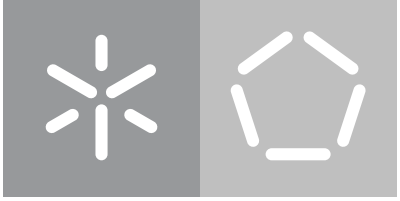
Universidade do Minho
Escola de Engenharia
Departamento de Informática

Nelson Correia Faria

Estratégia de Cibersegurança

outubro 2022



Universidade do Minho
Escola de Engenharia
Departamento de Informática

Nelson Correia Faria

Estratégia de Cibersegurança

Dissertação de Mestrado
Mestrado Integrado em Engenharia Informática

Trabalho efetuado sob a orientação do
Professor Doutor José Carlos Bacelar Almeida

outubro 2022

AGRADECIMENTOS

Em primeiro lugar, gostava de dedicar esta dissertação de mestrado ao meu pai, à minha mãe e à minha irmã, uma vez que foram as pessoas mais importantes para que eu conseguisse chegar a este ponto. Gostava de dizer-lhes que valeu a pena todo o esforço, insistência, dedicação e apoio que me deram ao longo deste tempo todo para eu concluir a dissertação com sucesso.

Depois, gostava de deixar um agradecimento especial ao Doutor José Eduardo Pina Miranda pela forma como me acompanhou em toda a tese e ajudou-me a tomar as melhores decisões. Estarei sempre eternamente grato por todas as horas que passou comigo a ajudar-me e a dar-me conhecimento e experiência na área da cibersegurança, sendo que acima de tudo será sempre um amigo de confiança para mim.

Por outro lado, gostava de agradecer à Imprensa Nacional — Casa da Moeda (INCM) pela oportunidade que me deram em realizar um estágio como CISO e em aplicar a estratégia de cibersegurança desta dissertação na empresa. Aqui, agradeço em especial à Rosa Tomás pela forma como me ajudou também na tese e pelo conhecimento que me foi passando. A sua simpatia e amabilidade para comigo, foram sempre fundamentais para a minha rápida integração na empresa e para me desenvolver mais como profissional na área. Gostava de dizer "obrigado" também ao Igor Sales e ao Miguel Soares que faziam parte da equipa e deram também *inputs* muito úteis para a dissertação. Na verdade, no geral, todas as pessoas da INCM foram sempre muito atenciosas comigo e deram-me sempre as melhores condições para haver sucesso na realização das várias tarefas.

Por último, queria deixar um agradecimento ao Doutor José Carlos Bacelar Almeida por ter aceitado ser o meu orientador da dissertação de mestrado e por mostrar sempre disponibilidade em me ajudar na tomada de decisões.

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico. Confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações, ou resultados em nenhuma das etapas conducente à sua elaboração.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

Universidade do Minho, Braga, outubro 2022

Nelson Correia Faria

RESUMO

No mundo de hoje, a cibersegurança, ou segurança digital, é cada vez mais relevante à medida que a tecnologia avança, o que é constatável por regulares notícias de ataques informáticos a infraestruturas de organizações que afetam muitas vezes os serviços das empresas e podem até resultar em consequências gravíssimas a nível económico e financeiro. Mesmo em Portugal, nota-se que o número de ataques informáticos a empresas ou grandes corporações têm aumentado e deixado um rasto de destruição em muitas delas, o que pode levar até à falência da empresa, fruto da má reputação adquirida por esta, o que deixa por vezes a empresa para trás relativamente à sua concorrência que apresenta melhores garantias em segurança.

Deste modo, esta dissertação de mestrado tem o principal intuito de mostrar a importância das empresas definirem e implementarem um plano de cibersegurança, pelo que é desenvolvida uma estratégia de cibersegurança capaz de mitigar ou eliminar potenciais consequências graves à infraestrutura de uma organização oriundas de incidentes de cibersegurança. Numa primeira fase, é analisado um conjunto de documentos relacionados ao tema em questão fundamentais para uma segunda fase onde são descritos um conjunto de 7 passos para ajudar as empresas a criarem um plano que reflita as medidas que estão e as que serão implementadas no âmbito da cibersegurança. Para isso, é seguida a NIST *Cybersecurity Framework* v1.1 (NIST CSF) como a base da estratégia, o *Cybersecurity Capability Maturity Model* (C2M2) v2.0 como ferramenta de autoavaliação e os CIS *Controls* v8.0 como controlos adicionais para reforço da cibersegurança, além de outras fontes relevantes na área, tais como os *standards* desenvolvidos pelo *International Organization for Standardization* (ISO). Numa terceira fase, a Estratégia de Cibersegurança é aplicada a uma empresa portuguesa que atua na área dos serviços de confiança, o que constitui uma evidência de que a estratégia definida pode ser aplicada em qualquer organização em Portugal.

Assim, seguindo todos os princípios-base da cibersegurança, através da análise documental de boas práticas, legislação, *frameworks* e *standards* de cibersegurança, é desenvolvida uma estratégia de cibersegurança dedicada às organizações, que teve aplicação prática num caso concreto e pode ser seguida por qualquer organização que tenha a intenção de reforçar a sua infraestrutura digital em cibersegurança. O objetivo final é que a cibersegurança fique formalizada na organização com planos/políticas que contenham o nível desejado em cibersegurança ("Perfil-Alvo") e se consiga gerir os riscos através da implementação de ações para combater as lacunas identificadas na empresa.

PALAVRAS-CHAVE Cibersegurança, Estratégia de Cibersegurança, Ataques Informáticos, Legislação/ *"Standards"*/Boas Práticas, Riscos de Cibersegurança, "Perfil-Alvo", Plano de Cibersegurança, Lacunas, Implementação de Ações, NIST CSF v1.1, C2M2 v2.0, CIS *Controls* v8.0, ISO.

ABSTRACT

In today's world, cybersecurity, or digital security, is increasingly relevant as technology advances, which can be seen in regular news reports of cyberattacks on organizations' infrastructures that often affect the companies' services and may even have very serious economic and financial consequences. Even in Portugal, the number of cyberattacks on companies or large corporations has increased and left a trail of destruction in many of them, which can even lead to the bankruptcy of the company, due to the bad reputation acquired by it, which sometimes leaves the company behind its competitors that have better guarantees in security.

Thus, this master's thesis has the main purpose of showing the importance of companies defining and implementing a cybersecurity plan, which is why a cybersecurity strategy capable of mitigating or eliminating potential serious consequences to the infrastructure of an organization arising from incidents of cybersecurity. In a first phase, a set of documents related to the topic in question is analyzed, which are fundamental for a second phase, where a set of 7 steps are described to help companies create a plan that reflects the measures that are and will be implemented within the scope of the cybersecurity. For this, the NIST Cybersecurity Framework v1.1 (NIST CSF) is followed as the basis of the strategy, the Cybersecurity Capability Maturity Model (C2M2) v2.0 as a self-assessment tool and the CIS Controls v8.0 as additional controls to reinforce cybersecurity, in addition to other relevant sources in the area, such as the standards developed by the International Organization for Standardization (ISO). In a third stage, the Cybersecurity Strategy is applied to a Portuguese company operating in the area of trust services, which is evidence that the defined strategy can be applied to any organization in Portugal.

Therefore, following all the basic principles of cybersecurity, through document analysis of best practices, legislation, frameworks and cybersecurity standards, a cybersecurity strategy dedicated to organizations is developed, which had practical application in a specific case and can be followed by any organization that intends to strengthen its digital infrastructure in cybersecurity. The ultimate goal is that cybersecurity is formalized in the organization with plans/policies that contain the desired level of cybersecurity ("Target Profile") and that risks are managed through the implementation of actions to combat the gaps identified in the company.

KEYWORDS Cybersecurity, Cybersecurity Strategy, Cyberattacks, Legislation/Standards/Best Practices, Cybersecurity Risks, "Target Profile", Cybersecurity Plan, Gaps, Implementation of Actions, NIST CSF v1.1, C2M2 v2.0, CIS Controls v8.0, ISO.

CONTEÚDO

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE ACRÓNIMOS

2FA Two-factor authentication.

C2M2 Cybersecurity Capability Maturity Model.
CBA Cost-Benefit Analysis.
CC Cartão de Cidadão.
CERT Computer Emergency Response Team.
CIA Confidentiality, Integrity and Availability.
CIDAN Confidencialidade, Integridade, Disponibilidade, Autenticidade e Não-repúdio.
CIS Center for Internet Security.
CIS CSAT CIS Controls Self Assessment Tool.
CISO Chief Information Security Officer.
CMD Chave Móvel Digital.
CNCS Centro Nacional de Cibersegurança.
COBIT Control Objectives for Information and Related Technologies.
CSIRT Computer Security Incident Response Team.
CVE Common Vulnerabilities and Exposures.
CVSS Common Vulnerability Scoring System.

DDoS Distributed Denial-of-service.
DLP Data Loss Prevention.
DMARC Domain-Based Message Authentication Message Conformance.
DMZ Demilitarized Zone.
DNS Domain Name System.
DoS Denial-of-service.

EC Entidade de Certificação.
eIDAS electronic IDentification, Authentication and trust Services.
ENISA European Network and Information Security Agency.
ENSC Estratégia Nacional de Segurança do Ciberespaço.
ESI Electronic Signatures and Infrastructures.
ETSI European Telecommunications Standards Institute.

HTTP Hypertext Transfer Protocol.

IA Inteligência Artificial.
ICMP Internet Control Message Protocol.
ICT Information and Communications Technology.
IEC International Electrotechnical Commission.
IETF Internet Engineering Task Force.

IG Implementation Group.
INCM Imprensa Nacional - Casa da Moeda.
IPS Intrusion Prevention System.
IRT Incident Response Team.
ISA International Society of Automation.
ISO International Organization for Standardization.
ISP Internet Service Provider.
IT Information Technology.

JNDI Java Naming and Directory Interface.

KPI Key Performance Indicator.

LDAP Lightweight Directory Access Protocol.

MIL Maturity Indicator Level.
MITM Man-in-the-middle.

N/A Not-Applicable.
NIS Network and Information Security.
NIST National Institute of Standards and Technology.
NIST CSF NIST Cybersecurity Framework.
NVD National Vulnerability Database.

OES Operators of Essential Services.
OID Object Identifier.
OSINT Open source intelligence.
OT Operation Technology.
OWASP Open Web Application Security Project.

PKI Public key infrastructure.
PME Pequena/Média Empresa.

QNRCS Quadro Nacional de Referência para a Cibersegurança.

RCE Remote Code Execution.
RFC Request for Comments.
RFI Request for Information.
RPO Recovery Point Objective.
RSA Rivest-Shamir-Adleman.
RTO Recovery Time Objective.

SCADA Supervisory Control and Data Acquisition.
SCEE Sistema de Certificação Electrónica do Estado.
SCRM Supply Chain Risk Management.
SDL Security Development Lifecycle.
SIEM Security Information and Event Management.

SLA Service Level Agreement.
SME Small/Medium Enterprise.
SMS Short Message Service.
SQL Structured Query Language.

TCP Transmission Control Protocol.
TIC Tecnologias da Informação e Comunicação.

UE União Europeia.
URL Uniform Resource Locator.

VPN Virtual Private Network.

Parte I

MATERIAL INTRODUTÓRIO

1

INTRODUÇÃO

O mundo tem sofrido diversas mudanças e evoluções que nos obrigam por diversas vezes a ter de mudar a forma como olhamos para tudo o que nos rodeia, nomeadamente aquelas que são as nossas posses ou ativos que queremos proteger. Porém, hoje em dia os nossos bens vão muito além daqueles que são os nossos recursos físicos. Além desses possuímos recursos digitais ou tecnológicos que também constituem um bem com muito valor que deve ser protegido contra outras pessoas ou entidades que os queiram atacar para tirar proveito do seu valor económico e destruir aquilo que em muitos casos levou muito tempo a construir. No caso empresarial, esses ativos digitais assumem ainda mais uma vertente preponderante no que diz respeito à sua segurança, pois as empresas sentem cada vez mais uma necessidade de evoluir e de se modernizarem para acompanhar o mundo cada vez mais tecnológico que nos rodeia.

Desta forma, para que as empresas não receiem a evolução tecnológica e invistam em novas formas de modernização, a cibersegurança surge como uma necessidade no nosso quotidiano, dado que garantir a segurança a nível informático torna-se algo imperativo e que, em casos mais extremos, se ocorrer um ataque severo à infraestrutura digital de uma organização, as consequências podem ir desde a perda financeira até à danificação de recursos físicos. Exemplo disso é um ataque que impossibilite os administradores de uma empresa de aceder às aplicações de faturação ou um ataque que danifique o sistema de ar condicionado de um centro de dados. Neste âmbito, as organizações/empresas devem ter em conta o aspeto de segurança digital mais do que nunca e devem definir uma estratégia de cibersegurança que consiga evitar ou mitigar possíveis problemas de ataques com origem em pessoas mal-intencionadas (atacantes).

1.1 ENQUADRAMENTO/CONTEXTO

Este documento surge no contexto de um projeto de Mestrado proposto pela empresa *Devise Futures, Lda.*, no âmbito da elaboração de uma estratégia de cibersegurança para a empresa Imprensa Nacional — Casa da Moeda, S.A. (INCM).

Na verdade, a cibersegurança constitui uma das principais prioridades não só para as empresas, mas principalmente para os governos dos vários países. Os governos definem um conjunto de regras ou até conjuntos de boas práticas que devem ser seguidas pelas empresas para serem respeitados alguns princípios de segurança básicos, como, por exemplo, a proteção de dados pessoais. Deste modo, garantem que os seus valores e direitos da sua população sejam respeitados e a segurança a nível digital possa ser assegurada. Assim que a Internet começou a ser usada pelas pessoas e empresas, as preocupações que estas tinham com a segurança não eram muitas, além dos protocolos e tecnologias que eram usados não estarem ainda com muitas proteções de segurança, como no caso do HTTP. Todavia, com o passar dos anos, começou a perceber-se que mais cedo ou mais tarde estas

questões teriam de ser abordadas e que os protocolos que regem a Internet teriam de ter mais atenção com a segurança.

À medida que a Internet começou a ficar mais acessível à população em geral, as vulnerabilidades existentes no *software* começaram a ser exploradas por parte de atacantes que, muitas das vezes, só faziam esses ataques por diversão ou com finalidades não maliciosas. Um destes casos foi o vírus Morris, um dos primeiros a afetar o ciberespaço, criado pelo na altura estudante de pós-graduação Robert Tapan Morris em 1988, sendo que ele queria simplesmente ver se este vírus poderia ser feito [109]. O problema é que os ataques podem ir muito além disto e irem para outros casos extremos como, por exemplo, ataques com motivações políticas, como foi o caso do Stuxnet em 2010. Este *"worm"* afetou as redes industriais no Irão, visando atingir o programa nuclear do país. Este *malware* foi dirigido ao SCADA, uma arquitetura de controlo de sistemas que controlava todas as reservas nucleares. O ciberataque ganhou uma dimensão tal que chegou mesmo a atingir os serviços de distribuição de rede elétrica, abastecimento de água e até mesmo os transportes públicos [34].

De modo geral, os governos e grandes corporações têm desenvolvido esforços conjuntos para aumentar a resiliência da infraestrutura digital dos seus países e preparar a economia e as sociedades para o futuro. Em Portugal, a 12 de junho de 2015 foi publicada a primeira Estratégia Nacional de Segurança do Ciberespaço (ENSC) com o intuito de estabelecer objetivos e linhas de ação com vista a uma eficaz gestão de crises, a uma coordenação da resposta operacional a ciberataques, a um desenvolvimento das sinergias nacionais e a uma intensificação da cooperação nacional, europeia e internacional neste domínio [29]. Porém, tendo em consideração a evolução digital ocorrida desde a aprovação da ENSC de 2015 até à data de escrita deste documento, já foi aprovada a ENSC 2019 – 2023 assente em três objetivos estratégicos: maximizar a resiliência, promover a inovação e gerar e garantir recursos [31], tendo sempre a colaboração do Centro Nacional de Cibersegurança (CNCS), enquanto Autoridade Nacional de Cibersegurança [15]. Além disso, foi estabelecido o "CERT.PT" como a equipa de resposta a incidentes de segurança informática nacional [13].

Efetivamente, muitos dos princípios de cibersegurança definidos para Portugal têm como base aqueles que estão definidos para a União Europeia (UE), sendo que esta baseia-se em instituições de segurança como a Agência Europeia para a Segurança das Redes e da Informação (ENISA). Deste modo, a Lei portuguesa n.º 46/2018 [17] estabelece o regime jurídico da segurança do ciberespaço, transpondo a diretiva NIS (*"Network and Information Security Directive"*) [35], do Parlamento Europeu e do Conselho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União Europeia [17]. A Diretiva NIS (Diretiva (UE) 2016/1148) é a primeira legislação europeia que tem em conta a cibersegurança, tendo sido publicada em 2016 e, posteriormente, transposta por todos os estados-membros da UE [35]. Como se irá perceber durante o desenvolvimento da presente dissertação, muitas mais instituições reúnem esforços para definir este tipo de estratégias de cibersegurança, sendo que na maior parte dos casos trabalham em colaboração e fornecem umas às outras informações úteis para haver uma maior eficácia na definição de medidas de segurança.

Muitos foram os ataques efetuados a infraestruturas de organizações ao longo dos últimos anos que causaram diversos tipos de problemas com consequências mais ou menos danosas, sendo que só em 2021 houve um crescimento de 81% em Portugal [101]. Um dos problemas é que os ataques podem ser de tipos variados e com o passar do tempo os atacantes tornam-se mais engenhosos e aproveitam diversas vulnerabilidades que podem surgir em diversos tipos de *software* ou *hardware*. Com o aumento dos ciberataques durante a crise do coronavírus (COVID-19), demonstrou-se a importância de proteger os hospitais, os centros de investigação e outras infraestruturas [18]. Além disso, com as tensões a aumentar constantemente devido ao conflito Rússia-Ucrânia, é

primordial que os responsáveis de uma determinada organização por assegurar a cibersegurança sejam proativos e não fechem os olhos à probabilidade da existência de brechas na empresa [79].

Assim, se queremos que a evolução digital comece a acelerar no meio empresarial, é crucial que haja a definição de uma estratégia de cibersegurança tanto a nível externo como interno à organização, de acordo com normas, boas práticas e legislação, para que desta forma os riscos associados à inserção de novas tecnologias seja menor e a organização possa prosperar neste mundo cada vez mais digital.

1.2 PRINCIPAIS OBJETIVOS

Os principais objetivos a atingir com esta dissertação de tese de mestrado são:

- Estudar e analisar o estado da arte da cibersegurança, nomeadamente a legislação em vigor, *standards* existentes e boas práticas de segurança digital;
- Elaborar um *"roadmap"* que permita ajudar as empresas a definirem e implementarem uma estratégia de cibersegurança, identificando os vários pontos relevantes a considerar, assim como os documentos e tipos de documentos de política empresarial (estratégias, políticas, procedimentos, etc.) que serão necessários elaborar;
- Aplicar o *"roadmap"* a uma empresa portuguesa que atua na área dos serviços de confiança.

1.3 ESTRUTURA DO DOCUMENTO

No primeiro capítulo, é efetuada uma pequena introdução através da explicação do contexto, objetivos e estrutura desta dissertação.

No capítulo 2, é revisto todo o estado da arte relacionado com a criação de uma estratégia de cibersegurança, pelo que são explicados os conceitos gerais subjacentes e ainda são descritos um conjunto de documentos considerados úteis para o desenvolvimento desta dissertação.

