacional orientada para a resiliência digital.

No âmbito da gestão de risco de terceiros em cibersegurança, os regulamentos apresentam diretrizes sobre o que deve ser prioritário para as organizações e estas deveriam considerá-los como o ponto de partida, isto é, o nível mínimo de desempenho. As organizações devem tomar medidas para diminuir o seu nível de risco até ao nível de esforço máximo que a organização esteja disposta a investir nessa redução, de acordo com a sua tolerância ao risco.

Como verificado, os ataques à cadeia de fornecedores representam uma ameaça significativa à segurança das organizações e por isso devem exigir por parte das mesmas, a adoção de abordagens de defesa holísticas que combinem mecanismos técnicos robustos, práticas de *cyber hygiene*, e uma avaliação contínua do risco associado a terceiros.

Ao longo da relação contratual estabelecida entre a organização e o fornecedor, e dada a complexidade adicional que as repercussões ao longo da cadeia de fornecimento acrescentaram no processo de gestão de incidentes, é essencial que as organizações mantenham processos colaborativos e bem definidos com os seus fornecedores para a deteção, comunicação, contenção e resolução de incidentes.

Com o desenvolvimento desta abordagem incentiva-se a que as ações tomadas pelas organizações com vista à redução do risco não sejam encaradas como simples tarefas burocráticas de cumprimento de uma obrigação de conformidade para satisfazer apenas as exigências de auditores (internos e/ou externos) e reguladores.

A ausência desta postura tem contribuído para que o tema da Gestão de Risco de Terceiros não receba a prioridade e o empenho que realmente exige, mesmo para as organizações que realizam as diligências adequadas, mas que ainda assim, não atingem o nível necessário para uma mitigação eficaz do risco.

Por isso, as organizações que contrariam este *modus operandi*, tendem a estar mais bem protegidas contra ameaças futuras.

Pelo que a adoção de uma abordagem por processo para a gestão de risco de fornecedores apresenta potenciais benefícios, nomeadamente na minimização do risco organizacional e na garantia da continuidade e qualidade dos processos nas organizações.

12 Trabalho Futuro

Como trabalho futuro, sugere-se a implementação prática do modelo e avaliação futura dos seus resultados, através da medição da eficácia da implementação da abordagem por processo com recurso a métricas de desempenho nomeadamente, as melhorias identificadas na qualidade dos processos organizacionais, a robustez das estratégias de mitigação de risco implementadas assim como, a redução de incidentes de cibersegurança desencadeados a partir de fornecedores, parceiros ou terceiras partes da organização.

Por fim, sugere-se a confrontação dos resultados obtidos a partir do estudo de caso com os dados registados antes e depois da implementação da nova abordagem.

13 Referências Bibliográficas

[1] T. J. G. Brás, Arquitetura Informacional de Referência para o Setor da Saúde Portuguesa, Dissertação de Mestrado, out. 2015.

[2] A. R. Hevner et al., "Design Science in Information Systems Research," MIS Quarterly, vol. 28, n.º 1, pp. 75–105, 2004.

[3] H. Hasan, "Information Systems Development as a Research Method," Australasian Journal of Information Systems, vol. 11, n.º 1, pp. 4–13, 2003.

[4] M. Heckmann, T. Comes e S. Nickel, "A Critical Review on Supply Chain Risk – Definition, Measure and Modeling," Omega, 2015; S. Vaidya et al., "Managing Risks in Supply Chains," 2018.

[5] ENISA, "Sobre a ENISA – Agência da União Europeia para a Cibersegurança," 2022. [Online]. Disponível: https://www.enisa.europa.eu/about-enisa/about/pt. [Acedido em: 14-jan-2024].

[6] União Europeia, Diretiva (UE) 2022/2555 (NIS 2), 2022. [Online]. Disponível: https://eur-lex.europa.eu. [Acedido em: 14-jan-2024].