No capítulo 3, é apresentado o problema analisado nesta dissertação e quais os principais desafios para o tentar resolver, sendo que também são apresentadas algumas soluções para os vários desafios apresentados durante o capítulo.

No capítulo 4, serão descritos todos os passos efetuados na criação do *"roadmap"* para ajudar as empresas a definirem e implementarem uma estratégia de cibersegurança, assim como evidências científicas de como a presente dissertação contribui para a evolução do estado da arte.

No capítulo 5, será descrita toda a aplicação prática do *"roadmap"* desenvolvido, ou estratégia de cibersegurança, efetuada para a empresa Imprensa Nacional — Casa da Moeda (INCM), pelo que serão descritos os resultados práticos e alguns exemplos.

Por fim, no capítulo 6 será feita a conclusão da dissertação através da descrição dos seus vários pontos positivos e valor que esta constitui, assim como ideias sobre como o trabalho pode evoluir no futuro.

2

ESTADO DA ARTE

Nas próximas secções, será feita uma explicação dos principais conceitos relacionados com a cibersegurança e ainda uma revisão da literatura considerada mais relevante para a construção de uma estratégia de cibersegurança. Assim, na primeira secção é dado um olhar geral para os principais termos que estão intrinsecamente ligados à cibersegurança. Nas três secções seguintes serão mostradas diferentes abordagens à construção de uma estratégia de cibersegurança por parte de grandes organizações nacionais e internacionais. Por fim, nas últimas secções serão revistos alguns documentos considerados importantes para a elaboração de uma estratégia de cibersegurança.

2.1 CONCEITOS GERAIS

Antes de seguir por caminhos que nos levam a normas ou boas práticas de cibersegurança publicadas por diversas entidades relacionadas à segurança informática, é importante explicar alguns dos conceitos-base. Deste modo, a seguir pretende-se dar uma definição desses conceitos para ser depois mais fácil perceber as secções seguintes.

2.1.1 *O que é a cibersegurança?*

A cibersegurança, ou segurança cibernética, é a arte de proteger redes, dispositivos e dados contra acesso não autorizado ou uso criminoso, e a prática de garantir a confidencialidade, integridade e disponibilidade da informação no ciberespaço [7].

De modo geral, a segurança de informações, das redes de computadores, das aplicações de *software* e dos sistemas operativos estão no âmbito da cibersegurança, bem como medidas de recuperação de incidentes de cibersegurança e de educação do utilizador final. Efetivamente, com a evolução da tecnologia, estas áreas estão a merecer mais atenção, o que faz com que cada vez mais a cibersegurança expanda e que tenha continuamente de adaptar-se face à existência de novos perigos do ciberespaço.

2.1.2 *Porquê a necessidade de uma estratégia?*

As empresas estão cada vez mais a procurar novas formas de se modernizarem com equipamento e soluções digitais para conseguirem aumentar os lucros, a competitividade e a eficácia da produção. Porém, cada novo recurso tecnológico inserido numa organização constitui uma porta de entrada para possíveis ataques informáticos ou ciberataques. Um ataque informático visa aceder, alterar ou destruir informações confidenciais; extorquir dinheiro dos utilizadores; ou interromper os processos normais de negócio [9].

Deste modo, é crucial que as organizações implementem uma estratégia de cibersegurança empresarial, pelo que esta pode ser vista como um conjunto de passos ou instruções úteis para definir quais os objetivos a

serem atingidos e quais os estados atual e alvo relativos à cibersegurança e aos riscos associados. Atualmente, implementar medidas eficazes de cibersegurança é particularmente desafiador, isto porque além dos ciberataques serem cada vez mais sofisticados, o pessoal interno da empresa pode de forma voluntária ou involuntária ser responsável por uma falha de segurança. Todavia, a estratégia a ser montada não precisa de ser perfeita, mas deve ser proativa, eficaz, com suporte ativo e em evolução [102]. Além disso, é provável que tenha de ser revista em menos de 3 anos, dependendo da evolução dos riscos e dos ataques, assim como do tipo de informação manipulada pela organização. Assim, a estratégia deve essencialmente dar resposta a perguntas como: Onde estamos?, Para onde queremos ir? e Como lá chegamos?. Ou seja, deve ser o balanceamento entre os objetivos a serem atingidos e os recursos disponíveis.

2.1.3 *Riscos associados à cibersegurança*

Como falado na secção anterior, os riscos associados à cibersegurança são o principal motivo para a criação de uma estratégia. Claro que quando estamos a falar de riscos a que uma empresa está sujeita ao nível da segurança informática, temos de avaliar se (ou quais) os riscos existentes são um potencial perigo para a empresa. Porém, entender quais as ameaças que estão a afetar mais o mundo empresarial é importante para perceber se a empresa que pretende criar uma estratégia de cibersegurança incorre nesses riscos também com uma frequência e gravidade mais elevada.

Para se perceber como as empresas tem de ter cada vez mais cuidados com estas ameaças cibernéticas, no primeiro semestre do ano de 2022 foi registado no mundo um volume de 2,8 mil milhões de ataques de *"malware"*, representando uma tendência de crescimento face aos anos anteriores. Além disso, apesar de o volume de ataques de *"ransomware"* ter declinado 23% em todo o mundo, na Europa assistiu-se a um aumento de 63% destes ataques no primeiro semestre do ano de 2022 [105].

A cibersegurança tenta combater vários tipos de ameaças que normalmente são em forma de um ataque por parte de um indivíduo, ou grupo deles, para, entre outros, extorquir dinheiro, causar falhas no serviço, obter informações com motivações políticas, ou, em casos mais extremos, danificar sistemas eletrónicos com o pretexto de lançar o pânico. Deste modo, a seguir serão enumerados, por ordem alfabética, alguns dos ciberataques mais comuns que acontecem hoje em dia no ciberespaço segundo a Cisco [8]:

1. ***Denial-of-service* (DoS)**: Um ataque de negação de serviço é destinado a dificultar o acesso a uma máquina ou rede, tornando-a (e aos serviços que suporta) inacessível aos utilizadores, através da inundação do alvo com tráfego excessivo. Exemplos destes ataques são os de *ICMP flodding* (ou *smurf attack* ou *ping of death*, aproveita dispositivos de rede mal configurados e envia pacotes falsificados que executam *ping* em todos os computadores da rede de destino, em vez de apenas numa máquina específica), os de *SYN flodding* (envio de pacotes de SYN para várias portas, mas sem concluir o *handshake* do TCP, fazendo com os que utilizadores legítimos tenham dificuldades no acesso) e os ataques de *Distributed Denial-of-service (DDoS)* (em vez de ser só uma fonte a atacar, são várias em simultâneo de diferentes lugares) [89].

2. ***DNS Tunneling***: Um ataque de *DNS Tunneling*, ou encapsulamento de DNS, é um ataque que consiste em explorar o DNS para esconder dados em pedidos e respostas DNS. Esses dados escondidos em mensagens DNS e codificados, podem ser um modo de enviar dados confidenciais para um atacante, ou podem servir como uma forma do atacante controlar servidores e aplicações da organização [82].

3. ***Malware***: Um *malware*, ou *software* malicioso, é um termo genérico que descreve qualquer programa ou código malicioso que seja prejudicial para os sistemas. Alguns exemplos típicos vão desde o cavalo de tróia (*Trojan*) até ao *ransomware*. Um cavalo de tróia parece que é algo útil de forma a enganar o utilizador, mas quando entra no sistema, consegue obter acesso não autorizado ao sistema em causa e roubar informações financeiras ou até instalar outras ameaças. Um *ransomware* bloqueia o acesso a um dispositivo e/ou cifra os seus ficheiros e, normalmente, é exigido o pagamento de um resgate para a sua devolução. Este último exemplo foi considerado como a arma preferida dos *hackers*, uma vez que implica um pagamento rápido e rentável em criptomoeda, cujo rasto é difícil de seguir. O código por trás do *ransomware* é fácil de obter em mercados criminosos *online*, mas defender-se dele é extremamente difícil [85].

4. ***"Man-in-the-middle"* (MITM)**: Um ataque *"Man-in-the-middle"* é um tipo de ataque em que os intrusos interrompem uma comunicação existente ou transferência de dados. Acontece que após o atacante entrar no "meio" da transferência, ele finge ser ambos os participantes legítimos, permitindo intercetar informações e dados de qualquer uma das partes, ao mesmo tempo que envia *links* maliciosos ou outras informações para os dois participantes legítimos de uma forma que pode não ser detetada [107].

5. ***Phishing***: O *phishing*, que deve o seu nome à palavra inglesa *"fishing"* que significa "pescar", consiste em utilizar métodos tecnológicos que levam o utilizador a revelar dados pessoais e/ou confidenciais, como, por exemplo, carregar num *link* malicioso. Exemplo de tipos destes ataques são o *smishing* (baseia-se no envio de uma mensagem de telemóvel (SMS), cujo objetivo é levar o utilizador a fornecer dados pessoais e/ou confidenciais), o *vishing* (trata-se de um email que aparenta ser de uma instituição totalmente legítima, convidando o utilizador a contactar a entidade por telefone que, na forma de atendedor automático, solicita vários dados pessoais para "verificação de segurança") e o *spear-phishing* (trata-se de um email enviado por alguém que se faz passar por um colega ou chefe da empresa visando fazer com que o utilizador divulgue dados pessoais, dando acesso e controlo ao sistema informático da organização em causa) [104].

6. ***SQL injection***: Um SQL *injection* é uma falha de segurança que permite a um atacante efetuar consultas à base de dados de uma determinada aplicação, fazendo com que aceda a dados que normalmente não consegue obter. Estes dados podem ser pertencentes a outros utilizadores ou então quaisquer outros dados que a própria aplicação é capaz de aceder, pelo que, em muitos casos, um atacante pode modificar ou apagar esses dados, causando alterações persistentes no conteúdo ou comportamento da aplicação [99].

7. ***Zero-day exploit***: Um *Zero-day exploit* refere-se a um método usado por atacantes para atacar sistemas através de uma vulnerabilidade que ainda não foi descoberta pelos fornecedores do sistema. Como os criadores desses sistemas não sabiam da existência dessa vulnerabilidade ou foi descoberta recentemente, estes têm "zero dias" para desenvolverem um *patch* que a resolva, fazendo com que possíveis ataques que usem esse *exploit* tenham grande probabilidade de sucesso [83].

2.1.4 *Controlos de Segurança da Informação*

Quando se decidem as medidas de cibersegurança a implementar numa empresa, devem ser consideradas várias categorias de *standards*. Uma área que se relaciona muito com a cibersegurança é a segurança da informação, sendo que por vezes até pode ser difícil distinguir estas duas áreas, pois grande parte da informação que queremos armazenar, proteger e transmitir está no ciberespaço. Mas a principal diferença reside nas tecnologias da informação

e comunicação (TIC), sendo que quando se fala de tudo o que é vulnerável através das TIC, mesmo que não seja informação, fala-se de cibersegurança. Já a segurança da informação é a segurança de tudo o que é informação, independentemente do formato que esta se encontre, daí coincidir com a cibersegurança no que diz respeito a informação digital [77]. Assim, apesar de existirem diferenças nos temas abordados por estas duas áreas, e até se poder dizer que a cibersegurança possuí temas mais delicados e complexos, é relevante que se considere também a segurança da informação ao se reforçar a cibersegurança numa empresa.

Deste modo, nesta secção pretende-se dar um *overview* do *standard ISO/IEC 27002:2013* [46], sendo que existe outro semelhante que é o *NIST SP 800-53* [91]. O *ISO/IEC 27002:2013* define um conjunto de 14 cláusulas para as organizações selecionarem, implementarem e gerirem controlos para a segurança da informação [46]. Cada categoria de controlos de segurança contém um objetivo que indica aquilo que deve ser alcançado e contém ainda 1 ou mais controlos que podem ser aplicados para alcançar o objetivo. A seguir, pretende-se passar de forma muito resumida por todas as 14 cláusulas de controlos de segurança e observar a sua importância para a segurança da informação:

1. **Políticas de segurança da informação**

   Atendendo às responsabilidades na segurança da informação de cada pessoa que faz parte da organização, deve-se definir, aprovar, publicar e comunicar uma política de segurança da informação que contemple os requisitos e objetivos empresariais, além da gestão de incidentes, alterações, entre outros. Além disso, é importante que hajam revisões regulares às políticas em vigor e a definição de um ou mais responsáveis pela implementação e consequente revisão.

2. **Organização da segurança da informação**

   Deve haver a definição e atribuição de responsabilidades pela gestão do risco e a proteção de ativos, pelo que essa atribuição deve contemplar a separação de papéis para diminuir a probabilidade de usos e alterações não permitidas. Devem ainda existir medidas de proteção dos riscos associados ao uso de dispositivos móveis e trabalho remoto.

3. **Segurança de recursos humanos**

   A administração de uma organização tem a obrigação de garantir que as políticas e procedimentos de segurança da informação são cumpridos por todos os recursos humanos. Além disso, antes de contratarem alguém, devem ser verificados os antecedentes dos candidatos e devem ser impostas responsabilidades tanto para a organização como para o candidato, mesmo quando alguém cesse as suas funções (por exemplo, assinando um contrato de confidencialidade). Recomenda-se ainda ações de formação periódicas e processos disciplinares para quem não cumpra com as suas responsabilidades.

4. **Gestão de ativos**

   Deve-se inventariar e definir um responsável por cada recurso associado a informação com vista à sua proteção, além da definição de regras para o seu uso e, caso se aplique, devolução quando o funcionário ou entidade externa acabar a tarefa para o qual ele foi útil. Deve haver ainda a classificação da informação segundo o seu valor e requisitos legais pelo responsável do recurso de informação. Por fim, devem ser implementados procedimentos tanto para o manuseamento, processamento e arquivo de informação como para a remoção, destruição e transporte de equipamentos.

5. **Controlo de acessos**

Estabelecer políticas e procedimentos de controlo e registo de acessos pelos responsáveis dos recursos consoante os riscos que eles representam. O controlo deve ser estabelecido no acesso a redes e serviços de rede, no acesso à informação e a funcionalidades do sistema. A atribuição de direitos de acesso deve ter em atenção procedimentos para a gestão da autenticação, tais como a atribuição ou remoção de direitos de acesso aos utilizadores e ainda os direitos de acesso privilegiados devem ser controlados, incluindo programas que possam interferir nos controlos de sistemas e aplicações. Todos os utilizadores devem ainda manter a confidencialidade da informação de autenticação em segredo e os sistemas de gestão de *passwords* devem ser interativos e garantir a qualidade das mesmas.

6. **Criptografia**

   Definição e implementação de políticas para o uso de controlos criptográficos e gestão de chaves para garantir a confidencialidade, autenticidade e/ou integridade da informação. Nas políticas pode-se incluir algoritmos usados, tamanho de chaves (deve ter em conta a legislação em vigor e melhores práticas) e responsabilidades relacionadas com os controlos criptográficos (por exemplo, a geração de chaves, *backups* de chaves, entre outros).

7. **Segurança física e de ambientes**

   Para a proteção de áreas críticas para a segurança da informação, deve haver a definição de áreas de segurança física, registo de entradas, procedimentos para a realização de trabalhos nas mesmas e proteção contra ameaças externas ou desastres e condições naturais. A saída de recursos das instalações deve ser sempre autorizada, monitorizada e com medidas que garantam a sua segurança conforme o risco associado. A segurança física deve ser aplicada inclusive a equipamentos de suporte (por exemplo, eletricidade, comunicações, água) e a áreas de carga e descarga de mercadorias para não permitir acessos não autorizados. No caso de equipamentos com informações confidenciais, quando finalizar o seu período de vida, deve haver lugar à sua destruição física de modo a não ser possível a sua recuperação.

8. **Segurança das operações**

   Todas as alterações significativas devem ser registadas, planeadas, analisadas e devem passar por um processo de aceitação formal para serem implementadas, devendo existir também documentação que especifique a instalação e configuração de sistemas, o processamento de informação e o tratamento de erros. Os ambientes de desenvolvimento, teste e operações devem estar separados. Além disso, a organização deve definir e implementar procedimentos para a instalação de *software* que controle, eficazmente, a segurança do sistema, incluindo uma estratégia de *roll-back* (“reversão de operações”) e uma de *backup* (“cópia de segurança de dados”) que deve estar num local remoto. Por fim, deve haver um processo de gestão de vulnerabilidades para detetá-las e tratá-las eficazmente.

9. **Segurança de comunicações**

   Devem ser definidos procedimentos e responsabilidades para a gestão das redes que suportam as instalações de processamento de dados de forma a garantir a confidencialidade, integridade e disponibilidade (CIA = *Confidentiality, Integrity and Availability*) dos dados que passam nas redes. Além disso, devem ser feitos acordos de confidencialidade entre a empresa e as partes externas que deem garantias de proteção da informação.

10. **Aquisição, desenvolvimento e manutenção de sistemas**

A identificação dos requisitos de segurança deve ser introduzida nos estados iniciais dos projetos, pelo que também deve-se ter isto em conta na altura da compra de um produto. É assim relevante definir critérios para a aceitação do produto e que estes sejam tidos em consideração na altura da avaliação e teste do mesmo. É importante ainda garantir que os programadores e outros trabalhadores recebam o treino apropriado e existam ambientes de desenvolvimento seguros para o desenvolvimento de *software* seguro.

11. **Relações com fornecedores**

    Deve ser efetuada uma verificação, monitorização e revisão regular dos termos e condições acordados com os fornecedores, para ver se os requisitos de segurança da informação em vigor são cumpridos.

12. **Gestão de incidentes de segurança da informação**

    Na gestão de incidentes, é importante que a organização defina e implemente procedimentos para a deteção, análise e resposta a eventos de segurança. Um evento de segurança é uma situação anómala materializada ou com probabilidade de se materializar num incidente, pelo que a diferença é que o incidente tem uma probabilidade significativa de comprometer as operações da empresa. Deste modo, todas as partes interessadas têm a função de comunicar as fraquezas e eventos de segurança, pelo que essa comunicação deve ser fácil e acessível. A resposta a incidentes deve seguir o que está documentado e deve incluir, entre outros, a recolha de evidências e registo de todas as atividades. Após ocorrer um incidente, é importante que todos percebam bem o que se passou (lições aprendidas) para evitar e diminuir o impacto de incidentes futuros.

13. **Aspetos de segurança de informação da gestão de continuidade de negócio**

    Na gestão de continuidade de negócio deve ser incluída a segurança da informação, pelo que a organização deve estabelecer e implementar controlos de segurança nos processos, procedimentos, sistemas e ferramentas da continuidade do negócio, devendo estes controlos serem revistos com regularidade. Deve também ser considerada a necessidade de instalações secundárias de processamento de informação para garantir a disponibilidade dos sistemas em situações adversas, pelo que estes sistemas devem ser testados para verificar se continuam a cumprir as suas funções.

14. **Conformidade (*"Compliance"*)**

    Deve ser feito regularmente ou mal haja uma alteração significativa uma revisão independente da gestão da segurança e deve-se confirmar se os sistemas seguem os procedimentos expressos nos *standards* e políticas. Caso haja oportunidade de melhorar esses procedimentos ou existam problemas de conformidade, deve ser feita a geração de relatórios técnicos para a análise e identificação dessas oportunidades de colmatar lacunas.