[7] K. Peffers, T. Tuunanen, M. A. Rothenberger e S. Chatterjee, "A Design Science Research Methodology for Information Systems Research," Journal of Management Information Systems, vol. 24, n.º 3, pp. 45–77, dez. 2007, doi: 10.2753/MIS0742-1222240302.

[8] F. C. P. Gil, A Implementação do Regulamento de Cibersegurança (Cybersecurity Act) e o seu Impacto na Cibersegurança, nov. 2021. [Online]. [Acedido em: 02-fev-2024].

[9] ISO/IEC, ISO/IEC 27002:2022 – Information Security Controls, 2022. [Online]. Disponível: https://www.iso.org/standard/75652.html. [Acedido em: 02-fev-2024].

[10] S. AlGhamdi, W. K. Than e E. Vlahu-Gjorgievsk, "Information Security Governance Challenges and Critical Success Factors: A Systematic Review," dez. 2020. [Online]. Disponível: ScienceDirect. [Acedido em: 02-fev-2024].

[11] R. von Solms e J. van Niekerk, "From Information Security to Cyber Security," out. 2013. [Online]. Disponível: ScienceDirect. [Acedido em: 02-fev-2024].

[12] B. von Solms e R. von Solms, "Cybersecurity and Information Security – What Goes Where?," mar. 2013. [Online]. Disponível: Emerald Insight. [Acedido em: 02-fev-2024].

[13] NIST, “Cyber Attack – Glossary,” CSRC. [Online]. Disponível: https://csrc.nist.gov. [Acedido em: 02-fev-2024].

[14] ENISA, “Sobre a ENISA – Agência da União Europeia para a Cibersegurança,” 2022. [Online]. Disponível: https://www.enisa.europa.eu. [Acedido em: 14-jan-2024].

[15] ENISA, ENISA Threat Landscape 2022, 2022. [Online]. Disponível: https://www.enisa.europa.eu. [Acedido em: 14-jan-2024].

[16] NIST, Key Practices in Cyber Supply Chain Risk Management (SP 1100), 2022.

[17] ENISA, Threat Landscape for Supply Chain Attacks, 2021.

[18] C. Hadnagy, Social Engineering: The Science of Human Hacking, 2.ª ed., Wiley, 2018.

[19] R. Anderson et al., Security Economics and the Internal Market, ENISA, 2020.

[20] Procurement Magazine, “WEF: Supply Chains at the Heart of Cybersecurity Threats,” 2025. [Online]. [Acedido em: 06-mai-2025].

[21] Insurance Business Magazine, “Supply Chain Cyberattacks Surge Over 400% – Cowbell Report,” 2025. [Online]. [Acedido em: 06-mai-2025].

[22] SecurityScorecard, The State of Third-Party Cyber Risk 2024, 2025. [Online]. [Acedido em: 06-mai-2025].

[23] SC Media, “Third-Party Risk Remains Key Cybersecurity Concern,” 2025. [Online]. [Acedido em: 06-mai-2025].

[24] BlueVoyant, Global Insights: Third-Party Cyber Risk, 2025. [Online]. [Acedido em: 06-mai-2025].

[25] M. E. Whitman e H. J. Mattord, Principles of Information Security, 2022.

[26] W. Stallings, Computer Security: Principles and Practice, Pearson, 2017.

[27] C. P. Pfleeger e S. L. Pfleeger, Security in Computing, Prentice Hall, 2012.

[28] ISO/IEC, ISO/IEC 27001:2013 – Information Security Management Systems, 2013.

[29] ISO/IEC, ISO/IEC 27000:2020 – Overview and Vocabulary, 2020. [Acedido em: 02-fev-2024].

[30] M. Bishop, Computer Security: Art and Science, Addison-Wesley, 2003.

[31] D. Gollmann, Computer Security, Wiley, 2011.