2.1.5 *Controlos de Cibersegurança*

Como já foram abordadas as cláusulas de segurança da informação da ISO, faz sentido abordar também as cláusulas de cibersegurança. O novo ISO/IEC 27032 [73], que ainda não está formalmente aprovado (*"DIS stage"*), fornece principalmente controlos para a segurança na Internet, apesar de referir que isto é só um subconjunto da cibersegurança. Os controlos abordados fornecem instruções para a preparação, prevenção, deteção, monitorização e resposta a ataques oriundos da Internet. Além dos controlos, são dados esclarecimentos sobre conceitos ligados

à cibersegurança, tais como ataques, ameaças ou vulnerabilidades, além de referir que as organizações devem desenvolver políticas, procedimentos e capacidade de resposta para:

- Restringir o acesso à Internet por necessidade genuína;
- Definir quais os serviços que podem ser expostos na Internet;
- Identificar as ameaças, vulnerabilidades e vetores de ataque;
- Definir os papéis e responsabilidades dos diversos utilizadores da Internet;
- Implementar controlos para proteção contra diversos riscos de segurança na Internet;
- Consciencializar os utilizadores sobre as práticas seguras de uso da Internet;
- Estabelecer mecanismos de resposta a incidentes de cibersegurança;
- Realizar simulações de segurança para testar o mecanismo de resposta a ataques com origem na Internet.

Deste modo, o documento sugere que pelo meio de uma avaliação de risco é possível descobrir os vários riscos relevantes à segurança da Internet que podem ser resolvidos ou mitigados através de vários controlos, tais como os que são enumerados a seguir:

1. **Políticas de segurança na Internet**

   Relativamente ao uso e à segurança da Internet, deve-se preparar e publicar uma política que determine que serviços de Internet podem ser usados na empresa (conteúdos que podem visualizar, condutas proibidas na Internet, etc.), quem os pode usar (por exemplo, pessoal autorizado a aceder à Internet) e quais os objetivos de segurança a serem atingidos. Deste modo, devem ser atribuídas responsabilidades a todas as atividades relacionadas à Internet, além de que estas políticas devem ser definidas, aprovadas pela administração, publicadas, comunicadas e reconhecidas pelo pessoal relevante, contratados e externos.

2. **Controlo de acessos**

   Devem ser estabelecidas na organização regras para controlar o acesso físico e lógico. Desta forma, o acesso a informações e ativos, outros ativos associados à Internet e instalações de processamento de informações devem corresponder à política de controlo de acesso estabelecida. Devem ser implementados procedimentos de autenticação segura, sistemas de gestão de *passwords*, revisões regulares de todos os direitos de acesso (controlo e restrição dos privilégios concedidos aos sistemas de informação) e revisões regulares dos *logs* administrativos.

3. **Educação, Consciencialização (*Awareness*) e Treino**

   Os colaboradores de uma organização devem ser regularmente atualizados sobre as principais ameaças (por exemplo, *phishing*) e as ações que devem tomar para preveni-las e reagirem em caso de uma ação inadequada.

4. **Gestão de incidentes de cibersegurança**

   Devem ser estabelecidos procedimentos de gestão de incidentes para detetar, avaliar, responder, mitigar, relatar e aprender com eventuais ocorrências de eventos e incidentes de cibersegurança. Algumas medidas importantes são a criação de uma equipa de resposta a incidentes (IRT), o uso de ferramentas de

monitorização e de plataformas de *"Threat Intelligence"* para ajudar a detetar e mitigar eventos prejudiciais oriundos do ciberespaço. Além disso, é importante que a organização estabeleça um sistema para partilha e coordenação de informações para ajudar a preparar e responder a eventos e incidentes de segurança. Devem ainda ser considerados requisitos externos sobre a comunicação de incidentes às partes interessadas, sejam internas ou externas, e deve-se manter contacto com autoridades legais/regulatórias, grupos de interesse especial e outros fóruns ou associações profissionais especializadas em segurança. É relevante também que a organização defina e aplique procedimentos para a identificação, recolha, aquisição e preservação de informações, para servirem como prova em caso de violações de segurança. Por fim, recomenda-se o uso de ferramentas como o IPS (*"Intrusion Prevention System"*) e o SIEM (*"Security Information and Event Management"*) para ajudar a evitar futuros incidentes. Para orientações adicionais, deve-se consultar o ISO/IEC 27035 (parte 1 e 2) [56] [57].

5. **Gestão de ativos**

   É crucial que a organização possua um inventário de ativos, sendo importante que contenha informações sobre onde eles se localizam fisicamente. Além disso, os "ativos sensíveis" de rede devem ser localizados no que diz respeito aos "pontos de entrada" para possíveis atacantes (pode ser o acesso oficial à Internet — via *firewall* — e todas as outras conexões com os dispositivos móveis). É necessário também que sejam identificados os "caminhos críticos" geralmente usados por atacantes (autorizados ou não), dado que sem esse conhecimento, nenhuma segregação adequada das redes é possível. Por outro lado, devem ser estabelecidas regras e procedimentos para o uso aceitável de ativos e para a avaliação da criticidade das informações e dos ativos de ICT (*Information and communications technology*) que as possuem e transferem.

6. **Gestão de fornecedores**

   Todos os requisitos relevantes de segurança da informação devem ser estabelecidos e acordados com cada fornecedor com base no tipo de fornecedor e nos riscos associados. A gestão de riscos relativa à informação que os fornecedores de ICT armazenam, exploram ou a que podem aceder é fundamental para a elaboração de contratos que assegurem que os objetivos de segurança da informação da empresa sejam alcançados continuamente. Para serviços *cloud*, a organização deve gerir os seus riscos e deve rever e negociar os contratos com o(s) provedor(es) de serviços *cloud*. Por outro lado, ferramentas baseadas em *cloud*, como ferramentas de reuniões na *Web*, de *chat* na *Web* e de armazenamento em *cloud*, representam um risco para a organização se elas tiverem *bugs*, sendo importante que a organização estabeleça controlos para o seu uso. Para orientações adicionais, deve-se consultar os ISO/IEC 27036 (partes 1–4) [67] [74] [48] [58], ISO/IEC 23187 [66] e ISO/IEC 27017 [50].

7. **Continuidade de negócio sobre a Internet**

   Alguns negócios dependem muito da infraestrutura da Internet interna da organização, pelo que qualquer interrupção na infraestrutura (devido a DoS/DDoS, mau funcionamento de dispositivos de periferia ou uma interrupção do ISP) pode constituir risco de continuidade para a empresa. Deste modo, o processamento de informações deve ser implementado com redundância suficiente para atender aos requisitos de disponibilidade. Para isso, a empresa precisa de definir medidas de segurança para evitar interrupções, como medidas anti-DDoS, para continuidade dos dispositivos de rede. Para orientações adicionais, deve-se consultar o ISO/IEC 22301 [64] e o ISO/IEC 27031 [43].

8. **Proteção de privacidade sobre a Internet**

Muitas empresas e utilizadores finais recorrem a serviços de hospedagem de *sites*, a aplicações *online* ou até a *data centers* disponibilizados por provedores de serviços. Porém, caso estes assinantes de hospedagem configurem mal um servidor ou hospedem conteúdos maliciosos nos seus *sites* ou aplicações, então a segurança dos seus consumidores irá ser prejudicada. Deste modo, é importante que estes serviços cumpram com os termos dos contratos e requisitos legais que cobrem a proteção de dados e a privacidade dos utilizadores, sendo que devem publicar um aviso de privacidade no seu *site* para informar os requisitos aos seus clientes. Além disso, os provedores têm de exigir que os assinantes cumpram com práticas de segurança também no nível aplicacional. Por outro lado, dependendo do *browser*, existem algumas configurações de privacidade que podem ser alteradas pelo utilizador. Assim, as medidas de prevenção de divulgação de dados devem ser aplicadas a sistemas e redes que processam, armazenam ou transmitem informações confidenciais. Para orientações adicionais, deve-se consultar o ISO/IEC 27701 [65].

9. **Gestão de vulnerabilidades**

   As informações sobre vulnerabilidades nos sistemas de informação em uso devem ser obtidas em tempo útil, a exposição da organização a tais vulnerabilidades deve ser avaliada e medidas apropriadas devem ser tomadas para lidar com o risco associado. Os fornecedores de produtos e serviços devem implementar medidas eficazes para identificar, tratar e publicar vulnerabilidades, sendo que esta informação irá ser útil para as empresas que consomem estes produtos e serviços. Além disso, estes fornecedores devem receber relatórios sobre *malware*, *spyware* ou outros problemas de cibersegurança de outras organizações, sendo por isso relevante que as empresas mantenham contacto com os fornecedores. Por outro lado, as empresas devem definir e aplicar uma política estrita sobre quais tipos de *software* os seus colaboradores podem instalar. Havendo a descoberta de novas vulnerabilidades, os *patches* de *software* são a melhor forma de os remover ou reduzir. Isto significa que, no momento em que fornecedores de *software* deixarem de suportar versões mais antigas, a organização deve estudar os riscos e perceber se deve confiar nesse *software* (seja ele de código proprietário ou código aberto). Se possível, qualquer *software* usado pela organização deve estar sempre atualizado na última versão.

10. **Gestão de redes**

    A integridade e a confidencialidade dos dados que passam na Internet devem ser salvaguardadas através de controlos para proteger os sistemas e as aplicações conectadas. Deste modo, os sistemas conectados à infraestrutura de Internet das organizações devem ser restritos e autenticados, além de existir a necessidade de serem monitorizados e guardados *logs* para registo e deteção de ações que podem afetar ou serem relevantes para a segurança da Internet. Além disso, deve-se considerar a gestão da segurança dos sistemas conectados à Internet, segregando-os de outras redes organizacionais, como redes privadas e de perímetro DMZ (*"demilitarized zone"*). Por fim, a organização, dependendo da sua configuração de rede, pode considerar usar dispositivos de rede que vêm com vários módulos de segurança de rede integrados, como *Firewall*, IPS, DLP e proteção contra ataques direcionados ao DNS. Para orientações adicionais, deve-se consultar o ISO/IEC 27033 (partes 1–7) [51] [45] [42] [49] [47] [54] [75].

11. **Proteção contra *malware***

    Medidas de prevenção, deteção e recuperação de correção de anti-*malware* devem ser implementadas e expandidas para proteger o tráfego e trocas indesejadas dos utilizadores, combinando com uma consciencialização dos mesmos.

12. **Gestão de mudanças**

    Devem ser estabelecidas políticas e processos de gestão de mudanças para garantir que seja mais fácil para a organização implementar mudanças na infraestrutura e nos sistemas e aplicações de IT para evitar interrupções não programadas, corrupção ou perda de dados. As políticas devem incluir declarações sobre responsabilidades e deveres dos gestores de sistemas, importação de *softwares* e ficheiros, controlo de acesso, entre outras. Estas políticas e processos são úteis para a organização solicitar, priorizar, autorizar, aprovar, agendar e implementar quaisquer mudanças na estrutura ou componentes de rede.

13. **Identificação da Legislação Aplicável e Requisitos de Conformidade**

    Sendo a Internet uma plataforma cada vez mais usada para serviços de transações, pode haver leis e regulamentos de segurança de dados, cibersegurança e privacidade que controlem e limitem a proteção da confidencialidade, integridade e disponibilidade dos detalhes dessas transações. Transações bancárias, canais de pagamento, transações em aplicações móveis e outras atividades no mesmo âmbito são geralmente regulamentadas por estarem envolvidas com dinheiro em formato digital. A organização deve identificar, documentar e manter atualizados todos os requisitos legais, estatutários, regulamentares e contratuais de segurança de informação e cibersegurança. Por fim, devem ser mantidos e protegidos *logs*, uma vez que estes podem ser exigidos como evidência de que uma organização opera dentro das regras/leis, para garantir a defesa contra possíveis ações civis/criminais.

14. **Uso de criptografia**

    A criptografia é uma das formas de garantir a proteção das informações transmitidas e impedir a análise de tráfego, garantindo a confidencialidade, autenticidade e/ou a integridade. Algumas soluções incluem o uso de redes privadas virtuais (VPN) e HTTPS para conexões seguras. Porém, ao se selecionar as técnicas criptográficas e ao avaliar as questões de fluxo transfronteiriço de informações cifradas, deve-se ter em atenção as melhores práticas e as regulamentações e restrições nacionais que se podem aplicar. A gestão de chaves requer processos seguros para gerar, armazenar, arquivar, recuperar, distribuir, retirar e destruir chaves criptográficas, além de que as chaves secretas e privadas precisam de proteção contra uso não autorizado e divulgação. Por fim, quando relevante, deve haver a proteção física dos equipamentos usados para gerar, armazenar e arquivar chaves.

15. **Segurança de *software* para aplicações acessíveis pela Internet**

    Uma nova tecnologia adicionada a um sistema que faça parte da infraestrutura da Internet deve ser submetida a análise de riscos de segurança e *design* tendo em conta os padrões de ataque conhecidos atualmente. Um sistema deve ser projetado dando importância à sua segurança e deve ser revisto várias vezes, garantindo que se mantém atualizado face aos novos ataques e vulnerabilidades. As organizações devem conseguir garantir que o seu pessoal não consiga aceder a *sites*/aplicações *web* que possam dar origem a vulnerabilidades. No que toca a código, este deve ser documentado e o comportamento avaliado para identificar possíveis falhas. Este processo deve ser feito por um auditor competente e qualificado na área que será responsável por certificar que o *software* se enquadra nos critérios de classificação dos fornecedores de *anti-spyware* que seguem as melhores práticas. Deste modo, as empresas devem considerar usar *software* automatizado para análise de código e *scanners* de vulnerabilidades. Por último, as organizações devem ter presentes no seu *software* sistemas de assinatura digital, para garantir que o proprietário dos ficheiros produzidos pelo sistema sejam facilmente identificados e desta forma considerados seguros antes de qualquer análise. Para

orientações adicionais, deve-se consultar o ISO/IEC 15408 (partes 1–5) [68] [69] [70] [71] [72] e o ISO/IEC 27034 (partes 1–7) [44] [52] [62] [76] [59] [55] [63].

16. **Gestão de dispositivos de *endpoint* (*"endpoint devices"*)**

    Os pontos de extremidade de comunicação (*endpoints*) usados para acesso, processamento e armazenamento de informações devem ser protegidos. O mesmo deve acontecer para os dispositivos de *endpoint* que precisam de ser controlados em áreas seguras, no momento do transporte e uso dos mesmos. Para isso, convém ser desenvolvida uma estratégia de segurança para gestão, tanto dos dispositivos como dos *endpoints*, que inclua controlo de *firewall*, ferramentas de filtragem, segurança e criptografia, gestão de dispositivos móveis e deteção de intrusão.

17. **Monitorização**

    Atividades, exceções, falhas e outros eventos relevantes no sistema devem ser registados, protegidos e mantidos em *logs*, que posteriormente terão também de ser analisados. Além disso, os próprios sistemas, redes e aplicações devem ser monitorizados com o intuito de detetar comportamento anómalo e agir apropriadamente para avaliar se é um incidente de segurança de informação.

2.2 EU CYBERSECURITY STRATEGY

A Estratégia de Cibersegurança da União Europeia (UE) [41] visa criar resiliência às ameaças cibernéticas e garantir que os cidadãos, as empresas e outras entidades beneficiem de tecnologias digitais fiáveis. A transformação digital da sociedade, intensificada pela COVID-19, ampliou o panorama de ameaças e trouxe novos desafios, que exigem respostas adaptadas e inovadoras.

Esta estratégia da União Europeia contém propostas concretas para o desenvolvimento de iniciativas regulamentares, iniciativas de investimento e iniciativas políticas, abordando 3 áreas de ação [18]:

- **Resiliência, soberania tecnológica e liderança**

  Nesta área de ação, a Comissão Europeia propõe usar a diretiva *NIS* 2016/1148 [21] (*Network and Information Security*), que é uma diretiva sobre medidas de alto nível de cibersegurança, com vista a reformar as regras de segurança das redes e dos sistemas de informação em toda a União Europeia. Há ainda uma proposta para lançar uma rede de centros de operações de segurança, alimentada por IA ("Inteligência Artificial") e tecnologias quânticas, capaz de detetar sinais de ciberataques a tempo e permitir uma maior proatividade, agindo antes que o incidente ocorra. Mais propostas contemplam o apoio a PMEs e mais esforços para atrair e melhorar a força de trabalho, de forma a serem formadas pessoas de excelência com talento para a cibersegurança, capazes de efetuarem pesquisas mais inovadoras. Além disso, há a preocupação em criar uma abordagem abrangente e objetiva baseada no risco para a segurança que o 5G ou futuras gerações de redes podem constituir. Por fim, há a proposta do desenvolvimento de um serviço de resolução de nomes (*DNS*) da UE como alternativa segura e aberta para os cidadãos da UE acederem à *Internet*.

- **Capacidade operacional para prevenir, dissuadir e responder**

  Com vista ao reforço da cooperação entre os organismos da UE e responsáveis pela prevenção, dissuasão e resposta a ciberataques, tais como autoridades dos Estados-Membros, civis, forças policiais, comunidades diplomáticas e de defesa do ciberespaço, está a ser preparada pela Comissão Europeia uma nova Unidade Cibernética Conjunta (*Joint Cyber Unit*).

- **Cooperação para promover um ciberespaço global e aberto**

  A União Europeia promete aumentar parcerias internacionais para fortalecer a ordem global através de regras e *standards*, protegendo sempre os direitos e liberdades das pessoas. Através de acordos conjuntos com os estados-membros para os orçamentos da UE e dos próprios países, há a promessa de um maior reforço das indústrias e tecnologias da UE em matéria de cibersegurança.

2.3 Estratégia Nacional de Segurança do Ciberespaço 2019 – 2023

Muitas das medidas que estão em vigor em Portugal seguem os princípios-base da Estratégia de Cibersegurança da União Europeia (secção 2.2), porém em alguns pontos com algumas variantes. Conforme a resolução do conselho de ministros n.º 92/2019 [31], a coordenação da elaboração, acompanhamento e revisão do plano de ação de cibersegurança está entregue ao Centro Nacional de Cibersegurança (CNCS), que está nomeado como Autoridade Nacional de Cibersegurança.

A ENSC ("Estratégia Nacional de Segurança do Ciberespaço") 2019 – 2023 [10] assenta em três objetivos estratégicos: maximizar a resiliência, promover a inovação e gerar e garantir recursos. As implicações e necessidades associadas a cada um dos objetivos estratégicos permitem definir uma orientação geral e específica, traduzida em seis eixos de intervenção, que enformam linhas de ação concretas destinadas a reforçar o potencial estratégico nacional no ciberespaço [31]. Os seis eixos de intervenção são:

1. Estrutura de segurança do ciberespaço;
2. Prevenção, educação e sensibilização;
3. Proteção do ciberespaço e das infraestruturas;
4. Resposta às ameaças e combate ao cibercrime;
5. Investigação, desenvolvimento e inovação;
6. Cooperação nacional e internacional.

Está previsto que esta estratégia de cibersegurança seja objeto de revisão regular e periódica, sendo que caso nessas revisões não surjam contratempos que obriguem a uma revisão antecipada, ela continuará com a duração de 5 anos, ou seja, permanecerá em vigor até 2023.

2.4 Exemplo de outras estratégias de cibersegurança

Nesta secção, o objetivo é dar uma visão global de outras estratégias de cibersegurança publicadas por instituições de âmbito governamental, pelo que vai-se falar da estratégia de cibersegurança do Departamento de Energia dos Estados Unidos (2018 – 2020) e da estratégia de cibersegurança publicada pelo *Castle Point Council*, que está em conformidade com o *Cyber Essentials Scheme* [4] que foi desenvolvido pelo governo do Reino Unido.

A estratégia de cibersegurança do Departamento de Energia dos Estados Unidos [25] alinha-se com estruturas e estratégias relacionadas, incluindo a *National Institute of Standards and Technology (NIST)'s Cybersecurity Framework* [90] e a Agenda de Gestão do Presidente dos Estados Unidos [25]. Conforme descrito na Figura 1, os objetivos estratégicos de cibersegurança estão organizados em metas de IT (*information technology*) que possuem

cada uma delas objetivos de cibersegurança, apoiados pelas principais tarefas a serem feitas para atingir as metas de segurança. De notar que o objetivo da meta de IT número 2 é referente à Estrutura Básica da *NIST Framework*, que será abordada com mais detalhe na secção 2.5.

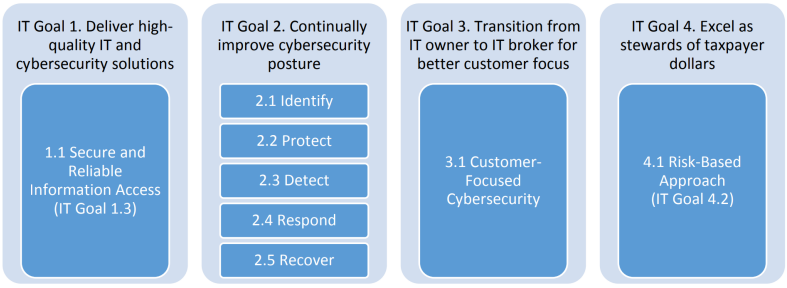


Figura 1: Objetivos da estratégia de cibersegurança do Departamento de Energia dos Estados Unidos (Fonte: U.S. Department of Energy Cybersecurity Strategy 2018 – 2020 [25])

Relativamente à estratégia da *Castle Point Council*, o seu principal objetivo é garantir aos residentes do Reino Unido e a todas as partes interessadas que todos os esforços estão a ser feitos para tornar os sistemas seguros e confiáveis [3]. As principais prioridades rodam em torno do meio ambiente, habitação, saúde e segurança das pessoas. Para haver uma proteção contra ameaças, estão definidos uma série de controlos que vão desde um mecanismo para uma empresa poder demonstrar aos clientes que tomou precauções até a um conjunto de 10 passos para a cibersegurança. Esses 10 passos são os seguintes:

- **Passo 1** — Regime de gestão de risco;
- **Passo 2** — Configuração segura, através da remoção de funcionalidades desnecessárias e resolução de vulnerabilidades;
- **Passo 3** — Segurança das redes;
- **Passo 4** — Manutenção de privilégios dos utilizadores;
- **Passo 5** — Educação e consciencialização do utilizador;
- **Passo 6** — Manutenção de incidentes;
- **Passo 7** — Prevenção de *malwares*;
- **Passo 8** — Monitorização de sistemas;
- **Passo 9** — Dispositivos periféricos removíveis;
- **Passo 10** — Gerir riscos do trabalho doméstico e móvel.

2.5 NIST FRAMEWORK

Antes de mais, interessa referir que esta secção foi elaborada com base no documento da NIST *Framework* (NIST CSF v1.1) [90].

As estratégias de cibersegurança diferem entre países, organizações e, às vezes, até departamentos da mesma empresa, causando falta de *standards* (padrões), problemas de conhecimento da situação em cibersegurança e

uma infraestrutura de cibersegurança mal construída. A *framework* (“guia”) da NIST foi estabelecida para corrigir esses problemas [106].

Baseada em *standards*, diretrizes e práticas internacionais, uma *framework* oferece uma taxonomia e mecanismos comuns para que as organizações consigam descrever a sua situação atual e quais os seus objetivos no que diz respeito à cibersegurança. Deste modo, é possível que elas avaliem o seu progresso relativamente aos objetivos e identifiquem e priorizem medidas de aperfeiçoamento. Por fim, a *framework* é útil também para explicar aos *stakeholders* (“partes interessadas”) internos e externos à organização os riscos que existem perante a atual estratégia de cibersegurança usada pela organização. Porém, começar a usar esta *framework* não significa ter de substituir o programa de cibersegurança ou o processo de gestão de risco de cibersegurança atual da empresa, mas significa complementá-los, fazendo com que estes se tornem mais aperfeiçoados e completos.

A *Framework* da NIST (*National Institute of Standards and Technology*) é então uma abordagem baseada em riscos que visa auxiliar a gestão do risco de cibersegurança e é composta por três partes [90]:

1. *Framework Core* (“Estrutura Básica”);
2. *Framework Implementation Tiers* (“Níveis de Implementação da Estrutura”);
3. *Framework Profiles* (“Avaliações da Estrutura”).

Todavia, antes de explicar cada uma das partes da *framework* nas próximas subsecções, é de interesse explicar melhor a gestão de riscos.

2.5.1 *Gestão de Riscos*

A gestão de riscos é um processo contínuo de identificação, avaliação e resposta ao risco. Deste modo, as organizações podem priorizar as atividades de cibersegurança mediante uma compreensão da tolerância ao risco. Esta tolerância ao risco é definida pela empresa e está relacionada tanto com a relação custo-benefício introduzida por um reforço da cibersegurança, como com as consequências de cibersegurança que podem advir do tratamento ou não do risco, pelo que pode acontecer de nem ser possível eliminar ou mitigar o risco.

Assim, a mitigação e prevenção do risco é algo importante a se ter em conta, mas uma aceitação do risco é uma realidade que todas as organizações vão ter de lidar. Na verdade, a organização estará sempre sujeita ao risco, dependendo só do nível de investimento efetuado em cibersegurança, normalmente decidido pelos executivos da organização, das consequências do risco, que podem não justificar o seu tratamento, e também da viabilidade de ser ou não eliminado.

2.5.2 *Framework Core*

A parte fundamental é a *Framework Core*, ou Estrutura Básica, constituída por um conjunto de *standards*, diretrizes, controlos, práticas, etc., que permitem a comunicação das atividades e dos resultados da cibersegurança em toda a organização, desde o nível executivo até ao nível operacional ou de implementação [90]. Deste modo, esta *framework* apresenta essencialmente os principais resultados de cibersegurança identificados por vários *stakeholders* e considerados úteis na gestão de riscos, sendo que não é uma espécie de *checklist* de ações a serem realizadas na organização.

De modo geral, e como se pode constatar pela Figura 2, os elementos da *Framework Core* funcionam na totalidade e estão organizados em Funções, Categorias e Subcategorias da seguinte forma:

Figura 2: Estrutura da *Framework Core* (Fonte: NIST *Cybersecurity Framework Version* 1.1 [90])

- **Funções**

  As funções auxiliam uma organização a demonstrar a sua gestão de riscos de cibersegurança, através da possibilidade da tomada de decisões de gestão de riscos, do tratamento de ameaças, da organização das informações, da melhoria com base em atividades anteriores de cibersegurança, da gestão de incidentes e ainda da ajuda a demonstrar o impacto dos investimentos em cibersegurança. São 5: Identificar, Proteger, Detetar, Responder e Recuperar;

- **Categorias**

  São as subdivisões de uma Função em grupos de resultados de cibersegurança ligados a atividades específicas. Exemplos: “Gestão de Ativos”, “Gestão de Identidades e Controlo de Acesso”, “Processos de Deteção”, etc.;

- **Subcategorias**

  Basicamente desmembram uma Categoria em resultados específicos de atividades técnicas e/ou de gestão. Exemplos: “Catalogação de Sistemas de Informação Externos”, “Proteção de Dados em Repouso”, “Investigação de Notificações de Sistemas de Deteção”, etc.;

- **Referências Informativas**

  Estão associadas a cada subcategoria, possuindo normas, diretrizes e práticas comuns entre as organizações e ilustram um método para alcançar os resultados especificados em cada subcategoria.

As funções devem ser executadas simultânea e continuamente, pelo que é elaborada uma descrição mais detalhada dos objetivos da cada uma delas:

1. Identificar (*“Identify”*) — Refere-se à compreensão por parte da organização do contexto do seu ambiente/meio, dos recursos que suportam funções críticas para a organização e dos riscos de cibersegurança envolvidos. Algumas categorias relacionadas: Gestão de Ativos; Ambiente Empresarial; Governação; Avaliação de Risco; Estratégia de Gestão de Risco; Gestão do Risco da Cadeia Logística.

2. Proteger (*"Protect"*) — Desenvolver e implementar proteções necessárias para garantir a prestação de serviços críticos. Algumas categorias relacionadas: Gestão de Identidades, Autenticação e Controlo de Acessos; Formação e Sensibilização; Segurança de dados; Procedimentos e Processos de Proteção da Informação; Manutenção; Tecnologia de Proteção.

3. Detetar (*"Detect"*) — Permite a descoberta oportuna de ocorrências de cibersegurança. Algumas categorias relacionadas: Anomalias e Eventos; Monitorização Contínua de Segurança; Processos de Deteção.

4. Responder (*"Respond"*) — Suporta a capacidade de conter o impacto de um possível incidente de cibersegurança. Algumas categorias relacionadas: Plano de Resposta; Comunicações; Análise; Mitigação; Melhorias.

5. Recuperar (*"Recover"*) — Oferece apoio ao restabelecimento pontual para as operações normais de modo a reduzir o impacto de determinado incidente de cibersegurança. Algumas categorias relacionadas: Plano de Recuperação; Melhorias; Comunicações.

2.5.3 *Framework Implementation Tiers*

A *Framework Implementation Tiers*, ou Níveis de Implementação da Estrutura, apresentam contexto sobre como uma organização lida com o risco de cibersegurança e os processos envolvidos para gerir esse risco. Desta forma, os níveis descrevem um grau crescente de rigor e sofisticação nas práticas de gestão de riscos de cibersegurança [90]. Existem quatro níveis de implementação (do nível 1 ao 4): Parcial ("*Partial*"), Risco Informado ("*Informed Risk*"), Reproduzível ("*Repeatable*") e Adaptável ("*Adaptive*").

Muitos são os aspetos de cibersegurança que devem ser tidos em conta na altura da seleção de nível, nomeadamente as práticas correntes de gestão de riscos da organização, o ambiente de ameaças, os requisitos legais e regulamentares, as práticas de partilha de informações, os objetivos de negócio, os requisitos de cibersegurança da cadeia de abastecimento/logística (*"supply chain"*) e ainda restrições da própria organização. Além disso, também não são esquecidas as questões de privacidade e liberdade das pessoas na gestão de riscos de cibersegurança.

Assim, as organizações devem determinar um nível desejado que seja viável e que reduza os riscos de cibersegurança em ativos e recursos críticos para níveis aceitáveis para a organização. Além disso, devem ainda ser consideradas fontes externas para auxiliar na determinação do nível desejado, como, por exemplo, modelos de maturidade. E, como referido no documento da NIST *Framework* [90], os níveis de implementação não representam níveis de maturidade, apesar de haver sempre um incentivo de a organização mudar para níveis superiores. Só que essa mudança deve somente ser feita se, aquando de uma análise de custo-benefício, se verificar uma redução viável e económica do risco de cibersegurança. Por fim, apesar da seleção e designação de um nível afetar a *Framework Profile*, é na altura de se obter resultados da(s) Avaliação(s) Desejada(s) que se pode dizer que houve uma implementação bem-sucedida da *framework* e não na determinação do nível.

As definições dos Níveis (*"Tiers"*) são as seguintes:

- **Nível 1: Parcial (*"Partial"*)** — As estratégias de cibersegurança não são formalizadas e o risco é gerido de forma reativa e *ad-hoc*. A organização não colabora nem recebe informações de outras entidades e não tem noção dos riscos dos produtos e serviços que fornece e que usa da cadeia de logística;

- **Nível 2: Risco Informado (*"Informed Risk"*)** — Existem algumas práticas de gestão de risco, mas elas não são formalizadas e padronizadas em toda a empresa. A organização colabora e recebe algumas informações

de outras entidades e gera algumas das suas próprias informações, mas pode não as partilhar com outras pessoas e, apesar de ter noção dos riscos dos produtos e serviços que fornece e que usa da cadeia de logística, não age de maneira consciente e formal sobre esses riscos;

- **Nível 3: Reproduzível (*"Repeatable"*)** — Existe uma estratégia de cibersegurança formalizada e expressa como política para toda a organização, pelo que todos os funcionários já possuem o conhecimento e habilidades para desempenhar as suas funções e responsabilidades. A organização pode ainda contribuir para o entendimento mais amplo da comunidade sobre os riscos, pelo que colabora e recebe regularmente informações de outras entidades que complementam as já existentes. A organização está ciente dos riscos da cadeia de abastecimento de recursos cibernéticos associados a produtos e serviços que ela utiliza e fornece;

- **Nível 4: Adaptável (*"Adaptive"*)** — A empresa exibe uma abordagem sofisticada de cibersegurança que conta com a experiência anterior e indicadores preditivos no ambiente de ameaças e consegue, através de um aperfeiçoamento contínuo, responder eficazmente às ameaças mais sofisticadas e em evolução. O planeamento económico da organização baseia-se na compreensão do ambiente de risco atual e o previsto, assim como na compreensão da tolerância ao risco. A organização usa informações em tempo real ou quase para entender e agir consistentemente sobre os riscos da cadeia de abastecimento de recursos cibernéticos, pelo que comunica de forma proativa e com mecanismos formais (por exemplo, acordos) e informais para desenvolver e manter fortes relacionamentos com a cadeia de abastecimento.

2.5.4 *Framework Profile*

A última parte da *framework* é o *Framework Profile*, ou Avaliação da Estrutura, que é o alinhamento das Funções, Categorias e Subcategorias com os requisitos de negócio, a tolerância a riscos e os recursos da organização, sendo assim possível definir um *"roadmap"* para reduzir o risco de cibersegurança [90].

Os *Framework Profiles* são úteis porque permitem comparar o estado atual da estratégia de cibersegurança usada com o estado de destino desejado. A comparação de avaliações atual e desejada pode revelar as lacunas a serem tratadas de modo a atender aos objetivos de gestão de riscos de cibersegurança, pelo que um plano de ação para combater estas falhas pode contribuir para o *"roadmap"* falado anteriormente.

2.5.5 *Como Utilizar a Framework?*

A *framework* não foi projetada para substituir o processo existente de gestão de riscos de cibersegurança, mas antes pode ser usada para sobrepor o processo atual à *framework* para determinar lacunas na atual abordagem de risco de cibersegurança e desenvolver um *"roadmap"* para o aperfeiçoamento. Porém, a *framework* tanto pode ser usada para melhorar o programa de cibersegurança já existente como para um novo programa.

De modo geral, a *Framework Core* serve para identificar temas distintos relacionados a cibersegurança, sendo que o objetivo é que sejam olhadas cada uma das subcategorias e depois, recorrendo às referências informativas, sejam implementadas um conjunto de medidas para cumprir com o que está numa determinada subcategoria. Além disso, para haver uma noção sobre como a organização lida com o risco de cibersegurança, existem os *Framework implementation tiers*, que também podem ser usados para definir um nível alvo a atingir. Porém, a *Framework Core* e os *Framework implementation tiers* são uma base de referência, sendo depois necessário interligá-los e

adaptá-los às necessidades da empresa. Assim, dependendo da empresa, existem subcategorias com prioridades maiores ou se adequam mais que outras, pelo que é aqui que surge a noção de *Framework Profile*. Nesta parte, dependendo dos objetivos de negócio, ambiente de ameaças e requisitos/controlos atuais, será desenhado um perfil para a empresa. Com base neste perfil, será possível identificar as lacunas que existem entre a situação atual e aquilo que está definido através das prioridades atribuídas na *Framework Core* para o perfil desejado. Além disso, é no *Framework Profile* que se faz uma estimativa do custo das ações corretivas para diminuir as lacunas. Desta forma, a prioridade, dimensão da lacuna e o custo estimado das ações corretivas ajudam as organizações a planear e orçamentar as atividades de melhoria da cibersegurança. Assim, a criação de um *Framework Profile* é que irá relacionar todos os termos da NIST CSF, pelo que o objetivo final será o reforço das práticas de cibersegurança e gestão de riscos de cibersegurança, tendo em conta a importância da adaptação da *framework* às necessidades da empresa.

Para começar a utilizar a NIST *Framework*, deve existir numa empresa uma divisão de responsabilidades para cada *stakeholder*, tendo em conta o papel que desempenham. Deste modo, deve ser feita uma divisão em níveis na empresa: o nível executivo, o de negócio/processo e o de implementação/operações. Assim, cada pessoa sabe qual a sua função na implementação da *framework*, sendo que normalmente o nível executivo é responsável pela gestão de risco e, o nível de implementação, como o próprio nome indica, pela implementação prática da *framework*. Já quem está no nível de negócio funciona como uma ponte, ajudando tanto na gestão do risco como na implementação.

A seguir, serão mostradas várias formas alternativas de usar a *framework* por parte das organizações:

- Avaliação Básica das Práticas de Cibersegurança:

  A partir de uma Avaliação atual, as organizações podem examinar até que ponto atingem os resultados descritos nas Categorias e Subcategorias.

- Elaboração ou Melhoria de um Programa de Cibersegurança:

  As seguintes etapas, que devem ser repetidas o quanto for necessário, mostram como esta *framework* pode ser usada para criar ou melhorar um programa de cibersegurança:

  - 1.ª Etapa: Priorizar e determinar o *scope* ou prioridades organizacionais;
  - 2.ª Etapa: Orientar, identificar ativos e sistemas, requisitos regulamentares e abordagem de risco e ainda consultar fontes para identificar vulnerabilidades e ameaças aplicáveis a esses ativos e sistemas;
  - 3.ª Etapa: Criar uma avaliação atual;
  - 4.ª Etapa: Realizar uma avaliação de risco, ou seja, a probabilidade da ocorrência de um incidente e o impacto que ele poderia ter;
  - 5.ª Etapa: Criar uma avaliação desejada;
  - 6.ª Etapa: Determinar, analisar e priorizar as falhas/lacunas, através da comparação das avaliações atual e desejada, e criar um plano de ação priorizado para consertar as lacunas;
  - 7.ª Etapa: Implementar o tal plano de ação para que este ajuste as práticas atuais de cibersegurança de modo a alcançar a avaliação desejada.

- Informar os *stakeholders* sobre os requisitos de Cibersegurança:

  A organização pode usar as avaliações atual e desejada para comunicar às diferentes partes interessadas tanto externas como internas o estado atual da cibersegurança e os requisitos de gestão de risco. Esta

comunicação é especialmente relevante entre os *stakeholders* das cadeias de abastecimento/logística, devido às suas relações complexas e interconectadas, pelo que a gestão de riscos da cadeia de logística (*SCRM — Supply Chain Risk Management*) é uma função crítica. Acima de tudo se estivermos a falar de recursos tecnológicos, que podem conter funcionalidades potencialmente maliciosas ou serem falsificações, ou vulneráveis devido a uma má fabricação.

- Decisões de Compra:

  O objetivo é tomar a melhor decisão de compra entre vários fornecedores, tendo em vista os requisitos de segurança, o que significa muitas vezes um *trade-off*, comparando vários produtos ou serviços com as lacunas conhecidas para a avaliação desejada. Com o passar do tempo, a autoavaliação do risco de cibersegurança e a medição devem melhorar a tomada de decisões acerca das prioridades de investimento.

- Identificar oportunidades para referências informativas novas ou revistas:

  A organização pode colaborar com órgãos de normalização para redigir *standards*, diretrizes e práticas, caso julgue que existem poucas ou nenhumas referências informativas para uma determinada subcategoria, que pode ter sido desenvolvida pela própria organização.

- Desenvolver uma metodologia para proteger a privacidade e as liberdades civis:

  As atividades de cibersegurança podem criar riscos à privacidade e às liberdades civis quando as informações pessoais são recolhidas, processadas e mantidas ou divulgadas. Por exemplo, para lidar com a privacidade, os programas de cibersegurança podem incorporar a minimização de dados recolhidos, a transparência para certas atividades de cibersegurança, a qualidade, integridade e segurança dos dados, a prestação de contas e auditoria e o consentimento individual.