[32] S. F. R. Palma, Um Modelo de Apreciação de Risco IT de Terceiros, Dissertação de Mestrado, Universidade de Lisboa, 2023. [Online]. [Acedido em: 10-jun-2024].

[33] Portugal, Lei n.º 46/2018 – Regime Jurídico da Segurança do Ciberespaço. [Online]. Disponível: https://dre.pt. [Acedido em: 14-jan-2024].

[34] Portugal, Decreto-Lei n.º 65/2021. [Online]. Disponível: https://dre.pt. [Acedido em: 14-jan-2024].

[35] Comissão Europeia, "Critical Infrastructure," Migration and Home Affairs. [Online]. [Acedido em: 14-jan-2024].

[36] NIST, "Critical Infrastructure Perspectives," 2021. [Online]. [Acedido em: 14-jan-2024].

[37] NIST, Cybersecurity Framework. [Online]. [Acedido em: 14-jan-2024].

[38] NIST, Framework for Improving Critical Infrastructure Cybersecurity, 2018. [Online]. [Acedido em: 14-jan-2024].

[39] União Europeia, Diretiva 2008/114/CE, 2008. [Online]. [Acedido em: 14-jan-2024].

[40] ISO, ISO 31000:2018 – Risk Management – Guidelines, 2018.

[41] NIST, SP 800-30 Rev. 1 – Guide for Conducting Risk Assessments. [Acedido em: 02-fev-2024].

[42] "Supply Chain Risk Management: A Literature Review," International Journal of Production Research, vol. 53, n.º 16, abr. 2015.

[43] J. T. Mentzer et al., "Defining Supply Chain Management," Journal of Business Logistics, pp. 1–25, 2001.

[44] H. Peck, "Drivers of Supply Chain Vulnerability," International Journal of Physical Distribution & Logistics Management, pp. 210–232, 2005.

[45] G. M. Rosa, "Gestão de Riscos e a Norma ISO 31000," dez. 2015.

[46] FERMA, Norma de Gestão de Riscos, 2003.

[47] E. D. Pinto, Data Science na Gestão de Riscos de Supply Chain, ISCTE, 2021. [Online]. [Acedido em: 08-mai-2025].

[48] União Europeia, Diretiva (UE) 2022/2555 – SRI 2, 2022. [Online]. [Acedido em: 14-jan-2024].

[49] União Europeia, Regulamento (UE) 2016/679 (NIS). [Online]. [Acedido em: 14-jan-2024].

[50] A. Dimakopoulou e K. Rantos, "Comprehensive Analysis of Maritime Cybersecurity Landscape Based on NIST CSF v2.0," 2024. [Online]. [Acedido em: 08-mai-2025].

[51] P. M. M. Magalhães, CSE4CI – Cybersecurity Ecosystem for Critical Infrastructures, Dissertação de Mestrado, IPL, 2023.

[52] Arctic Wolf, "NIST CSF 2.0: Understanding and Implementing the Govern Function," 2025. [Online]. [Acedido em: 08-mai-2025].

[53] Portugal, Legislação Nacional – PGDL Lisboa. [Online]. Disponível: https://www.pgdlisboa.pt. [Acedido em: 14-jan-2024].

[54] CNCS, Quadro Nacional de Referência para a Cibersegurança, 2019. [Online]. [Acedido em: 05-mar-2024].

[55] Cloud Security Alliance, "About CSA." [Online]. [Acedido em: 05-mar-2024].

[56] Cloud Security Alliance, Security Trust & Assurance Registry (STAR). [Online]. [Acedido em: 05-mar-2024].

[57] Cloud Security Alliance, GDPR Code of Conduct. [Online]. [Acedido em: 05-mar-2024].

[58] IPQ, Gestão do Risco – Princípios e Linhas de Orientação, ago. 2012. [Online]. [Acedido em: 10-jun-2024].

[59] ResearchGate, "Diagrama do Processo de Gestão de Riscos ISO 31000." [Online]. [Acedido em: 05-mar-2024].