2.6 CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2)

O *Cybersecurity Capability Maturity Model* será apresentado com base nas descrições dadas no documento guia do C2M2 versão 2.0 de julho de 2021 [26].

O modelo de maturidade em cibersegurança (C2M2) pode ajudar organizações de todos os setores, tipos e tamanhos a avaliar e fazer melhorias nos seus programas de cibersegurança e fortalecer a sua resiliência operacional [26]. Deste modo, usando este modelo de maturidade, as organizações podem avaliar e medir as suas capacidades de cibersegurança, partilhar conhecimento com outras organizações e priorizar investimentos para aumentar a segurança informática. Acima de tudo, o principal objetivo deste modelo é o de ser usado com uma ferramenta de autoavaliação, que se encontra disponível mediante solicitação ou *online* no *site* do C2M2 [26], de forma à organização medir e melhorar o seu programa de cibersegurança. Porém, o modelo também pode ser usado para orientar o desenvolvimento de um novo programa de cibersegurança, sendo que oferece uma orientação descritiva em vez de prescritiva. As características deste modelo de maturidade fazem com que o C2M2 seja uma ferramenta muito útil para implementar a *NIST Cybersecurity Framework* (secção 2.5).

As organizações podem avaliar o nível de maturidade das suas práticas atuais e definir as metas e prioridades para as conseguirem melhorar, além de ainda poderem comparar o seu desempenho com outras organizações do mesmo setor, pois os resultados da avaliação são anónimos e partilháveis. O C2M2 usa uma escala cumulativa de níveis de indicadores de maturidade (*MILs — Maturity Indicator Levels*) com um conjunto de atributos associados a cada nível que vai de 0 a 3. Assim, cada organização que tenha determinado o seu estado atual pode definir

o estado futuro pretendido, que se espera que tenha uma maior maturidade, e elaborar um planeamento para o alcançar.

Conforme a descrição no documento do C2M2 [26], existe uma distinção importante a ser feita entre os termos empresa, organização e função. Quando se fala em empresa está a falar-se da unidade administrativa de mais alto nível, já a organização é uma unidade de mais baixo nível que a empresa (por exemplo, uma filial) onde a função reside, sendo que a função é uma parte de uma organização à qual o C2M2 será efetivamente aplicado (por exemplo, um departamento da filial). O C2M2 concentra-se essencialmente na implementação e gestão de práticas de cibersegurança associadas a ativos de informação, ativos de tecnologia da informação (*IT — information technology*) e a ativos de tecnologia de operação (*OT — operation technology*) e ambientes em que operam. O foco de uma avaliação do C2M2 é a função, pelo que a sua seleção irá determinar os ativos específicos e as pessoas a serem avaliadas. As funções podem incluir departamentos, linhas de negócio, zonas de segurança de rede, agrupamento de ativos ou ativos/processos/recursos geridos externamente (por exemplo, ativos *cloud*). Para garantir uma avaliação abrangente, as organizações devem contabilizar todos os tipos de ativos que podem entrar no âmbito da autoavaliação, como ativos virtualizados, regulamentados, em *cloud* ou móveis, sendo também importante perceber quais é que podem ser usados para constituírem uma ameaça.

Este modelo de maturidade é organizado em 10 domínios, cada um sendo um agrupamento lógico de práticas de cibersegurança. Cada prática é agrupada dentro de um domínio por objetivo, o resultado alvo que suporta o domínio. Por fim, dentro de cada objetivo, as práticas são ordenadas por níveis indicadores de maturidade (MILs). Várias práticas dentro de um domínio incluem ainda listas de exemplos para ajudar a ilustrar o significado delas. Nas próximas subsecções, explica-se cada um dos componentes da arquitetura deste modelo, e na última secção irá ser dada uma explicação conforme o C2M2 de como o usar.

2.6.1 *Domínios, Objetivos e Práticas*

O C2M2 v2.0 incluí 342 práticas de cibersegurança, agrupadas em 10 domínios [26]. Na Figura 3 pretende-se demonstrar a arquitetura do modelo com a relação entre domínios, objetivos e práticas.

Em cada um dos domínios existe associada uma declaração de propósito que diz a sua intenção e ainda notas introdutórias que fornecem contexto para o domínio e apresentam as suas práticas. Para ser mais fácil de referir cada domínio, é fornecido um nome abreviado que aparece ao lado de cada declaração de propósito. De notar ainda que cada prática pode ser referenciada usando uma notação que começa com o nome abreviado do domínio, um hífen, o número do objetivo e a letra da prática (por exemplo, *ASSET-1a*). Abaixo segue um breve resumo dos 10 domínios.

1. ***Asset, Change, and Configuration Management (ASSET)***

   Relacionado com a gestão dos ativos de *IT* e *OT* da organização, incluindo *hardware* e *software*, e ativos de informação proporcionais ao risco para os objetivos da organização.

2. ***Threat and Vulnerability Management (THREAT)***

   Estabelecer e manter planos e tecnologias para detetar, identificar, analisar, gerir e responder a ameaças e vulnerabilidades de cibersegurança, consoante o risco para os objetivos da organização.

3. ***Risk Management (RISK)***

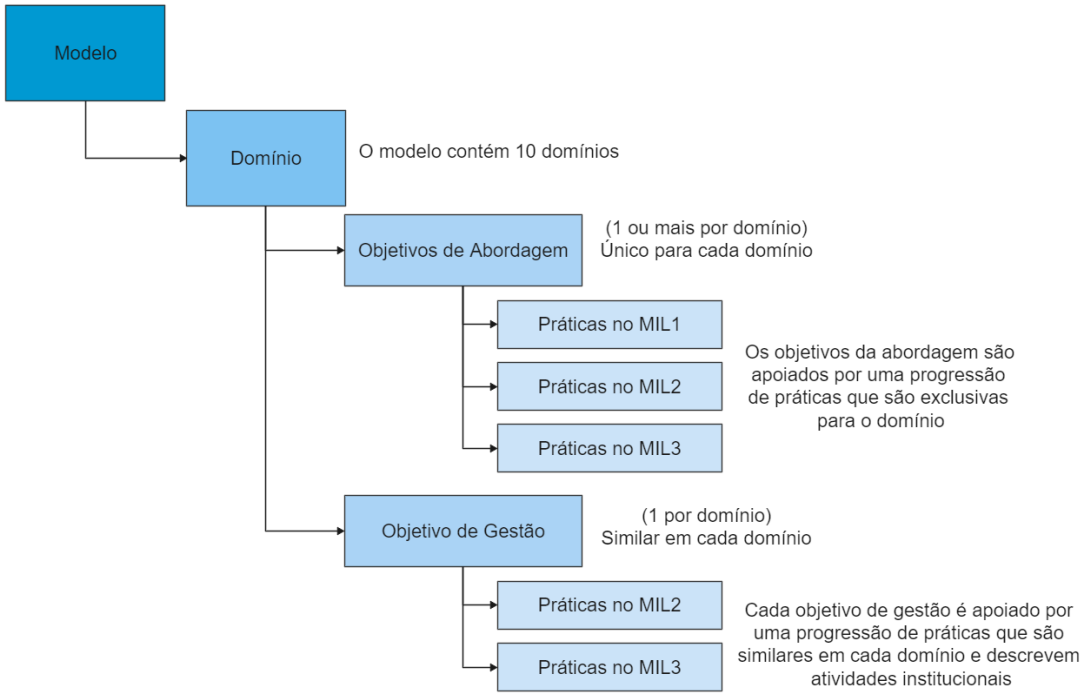


Figura 3: Modelo e elementos do domínio (autoria própria baseado no C2M2 [26])

Estabelecer, operar e manter um programa de gestão de cibersegurança para identificar, analisar e responder aos riscos a que a organização está sujeita.

4. ***Identity and Access Management (ACCESS)***

   Controlo de acesso aos ativos segundo o risco, através da criação e gestão de identidades para que as entidades possam receber acesso lógico/físico aos ativos da organização.

5. ***Situational Awareness (SITUATION)***

   Para estabelecer consciência situacional para o estado de cibersegurança, deve-se estabelecer e manter atividades e tecnologias para colecionar, analisar, relatar e para usar informações operacionais, de segurança e de ameaças, incluindo informações de *status* e resumo de outros domínios do modelo.

6. ***Event and Incident Response, Continuity of Operations (RESPONSE)***

   Com vista a sustentar as operações durante incidentes de cibersegurança, deve-se estabelecer e manter planos e tecnologias para detetar, analisar, mitigar, responder e recuperar-se desses incidentes.

7. ***Third-Party Risk Management (THIRD-PARTIES)***

   Deve-se estabelecer e manter controlos para gerir os riscos de cibersegurança decorrentes de fornecedores e terceiros.

8. ***Workforce Management (WORKFORCE)***

   Para garantir a adequação e competência contínua do pessoal da organização, deve-se estabelecer e manter procedimentos, tecnologias e controlos para criar uma cultura de cibersegurança.

9. ***Cybersecurity Architecture (ARCHITECTURE)***

Estabelecer e manter a estrutura e o comportamento da arquitetura de cibersegurança da organização, incluindo controlos, processos, tecnologias entre outros elementos conforme o risco.

10. ***Cybersecurity Program Management (PROGRAM)***

    Para alinhar os objetivos de cibersegurança com os objetivos estratégicos da organização e o risco, deve-se estabelecer e manter um programa de cibersegurança empresarial que forneça planeamento e governação para as várias atividades cibernéticas da organização.

Relativamente aos objetivos, existem objetivos de abordagem e de gestão, cada um com práticas associadas. Um objetivo de abordagem refere-se ao nível de desenvolvimento e profundidade de uma atividade num domínio, pelo que depende na maioria da iniciativa e experiência da equipa responsável pela realização das práticas. Já um objetivo de gestão descreve até que ponto uma prática está enraizada nas operações da organização, pelo que quanto mais enraizada estiver, maior a probabilidade de continuar a ser praticada ao longo do tempo, o que fazem os resultados da prática serem consistentes, reproduzíveis e de alta qualidade.

2.6.2 *Níveis Indicadores de Maturidade (MILs)*

Nível	Características
MIL 0	- Práticas não são aplicadas
MIL 1	- Práticas iniciais são aplicadas, mas podem ser *ad hoc*
MIL2	Características de gestão: - Práticas são documentadas - Recursos adequados são providenciados para suportar o processo Característica de abordagem: - Práticas são mais complexas ou avançadas que no MIL 1
MIL 3	Características de gestão: - Atividades são guiadas por políticas (ou outras diretivas) - Pessoal que aplica as práticas têm competências e conhecimentos adequados - Responsabilidade, contabilidade e autoridade para aplicar as práticas atribuídas - A efetividade de atividades é avaliada e monitorizada Característica de abordagem: - Práticas são mais complexas ou avançadas que no MIL 2

Tabela 1: Resumo das Características dos Níveis Indicadores de Maturidade (autoria própria com base no C2M2 [26])

O modelo define 4 níveis indicadores de maturidade, MIL 0 a MIL 3, que se aplicam independentemente a cada domínio no modelo, sendo que definem uma progressão dupla de maturidade: uma progressão de abordagem e uma progressão de gestão [26]. É importante ainda referir que as MIL's são acumulativas, ou seja, para chegar a um certo nível é necessário ter os que estão para trás implementados. Porém, pode parecer que fazer esforços para atingir uma certa MIL-alvo num determinado domínio é o mais indicado, só que as empresas devem primeiro avaliar os custos de obtenção dessa MIL específica em comparação com os seus benefícios potenciais. No entanto, o modelo foi projetado para que todas as empresas, independentemente do tamanho, consigam atingir a MIL 1 em todos os domínios. Na Tabela 1 pode-se ver um resumo das principais características das MILs.

2.6.3 *Como Utilizar o Modelo?*

Como se pode observar pela Figura 4, uma organização realiza a avaliação em relação ao modelo, usa essa avaliação para identificar lacunas na capacidade, prioriza essas lacunas, desenvolve planos para resolvê-las e, finalmente, implementa planos para selecionar as lacunas. Conforme os planos são implementados, os objetivos de negócio mudam e o ambiente de risco evolui, o processo é repetido [26].

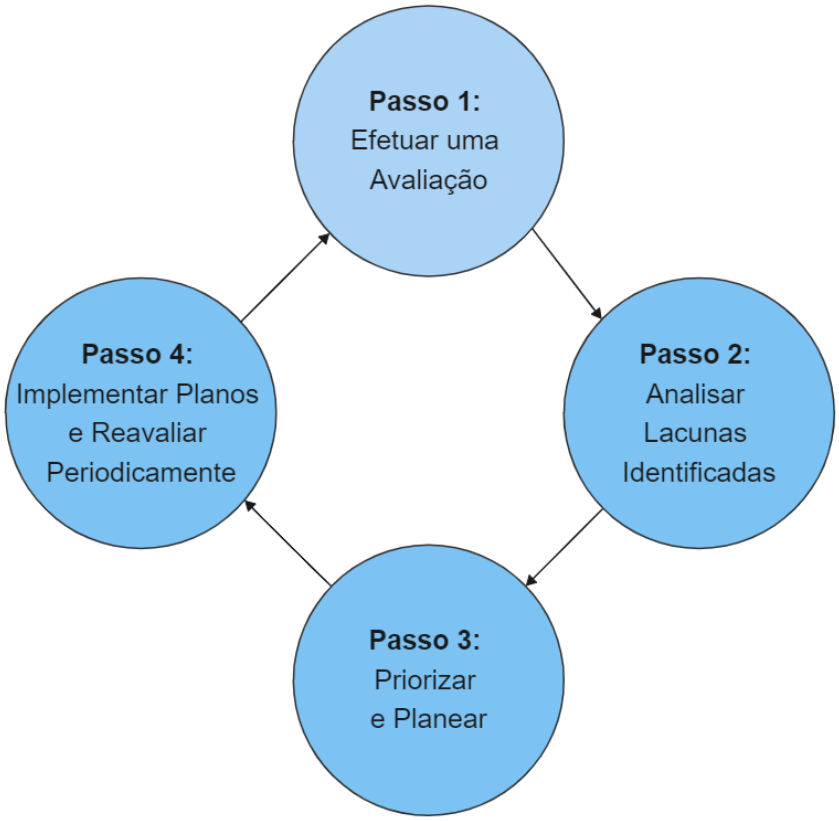


Figura 4: Possível abordagem para usar o modelo (autoria própria com base no C2M2 [26])

- **Passo 1: Efetuar uma avaliação**

  Através de diálogo aberto e consenso é efetuado um *workshop* de autoavaliação com todos os *stakeholders* da organização, usando uma das ferramentas disponíveis do C2M2 (questionário na versão *online* ou em formato PDF mediante solicitação por email), para decidir sobre o nível de maturidade para as práticas de cada domínio.

- **Passo 2: Analisar lacunas identificadas**

  O relatório final da autoavaliação irá identificar lacunas no desempenho das práticas do modelo, pelo que nesta fase serão analisadas para ver se são significativas para a organização abordar. Os *stakeholders* devem selecionar a maturidade pretendida nas práticas dos vários domínios, sendo aconselhável nunca selecionar um perfil de destino para uma determinada prática sem se ter a noção do seu estado atual de maturidade através da autoavaliação, principalmente se for a primeira vez que se usa esta abordagem.

- **Passo 3: Priorizar e planear**

Após a análise de lacunas, a organização deve priorizar as ações necessárias para implementar totalmente as práticas que permitem a obtenção da maturidade desejada em domínios específicos. Depois, um plano deve ser desenvolvido para abordar as lacunas selecionadas, pelo que pode demorar semanas, meses ou anos, dependendo das melhorias para fechar as lacunas. Deve-se ainda identificar um indivíduo com autoridade suficiente para executar o plano e designá-lo como o dono do plano.

- **Passo 4: Implementar planos e reavaliar periodicamente**

  Os planos desenvolvidos no passo 3 devem ser implementados para resolver as lacunas identificadas, sendo importante fazer-se periodicamente autoavaliações para garantir que o progresso desejado seja alcançado. Fazer reavaliações também deve ser considerado para dar resposta a grandes mudanças na tecnologia, mercado ou ambientes de ameaças para garantir que o perfil atual corresponde ao estado desejado da organização, pois aquilo que é hoje uma realidade amanhã pode já não ser.

2.7 CONTROLOS DE SEGURANÇA CRÍTICOS DA CIS

Os controlos da *CIS* versão 8.0 [6] estão feitos para projetar, implementar, medir, relatar e gerir a segurança das empresas. Como certas empresas podem não conseguir implementar alguns controlos, os subcontrolos ("*safeguards*") associados a cada controlo estão agrupados em grupos de implementação (IG1, IG2 e IG3) para ajudar a diferenciar os mais complexos e avançados em segurança. Deste modo, dá-se a hipótese de decidir quais subcontrolos implementar com base no perfil de risco e recursos da empresa. Por exemplo, o IG1 corresponde há chamada "higiene cibernética básica", sendo o conjunto de medidas de segurança fundamentais que toda a empresa deve aplicar para a proteção contra os ataques mais comuns, depois os outros grupos mais elevados incluem subcontrolos mais fortes e ainda os grupos anteriores, ou seja, o IG2 inclui o IG1 e o IG3 inclui o IG2 e IG1.

A seguir, serão sinteticamente descritos os 18 controlos de segurança da CIS:

1. ***CIS Critical Security Control 1*: Inventário e controlo de ativos da empresa**

   Refere-se essencialmente à gestão ativa (inventariar, procurar e corrigir) de todos os recursos da empresa, para saber com precisão a totalidade dos ativos que precisam de ser monitorizados e protegidos na organização. Deste modo, os 5 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
1.1) Estabelecer e manter um inventário detalhado de ativos da empresa	Dispositivo	Identificar	IG1 | IG2 | IG3
1.2) Endereçar ativos não autorizados	Dispositivo	Responder	IG1 | IG2 | IG3
1.3) Usar uma ferramenta de descoberta ativa	Dispositivo	Detetar	IG2 | IG3
1.4) Usar o *Dynamic Host Configuration Protocol* (DHCP) para atualizar o inventário de ativos corporativos	Dispositivo	Identificar	IG2 | IG3
1.5) Usar uma ferramenta de descoberta passiva	Dispositivo	Detetar	IG3

Tabela 2: Medidas de segurança do controlo de segurança 1 (autoria própria com base no CIS [6])

2. ***CIS Critical Security Control 2*: Inventário e controlo de ativos de *software***

Refere-se essencialmente à gestão ativa de todo o *software* na rede para que apenas o *software* autorizado seja instalado e executado, e para que o *software* não autorizado seja encontrado e impedido de ser instalado ou executado. Deste modo, os 7 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
2.1) Estabelecer e manter um inventário de *software*	Aplicações	Identificar	IG1 | IG2 | IG3
2.2) Assegurar que o *software* autorizado seja atualmente suportado	Aplicações	Identificar	IG1 | IG2 | IG3
2.3) Endereçar o *software* não autorizado	Aplicações	Responder	IG1 | IG2 | IG3
2.4) Utilizar ferramentas automatizadas de inventário de *software*	Aplicações	Detetar	IG2 | IG3
2.5) Lista de permissões de *software* autorizado	Aplicações	Proteger	IG2 | IG3
2.6) Lista de permissões de bibliotecas autorizadas	Aplicações	Proteger	IG2 | IG3
2.7) Lista de permissões de *Scripts* autorizados	Aplicações	Proteger	IG3

Tabela 3: Medidas de segurança do controlo de segurança 2 (autoria própria com base no CIS [6])

3. ***CIS Critical Security Control 3*: Proteção de Dados**

Refere-se ao desenvolvimento de processos e controlos para identificar, classificar, usar com segurança, reter e descartar dados. Deste modo, os 14 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
3.1) Estabelecer e manter um processo de gestão de dados	Dados	Identificar	IG1 | IG2 | IG3
3.2) Estabelecer e manter um inventário de dados	Dados	Identificar	IG1 | IG2 | IG3
3.3) Configurar listas de controlo de acesso a dados	Dados	Proteger	IG1 | IG2 | IG3
3.4) Aplicar retenção de dados	Dados	Proteger	IG1 | IG2 | IG3
3.5) Descartar dados com segurança	Dados	Proteger	IG1 | IG2 | IG3
3.6) Cifrar dados em dispositivos de utilizador final	Dispositivo	Proteger	IG1 | IG2 | IG3
3.7) Estabelecer e manter um esquema de classificação de dados	Dados	Identificar	IG2 | IG3
3.8) Documentar Fluxos de Dados	Dados	Identificar	IG2 | IG3
3.9) Cifrar dados em mídia removível	Dados	Proteger	IG2 | IG3
3.10) Cifrar dados sensíveis em trânsito	Dados	Proteger	IG2 | IG3
3.11) Cifrar dados sensíveis em repouso	Dados	Proteger	IG2 | IG3
3.12) Segmentar o processamento e o armazenamento de dados com base na sensibilidade	Rede	Proteger	IG2 | IG3
3.13) Implementar uma solução de prevenção contra perda de dados	Dados	Proteger	IG3
3.14) Registar o acesso a dados sensíveis	Dados	Detetar	IG3

Tabela 4: Medidas de segurança do controlo de segurança 3 (autoria própria com base no CIS [6])

4. ***CIS Critical Security Control 4*: Configuração segura de ativos da empresa e de *software***

Refere-se à configuração segura de ativos da empresa (*hardware* como portáteis, servidores, dispositivos de rede, etc.) e *software* (sistemas operativos e aplicações). Deste modo, os 12 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
4.1) Estabelecer e manter um processo de configuração segura	Aplicações	Proteger	IG1 | IG2 | IG3
4.2) Estabelecer e manter um processo de configuração segura para a Infraestrutura de Rede	Rede	Proteger	IG1 | IG2 | IG3
4.3) Configurar o bloqueio automático de sessão nos ativos da empresa	Utilizadores	Proteger	IG1 | IG2 | IG3
4.4) Implementar e gerir uma *firewall* nos servidores	Dispositivo	Proteger	IG1 | IG2 | IG3
4.5) Implementar e gerir uma *firewall* nos dispositivos de utilizador final	Dispositivo	Proteger	IG1 | IG2 | IG3
4.6) Gerir com segurança os ativos e *software* da empresa	Rede	Proteger	IG1 | IG2 | IG3
4.7) Gerir contas padrão nos ativos e *software* da empresa	Utilizadores	Proteger	IG1 | IG2 | IG3
4.8) Desinstalar ou desativar serviços desnecessários nos ativos e *software* da empresa	Dispositivo	Proteger	IG2 | IG3
4.9) Configurar servidores DNS confiáveis nos ativos da empresa	Dispositivo	Proteger	IG2 | IG3
4.10) Impor o bloqueio automático de dispositivos nos dispositivos portáteis do utilizador final	Dispositivo	Responder	IG2 | IG3
4.11) Impor a capacidade de limpeza remota nos dispositivos portáteis do utilizador final	Dispositivo	Proteger	IG2 | IG3
4.12) Separar os espaços de trabalho relacionados com a empresa nos dispositivos móveis	Dispositivo	Proteger	IG3

Tabela 5: Medidas de segurança do controlo de segurança 4 (autoria própria com base no CIS [6])

5. ***CIS Critical Security Control 5*: Gestão de Contas**

   Refere-se ao uso de processos e ferramentas para atribuir e gerir credenciais de autorização para contas de utilizadores de ativos da empresa e *software*, incluindo as dos administradores e as de serviço. Deste modo, os 6 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
5.1) Estabelecer e manter um inventário de contas	Utilizadores	Identificar	IG1 | IG2 | IG3
5.2) Usar senhas exclusivas	Utilizadores	Proteger	IG1 | IG2 | IG3
5.3) Desabilitar contas inativas	Utilizadores	Responder	IG1 | IG2 | IG3
5.4) Restringir privilégios de administrador a contas de Administrador dedicadas	Utilizadores	Proteger	IG1 | IG2 | IG3
5.5) Estabelecer e manter um inventário de contas de serviço	Utilizadores	Identificar	IG2 | IG3
5.6) Centralizar a gestão de contas	Utilizadores	Proteger	IG2 | IG3

Tabela 6: Medidas de segurança do controlo de segurança 5 (autoria própria com base no CIS [6])

6. ***CIS Critical Security Control 6*: Gestão do Controlo de Acesso**

   Refere-se ao uso de processos e ferramentas para criar, atribuir, gerir e revogar credenciais de acesso e privilégios para contas de utilizador, administrador e de serviço para ativos e *software* da empresa. Deste modo, os 8 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
6.1) Estabelecer um Processo de Concessão de Acesso	Utilizadores	Proteger	IG1 | IG2 | IG3
6.2) Estabelecer um Processo de Revogação de Acesso	Utilizadores	Proteger	IG1 | IG2 | IG3
6.3) Exigir MFA para aplicações expostas externamente	Utilizadores	Proteger	IG1 | IG2 | IG3
6.4) Exigir MFA para acesso remoto à rede	Utilizadores	Proteger	IG1 | IG2 | IG3
6.5) Exigir MFA para acesso administrativo	Utilizadores	Proteger	IG1 | IG2 | IG3
6.6) Estabelecer e manter um inventário de sistemas de autenticação e autorização	Utilizadores	Identificar	IG2 | IG3
6.7) Centralizar o controlo de acesso	Utilizadores	Proteger	IG2 | IG3
6.8) Definir e manter o controlo de acesso baseado em funções	Dados	Proteger	IG3

Tabela 7: Medidas de segurança do controlo de segurança 6 (autoria própria com base no CIS [6])

7. ***CIS Critical Security Control 7*: Gestão Contínua de Vulnerabilidades**

   Refere-se à necessidade de desenvolver um plano para avaliar e rastrear vulnerabilidades continuamente em todos os ativos da empresa dentro da sua infraestrutura e à necessidade de prestar atenção a fontes de informação públicas para saber novas informações sobre ameaças e vulnerabilidades, de modo a remediar e minimizar a janela de oportunidade para atacantes. Deste modo, os 7 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
7.1) Estabelecer e manter um processo de gestão de vulnerabilidades	Aplicações	Proteger	IG1 | IG2 | IG3
7.2) Estabelecer e manter um processo de remediação	Aplicações	Responder	IG1 | IG2 | IG3
7.3) Executar a gestão automatizada de *patches* do sistema operativo	Aplicações	Proteger	IG1 | IG2 | IG3
7.4) Executar a gestão automatizada de *patches* de aplicações	Aplicações	Proteger	IG1 | IG2 | IG3
7.5) Realizar *scans* automatizados de vulnerabilidades em ativos internos da empresa	Aplicações	Identificar	IG2 | IG3
7.6) Realizar *scans* automatizados de vulnerabilidades em ativos expostos externamente da empresa	Aplicações	Identificar	IG2 | IG3
7.7) Corrigir vulnerabilidades detetadas	Aplicações	Responder	IG2 | IG3

Tabela 8: Medidas de segurança do controlo de segurança 7 (autoria própria com base no CIS [6])

8. ***CIS Critical Security Control 8*: Gestão de Registos de Auditoria**

   Referente à recolha, análise e retenção de *logs* de auditoria de eventos que podem ajudar a detetar, compreender e recuperar de um ataque. Deste modo, os 12 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
8.1) Estabelecer e manter um processo de gestão de *logs* de auditoria	Rede	Proteger	IG1 | IG2 | IG3
8.2) Recolher *logs* de auditoria	Rede	Detetar	IG1 | IG2 | IG3
8.3) Garantir o armazenamento adequado do registo de auditoria	Rede	Proteger	IG1 | IG2 | IG3
8.4) Padronizar a sincronização de tempo	Rede	Proteger	IG2 | IG3
8.5) Recolher *logs* de auditoria detalhados	Rede	Detetar	IG2 | IG3
8.6) Recolher *logs* de auditoria de consulta DNS	Rede	Detetar	IG2 | IG3
8.7) Recolher *logs* de auditoria de requisição de URL	Rede	Detetar	IG2 | IG3
8.8) Recolher *logs* de auditoria de linha de comando	Dispositivo	Detetar	IG2 | IG3
8.9) Centralizar os *logs* de auditoria	Rede	Detetar	IG2 | IG3
8.10) Reter os *logs* de auditoria	Rede	Proteger	IG2 | IG3
8.11) Conduzir revisões de *logs* de auditoria	Rede	Detetar	IG2 | IG3
8.12) Recolher *logs* do fornecedor de serviços	Dados	Detetar	IG3

Tabela 9: Medidas de segurança do controlo de segurança 8 (autoria própria com base no CIS [6])

9. ***CIS Critical Security Control 9*: Proteção de email e *browsers web***

   Refere-se à necessidade de melhorar as proteções e deteções de ameaças de *email* e *web*, dado que são oportunidades para atacantes manipularem o comportamento humano através do envolvimento direto. Deste modo, os 7 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
9.1) Garantir o uso apenas de navegadores e clientes de email suportados plenamente	Aplicações	Proteger	IG1 | IG2 | IG3
9.2) Usar serviços de filtragem de DNS	Rede	Proteger	IG1 | IG2 | IG3
9.3) Manter e impor filtros de URL baseados em rede	Rede	Proteger	IG2 | IG3
9.4) Restringir extensões de cliente de email e navegador desnecessárias ou não autorizadas	Aplicações	Proteger	IG2 | IG3
9.5) Implementar o DMARC (*Domain-based Message Authentication, Reporting & Conformance*)	Rede	Proteger	IG2 | IG3
9.6) Bloquear tipos de ficheiros desnecessários	Rede	Proteger	IG2 | IG3
9.7) Implementar e manter proteções anti-*malware* de servidor de email	Rede	Proteger	IG3

Tabela 10: Medidas de segurança do controlo de segurança 9 (autoria própria com base no CIS [6])

10. ***CIS Critical Security Control 10*: Defesas contra *malware***

    Trata-se de controlar ou impedir a instalação, disseminação e execução de aplicações, códigos ou *scripts* maliciosos em ativos da empresa. Deste modo, os 7 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
10.1) Instalar e manter um *software* anti-*malware*	Dispositivo	Proteger	IG1 | IG2 | IG3
10.2) Configurar atualizações automáticas de assinatura anti-*malware*	Dispositivo	Proteger	IG1 | IG2 | IG3
10.3) Desabilitar a execução e reprodução automática para mídias removíveis	Dispositivo	Proteger	IG1 | IG2 | IG3
10.4) Configurar *scans* anti-*malware* automáticos de mídia removivel	Dispositivo	Detetar	IG2 | IG3
10.5) Habilitar recursos anti-exploração	Dispositivo	Proteger	IG2 | IG3
10.6) Gerir o *software* anti-*malware* de maneira centralizada	Dispositivo	Proteger	IG2 | IG3
10.7) Usar *software* anti-*malware* baseado em comportamento	Dispositivo	Detetar	IG2 | IG3

Tabela 11: Medidas de segurança do controlo de segurança 10 (autoria própria com base no CIS [6])

11. ***CIS Critical Security Control 11*: Recuperação de dados**

Refere-se a estabelecer e manter práticas de recuperação de dados suficientes para restaurar ativos da empresa para um estado pré-incidente confiável. Deste modo, os 5 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
11.1) Estabelecer e manter um processo de recuperação de dados	Dados	Recuperar	IG1 | IG2 | IG3
11.2) Executar *backups* automatizados	Dados	Recuperar	IG1 | IG2 | IG3
11.3) Proteger os dados de recuperação	Dados	Proteger	IG1 | IG2 | IG3
11.4) Estabelecer e manter uma instância isolada de dados de recuperação	Dados	Recuperar	IG1 | IG2 | IG3
11.5) Testar os dados de recuperação	Dados	Recuperar	IG2 | IG3

Tabela 12: Medidas de segurança do controlo de segurança 11 (autoria própria com base no CIS [6])

12. ***CIS Critical Security Control 12*: Gestão da infraestrutura de rede**

Referente ao estabelecimento, implementação e gestão ativa de dispositivos de rede, com a finalidade de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis. Deste modo, os 8 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
12.1) Assegurar que a infraestrutura de rede esteja atualizada	Rede	Proteger	IG1 | IG2 | IG3
12.2) Estabelecer e manter uma arquitetura de rede segura	Rede	Proteger	IG2 | IG3
12.3) Gerir a infraestrutura de rede com segurança	Rede	Proteger	IG2 | IG3
12.4) Estabelecer e manter diagrama(s) de arquitetura	Rede	Identificar	IG2 | IG3
12.5) Centralizar a autenticação, autorização e auditoria (AAA) de rede	Rede	Proteger	IG2 | IG3
12.6) Usar protocolos de comunicação e gestão de rede seguros	Rede	Proteger	IG2 | IG3
12.7) Assegurar que os dispositivos remotos utilizem uma VPN e estejam a conectar-se a uma infraestrutura AAA da empresa	Dispositivo	Proteger	IG2 | IG3
12.8) Estabelecer e manter recursos de computação dedicados para todo o trabalho administrativo	Dispositivo	Proteger	IG3

Tabela 13: Medidas de segurança do controlo de segurança 12 (autoria própria com base no CIS [6])

13. ***CIS Critical Security Control 13*: Monitorização e defesa da rede**

Refere-se a operar processos e ferramentas para estabelecer e manter a monitorização e defesa da rede contra ameaças de segurança em toda a infraestrutura de rede e base de utilizadores da empresa. Deste modo, os 11 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
13.1) Centralizar o alerta de eventos de segurança	Rede	Detetar	IG2 | IG3
13.2) Implementar uma solução de deteção de intrusão baseada em *host*	Dispositivo	Detetar	IG2 | IG3
13.3) Implementar uma solução de deteção de intrusão de rede	Rede	Detetar	IG2 | IG3
13.4) Realizar filtragem de tráfego entre segmentos de rede	Rede	Proteger	IG2 | IG3
13.5) Gerir controlo de acesso para ativos remotos	Dispositivo	Proteger	IG2 | IG3
13.6) Recolher *logs* de fluxo de tráfego da rede	Rede	Detetar	IG2 | IG3
13.7) Implementar solução de prevenção de intrusão baseada em *host*	Dispositivo	Proteger	IG3
13.8) Implementar uma solução de prevenção de intrusão de rede	Rede	Proteger	IG3
13.9) Implementar controlo de acesso no nível da porta	Dispositivo	Proteger	IG3
13.10) Executar filtragem da camada de aplicação	Rede	Proteger	IG3
13.11) Ajustar limites de alerta de eventos de segurança	Rede	Detetar	IG3

Tabela 14: Medidas de segurança do controlo de segurança 13 (autoria própria com base no CIS [6])

14. ***CIS Critical Security Control 14*: Consciencialização de segurança e treino de habilidades**

Referente ao estabelecimento de um programa de consciencialização de segurança para influenciar o comportamento da força de trabalho para ser consciente em segurança e devidamente qualificada para reduzir os riscos de cibersegurança para a empresa. Deste modo, os 9 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
14.1) Estabelecer e manter um programa de consciencialização de segurança	N/A	Proteger	IG1 | IG2 | IG3
14.2) Treinar os membros da força de trabalho para reconhecerem ataques de engenharia social	N/A	Proteger	IG1 | IG2 | IG3
14.3) Treinar os membros da força de trabalho nas melhores práticas de autenticação	N/A	Proteger	IG1 | IG2 | IG3
14.4) Treinar a força de trabalho nas melhores práticas de tratamento de dados	N/A	Proteger	IG1 | IG2 | IG3
14.5) Treinar os membros da força de trabalho sobre as causas da exposição não intencional de dados	N/A	Proteger	IG1 | IG2 | IG3
14.6) Treinar os membros da força de trabalho no reconhecimento e comunicação de incidentes de segurança	N/A	Proteger	IG1 | IG2 | IG3
14.7) Treinar a força de trabalho sobre como identificar e comunicar se nos seus ativos da empresa estão a faltar atualizações de segurança	N/A	Proteger	IG1 | IG2 | IG3
14.8) Treinar a força de trabalho sobre os perigos de se conectarem e transmitirem dados da empresa em redes inseguras	N/A	Proteger	IG1 | IG2 | IG3
14.9) Conduzir o treino de competências e consciencialização de segurança para funções específicas	N/A	Proteger	IG2 | IG3

Tabela 15: Medidas de segurança do controlo de segurança 14 (autoria própria com base no CIS [6])

15. ***CIS Critical Security Control 15*: Gestão de fornecedores de serviços**

Refere-se ao desenvolvimento de um processo para avaliar os fornecedores de serviços que mantêm dados sensíveis, ou são responsáveis por plataformas, ou processos de tecnologias da informação (*IT*) críticos de uma empresa, para garantir que estes estejam a proteger essas plataformas e dados adequadamente. Deste modo, os 7 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
15.1) Estabelecer e manter um inventário de fornecedores de serviço	N/A	Identificar	IG1 | IG2 | IG3
15.2) Estabelecer e manter uma política de gestão de fornecedores de serviços	N/A	Identificar	IG2 | IG3
15.3) Classificar fornecedores de serviços	N/A	Identificar	IG2 | IG3
15.4) Garantir que os contratos do fornecedor de serviços incluam requisitos de segurança	N/A	Proteger	IG2 | IG3
15.5) Avaliar fornecedores de serviços	N/A	Identificar	IG3
15.6) Monitorizar fornecedores de serviços	Dados	Detetar	IG3
15.7) Descomissionar com segurança os fornecedores de serviços	Dados	Proteger	IG3

Tabela 16: Medidas de segurança do controlo de segurança 15 (autoria própria com base no CIS [6])

16. ***CIS Critical Security Control 16*: Segurança de aplicações de *software***

Referente à gestão do ciclo de vida de segurança do *software* desenvolvido, hospedado ou adquirido internamente para prevenir, detetar e corrigir os pontos fracos de segurança antes que possam afetar a empresa. Deste modo, os 14 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
16.1) Estabelecer e manter um processo seguro de desenvolvimento de aplicações	Aplicações	Proteger	IG2 | IG3
16.2) Estabelecer e manter um processo para aceitar e endereçar vulnerabilidades de *software*	Aplicações	Proteger	IG2 | IG3
16.3) Executar análise de causa raiz em vulnerabilidades de segurança	Aplicações	Proteger	IG2 | IG3
16.4) Estabelecer e gerir um inventário de componentes de *software* de terceiros	Aplicações	Proteger	IG2 | IG3
16.5) Usar componentes de *software* de terceiros atualizados e confiáveis	Aplicações	Proteger	IG2 | IG3
16.6) Estabelecer e manter um sistema de classificação de gravidade e processo para vulnerabilidades de aplicações	Aplicações	Proteger	IG2 | IG3
16.7) Usar modelos de configurações de segurança padrão para infraestrutura de aplicações	Aplicações	Proteger	IG2 | IG3
16.8) Separar sistemas de produção e não produção	Aplicações	Proteger	IG2 | IG3
16.9) Treinar desenvolvedores em conceitos de segurança de aplicações e codificação segura	Aplicações	Proteger	IG2 | IG3
16.10) Aplicar princípios de *design* seguro em arquiteturas de aplicações	Aplicações	Proteger	IG2 | IG3
16.11) Aproveitar os módulos ou serviços controlados para componentes de segurança de aplicações	Aplicações	Proteger	IG2 | IG3
16.12) Implementar verificações de segurança no nível de código	Aplicações	Proteger	IG3
16.13) Realizar testes de intrusão de aplicações	Aplicações	Proteger	IG3
16.14) Conduzir aplicações de modelagem de ameaças	Aplicações	Proteger	IG3

Tabela 17: Medidas de segurança do controlo de segurança 16 (autoria própria com base no CIS [6])

17. *CIS Critical Security Control 17*: Resposta e gestão de incidentes

Referente ao estabelecimento de um programa para desenvolver e manter uma capacidade de resposta a incidentes para preparar, detetar e responder rapidamente a um ataque. Deste modo, os 9 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
17.1) Designar pessoal para gerir tratamento de incidentes	N/A	Responder	IG1 | IG2 | IG3
17.2) Estabelecer e manter informações de contato para relatar incidentes de segurança	N/A	Responder	IG1 | IG2 | IG3
17.3) Estabelecer e manter um processo empresarial para relatar incidentes	N/A	Responder	IG1 | IG2 | IG3
17.4) Estabelecer e manter um processo de resposta a incidentes	N/A	Responder	IG2 | IG3
17.5) Atribuir funções e responsabilidades chave	N/A	Responder	IG2 | IG3
17.6) Definir mecanismos de comunicação durante a resposta a incidentes	N/A	Responder	IG2 | IG3
17.7) Conduzir exercícios de resposta a incidentes de rotina	N/A	Recuperar	IG2 | IG3
17.8) Conduzir análises pós-incidente	N/A	Recuperar	IG2 | IG3
17.9) Estabelecer e manter limites de incidentes de segurança	N/A	Recuperar	IG3

Tabela 18: Medidas de segurança do controlo de segurança 17 (autoria própria com base no CIS [6])

18. *CIS Critical Security Control 18: Penetration Testing*

Refere-se ao teste da eficácia e da resiliência dos ativos da empresa através da identificação e exploração de fraquezas nos controlos e da simulação dos objetivos e ações de um atacante. Deste modo, os 5 subcontrolos associados com o tipo de ativo a que se referem, o mapeamento para as funções da NIST *Framework* e os seus respetivos grupos de implementação podem ser observados na tabela seguinte:

Medida de segurança	Tipo de Ativo	Função de Segurança (NIST *Framework*)	Grupo de Implementação
18.1) Estabelecer e manter um programa de testes de penetração	N/A	Identificar	IG2 | IG3
18.2) Realizar testes de penetração externos periódicos	Rede	Identificar	IG2 | IG3
18.3) Corrigir as descobertas do teste de penetração	Rede	Proteger	IG2 | IG3
18.4) Validar as medidas de segurança	Rede	Proteger	IG3
18.5) Realizar testes de penetração internos periódicos	N/A	Identificar	IG3

Tabela 19: Medidas de segurança do controlo de segurança 18 (autoria própria com base no CIS [6])

2.8 SUMÁRIO

De modo geral, este estado da arte aspirou mostrar alguns dos *standards*, boas práticas, estratégias ou documentos que existem publicados por organizações credíveis relacionados à cibersegurança e à definição de uma estratégia.

Primeiramente, foram analisados os principais conceitos em torno da cibersegurança e da definição de uma estratégia empresarial de cibersegurança através de algumas definições de conceitos e do relatar dos principais riscos e controlos de prevenção que existem e são de âmbito genérico para abordar o tema da cibersegurança. Deste modo, consegue-se entender a necessidade de uma empresa/organização definir uma estratégia de cibersegurança que consiga mitigar pelo menos alguns dos ataques mais comuns. Para enfrentar esse problema, pode-se simplesmente seguir as listas de controlos apresentadas. Porém, existem abordagens mais técnicas e estratégicas para resolver o problema, sendo este o âmbito da presente dissertação, daí a necessidade de abordar mais alguma documentação publicada por outras instituições de segurança que definem métodos mais estruturados e sistemáticos.

Por outro lado, antes de se falar em *frameworks* e controlos para definição de uma estratégia, pretendeu-se mostrar alguns dos princípios-base das estratégias de cibersegurança em organizações governamentais. Como a presente dissertação, apesar de poder ser usada por qualquer pequena e média empresa, está a ser desenvolvida em Portugal, que está inserido no espaço europeu, é efetuada uma referência às estratégias de cibersegurança da União Europeia (secção 2.2) e de Portugal (secção 2.3). A seguir, pretendeu-se falar de outras estratégias de cibersegurança (secção 2.4) que existem para enriquecer mais o conhecimento teórico no que a este tema diz respeito, pelo que é abordada uma estratégia que está mais no âmbito dos Estados Unidos da América e outra que foi feita no Reino Unido.

Por fim, é descrito um conjunto de documentos publicados por grandes instituições de segurança que serão úteis na altura de definir um plano de cibersegurança para as empresas. Deste modo, começa-se por falar da *NIST Framework* (secção 2.5), considerada por muitos um dos guias mais fundamentais para quem quer implementar uma estratégia de cibersegurança, sendo que é por aqui que se vai poder definir um *"roadmap"* de atuação e de implementação de certos controlos, procedimentos, regras e políticas nas empresas, sempre com preocupação com a gestão de riscos. Porém, apesar de a *NIST Framework* também disponibilizar uma forma de autoavaliar a situação da empresa, esta não define a maturidade da empresa ao nível de segurança, sendo por isso que na secção seguinte é apresentado um modelo de maturidade (*C2M2*) (secção 2.6). Com este modelo, é possível com mais precisão efetuar-se autoavaliações ao estado da cibersegurança da empresa e melhor identificar lacunas, pelo que a conjugação da *NIST Framework* com o *C2M2* é capaz de produzir os melhores resultados e atuar de forma mais eficaz na empresa. Por último, falou-se dos dezoito controlos de segurança da *CIS* (secção 2.7), dado que mostram um conjunto de controlos de segurança mais práticos e técnicos para as empresas, sendo que possuí ainda compatibilidade com a *NIST Framework*. Outra das grandes vantagens é o facto de dentro de cada controlo haverem medidas de segurança para os concretizarem e estes estarem divididos em grupos de segurança crescente, o que é

bom para empresas que não consigam implementar certas medidas, terem ao menos a noção qual é o básico que estas devem ter implementadas.

Assim, foi dada uma visão geral sobre a literatura relacionada à área da cibersegurança e algumas formas diferentes de atuar nas empresas com o intuito de definir uma estratégia capaz de proteger a empresa contra eventuais incidentes de segurança. É por este conjunto de noções de como se encontra o estado da arte que pode-se dar início à abordagem ao problema e efetivamente trabalhar no núcleo da dissertação.

3

PROBLEMA E DESAFIOS

Como já se percebeu pela leitura do estado da arte (capítulo 2), a necessidade de definir uma estratégia de cibersegurança nas empresas está a ganhar uma relevância maior. Isto deve-se não só à evolução tecnológica das empresas, mas também ao crescimento das ameaças informáticas a que as empresas estão sujeitas. Porém, nem sempre desenvolver uma política de cibersegurança que atue com precisão e eficácia nas empresas é algo fácil, e existem muitos desafios colocados na altura de a definir.

A proteção daqueles que são os nossos bens materiais sempre foram uma necessidade, não só a nível pessoal, mas especialmente quando se fala de uma empresa. Por exemplo, uma empresa de construção é normal que precise de máquinas, materiais de construção, entre outras coisas. Ora, esta empresa fez um investimento avultado em ativos que necessita para conseguir desempenhar as suas funções com maior eficácia e competitividade, todavia estes terão de estar guardados num local seguro contra roubos, provavelmente as instalações da empresa. Porém, para este lugar ficar seguro poderá ser necessário que a empresa também invista em segurança, por exemplo, contratando uma empresa de segurança ou até um sistema de alarmes e videovigilância. Deste modo, percebe-se que existem vários desafios a serem postos à empresa para conseguir proteger os seus ativos e assim impedir que o investimento feito tenha sido em vão.

Este problema da segurança empresarial ao nível dos ativos físicos pode ser transposto para a segurança informática. Aliás, tem também relação direta porque podemos agora imaginar que a empresa decide adquirir um conjunto de servidores em *cluster* que constituem um enorme investimento para a empresa. E neste caso, até pode ser mais prioritário o investimento em segurança, pois, alguns recursos informáticos são bastante valiosos. Porém, a partir do momento em que a empresa começa a evoluir mais e a tornar-se mais tecnológica, haverá certamente um número maior de desafios relacionados com a segurança da informação que terão de ser acautelados.

De modo geral, aquilo que se pretende com esta dissertação de mestrado é dar ênfase à necessidade de uma empresa criar uma estratégia de cibersegurança para a proteção dos seus ativos de informação, mas acima de tudo para evitar ataques que possam afetar tanto a disponibilidade ou integridade de um serviço seguro e confiável para os clientes da empresa, como afetar económica ou financeiramente a empresa através de roubo de informações confidenciais. Por exemplo, se houver um ataque à infraestrutura da empresa que bloqueie os seus serviços e haja por parte dos *hackers* um pedido de pagamento, por exemplo, usando criptomoedas, para voltar a disponibilizar à empresa os serviços, estamos perante uma situação complicada para a organização que em muitos dos casos pode originar um prejuízo de milhões caso a empresa não tenha já implementado uma estratégia efetiva de cibersegurança.

Uma empresa pode investir na criação de uma estratégia de cibersegurança através da contratação de um ou mais profissionais de cibersegurança que asseguram a sua implementação e mostram diversas alternativas de investimento para o reforço da segurança, sendo que a última palavra como é óbvio será sempre dos executivos da empresa. Os donos da estratégia de cibersegurança são responsáveis por definir como a cibersegurança de um

sistema atua para cumprir a sua missão, mesmo sob ataque [110]. Além disso, os donos devem conseguir planear e projetar a resiliência suficiente para reconhecer, resistir e recuperar de ataques e ainda devem avaliar alternativas durante as decisões de modo a determinar o nível de risco de cibersegurança aceite. Assim, é fundamental que consigam implementar os requisitos de segurança apropriados para garantir a confidencialidade, integridade e disponibilidade dos vários tipos de ativos de informação.

Todavia, existem vários desafios mesmo após a decisão de se fazer uma estratégia de cibersegurança, sendo que alguns deles já foram sendo referidos durante o capítulo 2 do estado da arte, mas são de salientar os seguintes:

- **Gestão de Riscos**: É fundamental que a empresa defina uma estratégia ou abordagem para gerir os riscos de cibersegurança. Deste modo, a empresa tem de tomar decisões relativamente ao nível de cibersegurança que planeia ter através da definição de prioridades de investimento e da aceitação do risco, levando também em consideração uma análise de custo-benefício. Efetivamente, ter o nível de segurança mais elevado de todos pode não ser a melhor estratégia para a empresa, muito porque a análise custo-benefício pode não o recomendar. Além disso, pode haver setores dentro de uma organização que são mais prioritários e necessitam de um maior nível de investimento. Assim, é quem está no nível da implementação, no de definição da estratégia e no nível executivo ou de administração da empresa que deve acordar, dialogar, analisar e verificar decisões de gestão de risco para que deste modo se consiga chegar a um consenso relativamente ao risco a que a empresa/organização irá estar exposta, sendo importante a documentação das decisões tomadas.

- **Evolução do ambiente de ameaças**: O ambiente de ameaças a que estaremos expostos no futuro é imprevisível e vai mudando com o tempo, seja porque aparecem novas ameaças ou porque estas tornam-se mais ou menos perigosas. Para este ambiente existem muitos fatores, como, por exemplo, a evolução da computação, dos métodos e algoritmos informáticos, das relações empresariais ou até relações entre países. Muitos dos ataques informáticos que acontecem têm na sua origem interesses económicos e financeiros, ou possuem motivações políticas, seja porque os países se encontram em guerra, ou devido a conflitos entre minorias. Exemplo disso foram os ataques efetuados à Estónia em 2007 que deixaram os *sites* do governo indisponíveis. Nestes ataques distribuídos de negação de serviço (DDoS), vários *sites* ficaram indisponíveis por algumas horas, não causando danos permanentes aos serviços da Estónia [108]. Acredita-se que estes ataques possam ter tido origem numa mudança, efetuada pelo governo da Estónia, do local de uma estátua localizada em *Tallinn* para o cemitério da Defesa de *Tallinn*, sendo que esta estátua era um memorial da 2.ª guerra mundial representativo da vitória da União Soviética sobre o nazismo. Esta mudança fez exaltar os russos dentro e fora da Estónia, tendo-se concluído que o governo da Rússia não estava envolvido diretamente nos ataques, sendo a sua origem desconhecida até hoje, mas as suspeitas continuam a recair sobre pessoas de origem russa. Até hoje, a Estónia e os seus cidadãos tem mantido uma postura, no que diz respeito à cibersegurança, de muito investimento e grande preocupação comparando com os outros países, sendo até pioneira em muitas das investigações da área [2].

- **Prazo de vida dos sistemas de *hardware***: Todos os sistemas de *hardware* têm o seu tempo de vida, tais como computadores portáteis e fixos, servidores, *routers*, impressoras, dispositivos de IoT ("*Internet of Things*"), entre outros. Esse facto pode ter implicações na altura de definir uma estratégia de cibersegurança, uma vez que certo *software* e sistemas operativos podem não ser perfeitamente compatíveis com esse *hardware*. Por isso, é importante que haja o inventário de todos os ativos da empresa para perceber quais os dispositivos disponíveis e ainda como se vai proceder para que a estratégia consiga ser implementada.

Estas decisões podem implicar tanto a manutenção destes dispositivos como a compra ou investimento em novos, mais atualizados, para o mesmo efeito. Por exemplo, um determinado dispositivo de *hardware* pode já estar tão obsoleto que não deve mais ser usado na empresa por questões de segurança, seja porque já não consegue correr *software* essencial para a segurança da empresa ou têm especificações que fazem dele um mau ativo no que diz respeito à cibersegurança.

- **Prazo de vida dos sistemas de *software***: Este é um dos aspetos mais importantes a se ter em conta na altura de definir uma estratégia de cibersegurança. Em termos de segurança, devem-se seguir modelos de desenvolvimento de *software* seguro, sendo que isso pode tornar os sistemas mais duradouros e com menos atualizações (*patches*). Mas, efetivamente, os sistemas de *software* quando são construídos e depois configurados numa empresa, não constituem um ativo duradouro, sendo que devem sofrer atualizações ao longo do tempo. Tudo isto devido à constante evolução tanto da tecnologia ou dos métodos de ataque como também na reparação de erros que vão surgindo no *software* e podem ser notados tanto pelos fornecedores desse sistema como por entidades externas, utilizadores do sistema ou até, em casos mais graves, por atacantes. Daí a necessidade de se falar em vulnerabilidades de *software*.

  As vulnerabilidades num sistema de *software* quando são notadas podem ser um meio para que atacantes usem essa falha para uma determinada entidade que use esse *software*, sendo que eles desenvolvem um determinado método de exploração, ou *exploit*, para ser possível efetuar um ataque com sucesso. Porém, a situação torna-se mais severa quando se fala de vulnerabilidades *"zero-day"*, como descrito na secção 2.1.3, mas ainda é preciso alertar as pessoas que certo *software* constituí um grande perigo, pois possuem vulnerabilidades gravíssimas que o tornam inseguro. Normalmente, o que os fornecedores de um determinado *software* com vulnerabilidades e respetivos *exploits* conhecidos fazem é desenvolver uma forma de tratamento dessas vulnerabilidades, o que acontece através de atualizações desse mesmo *software*. Para combater este desconhecimento por parte das pessoas que utilizam um determinado *software* sobre as vulnerabilidades a que os vários programas mais conhecidos estão sujeitos, e quais as versões afetadas, existem bases de dados de vulnerabilidades e *exploits* (como a da NIST [92]) e de falhas mais comuns (como a da MITRE [87]) aos quais os vários utilizadores podem aceder para verificarem os tipos de vulnerabilidades existentes, se existem *exploits* já conhecidos para os explorar e se as vulnerabilidades são de um tipo comum já conhecido de falha. Desta forma, é possível haver a partilha de conhecimento e colaboração entre as várias entidades interessadas.

  Para ilustrar os desafios colocados constantemente a um profissional de segurança e a atenção constante ao meio que este deve ter, será apresentado um exemplo atual de um *"Zero-day exploit"* que foi descoberto no dia 9 de dezembro de 2021 e tem preocupado a comunidade de programadores e as grandes indústrias de *software*. Esse *exploit* surgiu na biblioteca de *Java Log4j* (versão 2) na *Log4Shell*, e resulta num *Remote Code Execution* (RCE). A vulnerabilidade associada, identificada como CVE-2021-44228 [95], possuí conforme o que consta no *National Vulnerability Database* (NVD) da NIST um *Base Score* de **10.0 CRITICAL**, que é, segundo a medida de severidades e métricas do *CVSS 3.x*, a pontuação mais alta de gravidade que uma vulnerabilidade pode ter. Até ao momento da escrita desta dissertação, quase todas as versões do *log4j* versão 2 são afetadas, mas já foi lançada a versão 2.17.0 ou ainda *patches* do JNDI (*Java Naming and Directory Interface*) para mitigação temporária [111].

  Em suma, para que o *exploit* funcione é necessário:

  – Um servidor com uma versão *log4j* vulnerável;

– Um *endpoint* com qualquer protocolo (HTTP, TCP, etc.) que permite que um atacante envie a *string* de exploração,

– e uma instrução de *log* que efetua *logout* da *string* dessa solicitação.

Efetivamente, o que acontece é que o *Log4j* permite que mensagens de *log* contenham *strings* de formato que fazem referência a informações externas através do *Java Naming and Directory Interface* (JNDI). Isso permite que as informações sejam recuperadas remotamente através de uma variedade de protocolos já listados acima, como o *Lightweight Directory Access Protocol* (LDAP). Por exemplo, quando *Log4j* encontra a seguinte *string* numa mensagem de *log*:

```
${jndi:ldap://prplbx.com/security}
```

É dada a instrução ao JNDI para solicitar ao servidor LDAP localizado em *"prplbx.com"* o objeto *"security"*. Por *design*, o JNDI executará classes Java às quais um servidor LDAP faz referência, pelo que se a resposta do servidor LDAP fizer referência ao URL https://prplbx.com/security, o JNDI solicitará automaticamente o ficheiro security.class do servidor *web* e executará a resposta. Como o conteúdo das mensagens de *log* contém geralmente dados controlados pelo utilizador, os atacantes podem inserir referências JNDI apontando para os servidores LDAP que controlam, prontos para disponibilizar classes Java maliciosas que executam qualquer ação que eles escolherem [100]. Na Figura 5, pode-se ver uma ilustração da forma de exploração da vulnerabilidade do log4j CVE-2021-44228.

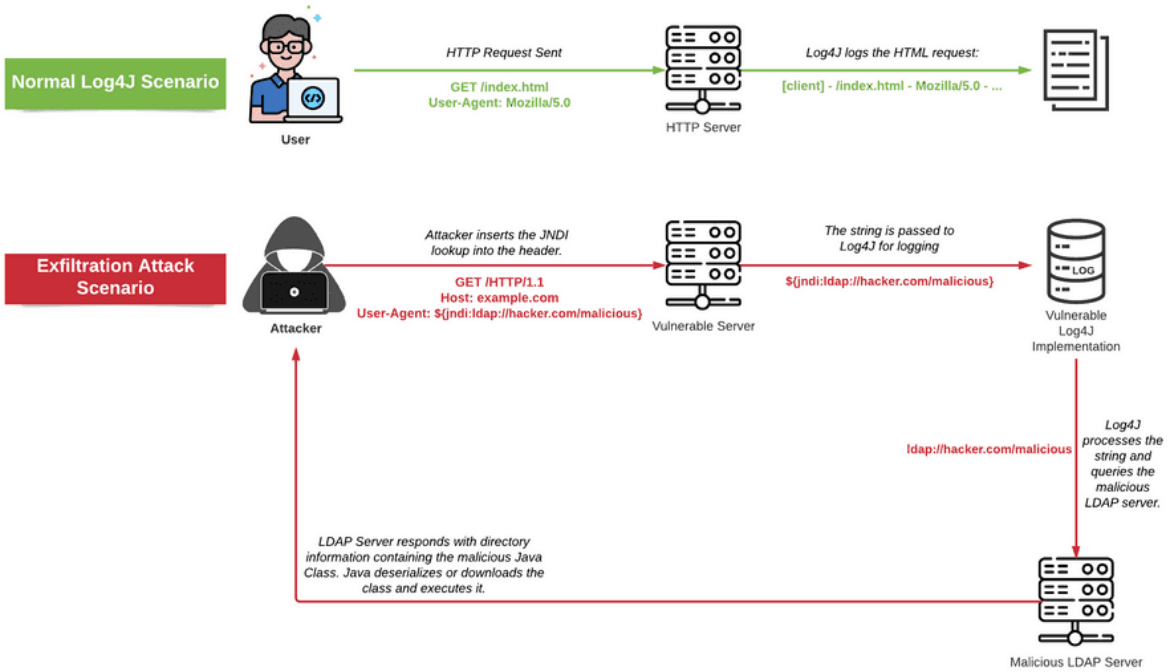


Figura 5: Ilustração de um exemplo de como se pode explorar a vulnerabilidade CVE-2021-44228 (Fonte: [100])

Assim, de uma forma relativamente simples, é possível colocar *malware* a correr no computador de clientes que utilizam aplicações *Java* vulneráveis a este *exploit*. Dada a omnipresença da biblioteca *Log4j*, o impacto do *exploit* (controlo total do servidor) e a facilidade de exploração, as consequências desta vulnerabilidade podem ser catastróficas. Muitos serviços são vulneráveis a este *exploit*, como serviços em *cloud* da *Steam*,

Apple iCloud e aplicações como *Minecraft*. Foi ainda demonstrado que a simples mudança do nome de um *iPhone* desencadeia a vulnerabilidade nos servidores da *Apple*. Outros serviços vulneráveis são o *Tencent*, *Twitter*, *Baidu*, *Didi*, *Cloudflare*, *Amazon*, *Tesla*, *ElasticSearch* e o *Ghidra* [88].

- **Legislação/normas em vigor**: As leis ou normas que estão em vigor no mundo da indústria vão mudando com o passar dos anos, dependendo muito do local onde a organização estiver inserida. Por exemplo, uma empresa que se situa nos Estados Unidos deve obedecer a leis e regras publicadas pelo governo desse país. No caso português, e o facto de Portugal pertencer à União Europeia, fazem com que as empresas tenham de se preocupar tanto com as leis e regras em vigor em Portugal como com as que são publicadas pela União Europeia. Nessa perspetiva, é sempre importante que, na altura de definir uma estratégia de cibersegurança numa empresa portuguesa, se tenha em consideração todos os pressupostos presentes nos documentos publicados tanto no Diário da República Português como os que estão publicados no *site* da Comissão Europeia. Deste modo, rever leis como a lei n.º 46/2018 [17], o RGPD (Regulamento Geral de Proteção de Dados) [22], entre outras, deve ser uma tarefa que quem está encarregue da estratégia deve ter em consideração. Assim, é possível averiguar se existem inconvenientes na implementação de determinada medida de cibersegurança na empresa ou então se a empresa obedece aos requisitos de cibersegurança impostos pela lei.

- **Evolução da ciência da computação**: Este é um tópico muito relacionado com a constante evolução tanto dos vários sistemas de *software* como de *hardware*. Efetivamente, com o passar dos anos, a ciência da computação vai evoluindo a um ritmo impressionante, o que faz com que tanto o *software* fique mais refinado e com mais potencialidades, como o *hardware* fique mais potente e capacitado para suportar algoritmos de computação que, em máquinas antigas, demorariam mais tempo a serem processados. Deste modo, algoritmos de criptografia que eram considerados antigamente seguros, com o passar do tempo podem tornar-se inseguros, havendo por isso a necessidade da criação de algoritmos com níveis de segurança maiores ou mudanças nos protocolos de segurança. Alguns exemplos vão desde algoritmos de cifragem tanto de chave pública como privada, algoritmos de *hash* ou até protocolos de segurança que com o tempo passaram a ser obsoletos. Exemplo de como a comunidade científica tenta constantemente evoluir e a testar a segurança de algoritmos considerados seguros é a emergência da computação quântica que planeia revolucionar, ainda mais, a maneira como se olha para segurança. O interesse geral e a excitação na computação quântica foram inicialmente desencadeados por Peter Shor em 1994, que mostrou como um algoritmo quântico poderia "acelerar" exponencialmente a computação clássica e fatorizar números grandes em primos com muito mais eficiência do que qualquer algoritmo clássico. Assim, a implementação do algoritmo de Shor num computador quântico de grande escala teria consequências devastadoras para os atuais protocolos de criptografia [96].

- **Cultura de cibersegurança**: A existência de uma cultura de cibersegurança é, na maior parte dos casos, dependente do meio onde a empresa se encontra. Como referido anteriormente, a Estónia tem investido fortemente em programas de educação e formação nos últimos anos, sendo que se digitalizou muito mais cedo do que outros países, concentrando-se em coisas como o ensino e serviços do governo *online*, adotando uma abordagem mais proativa à tecnologia [2]. Porém, quando se fala no ramo empresarial, é fundamental perceber que esta cultura também depende das medidas que a organização tiver em vigor. Por exemplo, a realização de palestras de cibersegurança por parte de profissionais na área para os funcionários da empresa pode ser um bom caminho para alertar todos os colaboradores e *stakeholders* da importância de se preocuparem com estas questões e, deste modo, treiná-los para responder a situações de risco ou para

terem boas práticas no desempenho das suas funções. Assim, se todos estiverem cientes das ameaças a que a organização está sujeita e respeitarem o programa de cibersegurança que a empresa tiver em vigor, será mais fácil produzir resultados mais eficazes e contribuir para o sucesso da estratégia de cibersegurança.

- **Uso ou criação de *software* com más práticas de programação segura**: Muitas vezes os programadores de *software* têm tendência a criar *software* sem grandes preocupações de segurança ou então usando os métodos mais fáceis e rápidos para o efeito. Isto porque a maioria deles estão mais interessados em ter o programa pronto e operacional para desempenhar as suas funcionalidades e ser o mais rentável possível, em vez de terem o cuidado de olharem com mais atenção para a segurança do *software*. Isto faz com que algumas empresas possam estar a usar *software* inseguro ou até os seus funcionários estarem a criar *software* inseguro. Caso a empresa esteja a usar programas inseguros, percebe-se claramente o perigo que isto pode trazer para a infraestrutura da empresa, pois contêm falhas ou lacunas que podem levar a intrusões nos seus sistemas. Já no caso de estarem a criar *software* inseguro, pode ser também negativo para a empresa, não só ao nível da segurança, mas também ao nível da reputação da empresa. Como, normalmente, o *software* será destinado a um determinado cliente, este cliente passará a estar inseguro, fazendo com que a probabilidade de ataques a esse cliente sejam maiores. Caso haja um ataque a esse cliente ou incidente de segurança, a responsabilidade será do fornecedor do *software*, o que pode manchar a empresa tanto a nível económico como até da sua reputação. Assim, é importante usar princípios de desenvolvimento de *software* seguro, como o Ciclo de Vida de Desenvolvimento Seguro (SDL — *Security Development Lifecycle*) da *Microsoft*, que apresenta considerações de segurança e privacidade em todas as fases do processo de desenvolvimento, ajudando os programadores a criar um *software* altamente seguro, a atenderem aos requisitos de conformidade de segurança e ainda a reduzirem os custos de desenvolvimento [86]. Por fim, para educar programadores de *software*, *designers*, arquitetos, gerentes e as organizações em geral sobre as consequências de existirem pontos fracos de segurança nas aplicações, recomenda-se seguir o **OWASP Top 10** de pontos fracos de segurança em aplicações da *web* mais comuns e importantes [98].

- **Cadeia de Abastecimento da Empresa**: Relativamente à cadeia de abastecimento, ou *supply chain* em inglês, existem muitos pontos a ter em consideração e é uma das componentes mais críticas de segurança. Efetivamente, tudo o que são fornecedores, transportadoras ou logística devem fazer parte da estratégia de cibersegurança, uma vez que estes podem também trazer potencialmente perigo para a organização. Neste âmbito devem-se definir políticas/regras de cibersegurança, sendo que inclusive se podem estabelecer acordos com fornecedores ou fabricantes para estes cumprirem os deveres de cibersegurança impostos pela organização. Assim, se todos os intervenientes da cadeia de abastecimento cumprirem com os protocolos de segurança da organização, nomeadamente os que fazem parte da estratégia de cibersegurança, há menos risco de intrusões na rede ou ciberespaço empresarial.

- **Trabalho Remoto (Proteção dos acessos remotos)**: O trabalho remoto, ou teletrabalho, está cada vez a ser mais utilizado em trabalhos em que isso é possível. A maior contribuição para esta nova moda de trabalho tem sido a COVID-19, uma vez que por causa deste ambiente pandémico é importante haver distanciamento social. Porém, o recurso ao trabalho remoto impõe novos perigos de cibersegurança para a organização, uma vez que ao trabalharmos fora do contexto físico da nossa organização tornamos os sistemas e a gestão da informação mais vulnerável, visto estarmos mais expostos a terceiros, quer em termos físicos, quer digitais [12]. Este acesso remoto, normalmente feito através de uma rede virtual privada (VPN), pode ser mais protegido através de medidas de segurança que a empresa deve ter, que servem tanto para proteger a

infraestrutura como os funcionários remotos. Por exemplo, os funcionários da empresa podem estar em casa a usar a *internet* para as suas tarefas indevidamente. Para isto, algumas medidas de segurança devem ser encorajadas por parte da empresa para que os funcionários tenham mais atenção à sua própria segurança e da empresa [84], tais como o uso de antivírus, autenticação de dois fatores (2FA), cópias de *backup*, monitorização de conexões de acesso remoto, criação e implantação de políticas/regras de acesso remoto seguro, atualização de *software* e sistemas operativos e a atualização constante das senhas para serem suficientemente fortes.

- **Resposta a incidentes de cibersegurança**: Este desafio é sem dúvidas um dos mais importante, senão o mais importante, uma vez que responder a um determinado incidente de cibersegurança é uma tarefa complexa. Isto deve-se ao facto da dificuldade em entender como reagir a um ataque que ainda não aconteceu e que pode ser de diversos tipos e origens. Deste modo, a estratégia de cibersegurança deve contemplar, nos seus conjuntos de medidas a implementar, a resposta a incidentes e a forma como prevenir ou evitar danos graves para a empresa que podem resultar em prejuízos elevados. É importante também que a organização mantenha contacto com outras entidades de segurança e comunique os incidentes de segurança para haver não só um maior acompanhamento, mas principalmente para que a informação do ataque fique disponibilizada para o público e possa contribuir para a evolução e a prevenção de futuros incidentes do género tanto na própria organização como noutras. Uma das entidades relevantes em Portugal com preocupações com a resposta a incidentes de cibersegurança em todo o ciberespaço nacional é a CERT.PT [1] [13], que é um serviço integrante do Centro Nacional de Cibersegurança (CNCS) e foi decretado na lei n.º 46/2018 [17] como a Equipa de Resposta a Incidentes de Segurança Informática (CSIRT) Nacional. Segundo o RFC 2350 [14], o CSIRT [2] responde a todos os tipos de incidentes de cibersegurança, tais como os que resultam numa violação de segurança dos tipos: código malicioso, disponibilidade, recolha de informação, tentativa de intrusão, intrusão, segurança da informação, fraude, conteúdo abusivo ou vulnerável. Relativamente a mais algumas medidas para resposta a incidentes, estas passam por ter um sistema de registos (*logs*) para registo dos eventos que acontecem na infraestrutura da organização, ter ainda um sistema de *backups*, ter um sistema de alarmes ou alertas que avise os administradores caso haja alguma anomalia, entre outras que podem ser vistas em diversos documentos de padrões ou boas práticas como os que foram abordados no estado da arte, por exemplo, a *NIST Framework* (secção 2.5).

1 CERT significa *"Computer Emergency Response Team"*
2 CSIRT significa *"Computer Security Incident Response Team"*

Parte II

NÚCLEO DA DISSERTAÇÃO

4

CONTRIBUIÇÃO

4.1 INTRODUÇÃO/CONTEXTUALIZAÇÃO

Após a leitura do material introdutório desta dissertação (capítulos 1, 2 e 3), percebe-se a necessidade de as empresas aplicarem continuamente uma estratégia de cibersegurança. Em Portugal, principalmente nas pequenas e médias empresas (PME's), existe alguma dificuldade em encontrar métodos simples e eficazes de introduzir gradualmente a cibersegurança na empresa e de a reforçar com base nas melhores práticas da indústria. Segundo o Centro Nacional de Cibersegurança (CNCS), as empresas portuguesas aplicam mais medidas de segurança que a média da União Europeia, mas há uma discrepância entre as políticas empregues pelas grandes empresas face às PME [20]. Além disso, segundo o "Relatório de Maturidade Digital em Cibersegurança", elaborado pela Minsait e SIA, 56% das empresas portuguesas carece de uma estratégia de cibersegurança bem definida [20]. Assim, a estratégia de cibersegurança desta tese planeia fornecer às empresas portuguesas uma abordagem eficaz, completa, flexível, inovadora e contínua de estas aplicarem medidas de cibersegurança através da criação de planos ou políticas formais para o efeito.

Para a criação de uma estratégia de cibersegurança é necessário serem consideradas diversas componentes, para ser possível dar início à definição de um *"roadmap"* para a estratégia capaz de abranger ao máximo todas as áreas da cibersegurança de uma empresa e incentivar ao seu reforço. Deste modo, a seguir serão enumeradas as componentes que se tomaram como ponto de partida:

1. Conhecimentos sobre cibersegurança, nomeadamente principais ameaças existentes e *standards* de referência mais conhecidos para a mitigação ou eliminação desses riscos;
2. Conhecimentos gerais das normas e regulamentos de cibersegurança da União Europeia e de Portugal, tal como leis/regras/obrigações que estejam em vigor;
3. Uso da *NIST Framework* [90] como ponto de referência para a criação da estratégia de cibersegurança, sendo amplamente reconhecida a nível internacional [80];
4. Uso do modelo de maturidade C2M2 ("*Cybersecurity Capability Maturity Model*") [26] para complementar as avaliações de desempenho na implementação das práticas de cibersegurança resultantes da estratégia;
5. Uso de diversos controlos/*standards*/medidas de cibersegurança adicionais de várias fontes para serem usados na criação do plano resultante da estratégia de cibersegurança, tais como os 18 controlos da *CIS* v8.0 [6].

É importante ainda referir que a abordagem para a criação de uma estratégia de cibersegurança descrita neste capítulo foi elaborada tendo em vista a sua utilização por empresas portuguesas que tenham intenções de estar

em "*compliance*" e se reforçarem recorrendo a práticas e controlos internacionais de cibersegurança. Porém, com algumas alterações que reflitam o tamanho da empresa, é possível aplicar esta estratégia tanto a PME's como a grandes empresas. Segundo a NIST [90], a *framework* permite a escalabilidade porque está mais orientada para os resultados de cibersegurança a alcançar por uma organização do que para a maneira como ela lá chegou. Desta forma, tanto uma pequena empresa com baixo orçamento como uma grande com orçamento maior para cibersegurança podem usar a NIST CSF com abordagens distintas para atingirem os seus resultados. Assim, é esta flexibilidade da *Framework* que permite a utilização dela tanto por organizações que estão apenas a começar a estabelecer um programa de cibersegurança, como por organizações com programas mais avançados.

Pretende-se com esta abordagem que a empresa que a utilizar possa reforçar o seu conhecimento e cultura de cibersegurança, assim como ficar em *compliance* com a legislação/regras/*standards* de cibersegurança aplicáveis à sua atividade.

4.2 ESTRATÉGIA DE CIBERSEGURANÇA

A leitura da dissertação até ao momento mostra a necessidade de uma empresa construir ou manter um plano e uma estratégia de cibersegurança. Só o facto de uma organização manter regularmente estas preocupações de cibersegurança já pode ser considerada uma medida de cibersegurança. Seja mais formal ou informal, o importante é que a empresa tenha o cuidado de garantir que está o mais cibersegura possível, mantendo uma postura atenta e informada dos riscos de cibersegurança que existem e tentando ao máximo desenvolver os controlos de segurança necessários para eliminar ou mitigar as brechas ou lacunas que existem.

É claro que a inclusão de novas ferramentas de cibersegurança ajuda a garantir esse propósito, mas é fundamental existir uma formalização através de um plano que contenha as medidas, regras e controlos de cibersegurança em vigor na empresa. Desse modo é mais fácil:

- Perceber aquilo que está feito;
- Como se pode melhorar no futuro;
- Priorizar a implementação de certos controlos;
- Informar todas as partes interessadas das suas responsabilidades e deveres;
- Garantir a conformidade com as leis e obrigações a que a empresa está sujeita;
- Melhorar os processos de auditoria de segurança;
- Garantir que todos os colaboradores da organização cumprem com o que está estipulado no plano (que eventualmente pode transformar-se em política da empresa).

Como visto no capítulo "Problema e seus desafios" (capítulo 3), é complexo desenvolver uma estratégia de cibersegurança para uma empresa, pelo que ela nunca será perfeita e à "prova de bala". Porém, se esta usar fontes de informações de cibersegurança fidedignas, se for um processo repetitivo e formalizado para lidar com as mudanças inerentes do mundo e usar formas de medir e também garantir o progresso em cibersegurança na empresa, então é provável que a estratégia seja suficiente para eliminar ou mitigar maior parte dos desafios e riscos existentes.

De modo geral, a estratégia de cibersegurança apresentada nesta dissertação tem por base a abordagem recomendada pela NIST *Framework* (secção 2.5). Em complemento, são introduzidos alguns conceitos diferenciadores que irão refinar ou facilitar o processo de elaboração do plano de cibersegurança, que será o resultado principal da estratégia de cibersegurança.

Um dos conceitos é o de modelo de maturidade em cibersegurança que serve, como o próprio nome diz, para medir a maturidade da empresa em cibersegurança, sendo adequado para realizar as avaliações presentes na NIST *Framework*. O modelo de maturidade escolhido foi o C2M2 (secção 2.6) que inclui um conjunto de ferramentas de autoavaliação que dão orientações para:

- Identificar as práticas de cibersegurança e gestão de riscos da empresa;
- Mapear essas práticas para níveis específicos de maturidade no modelo;
- Definir níveis de maturidade alvo;
- Identificar lacunas e práticas potenciais para permitir que os processos de cibersegurança da organização melhorem ao longo do tempo.

O C2M2 tem compatibilidade com a "*Framework Core*" e com os "*Implementation Tiers*" da NIST *Framework*, pelo que é neste âmbito que a estratégia de cibersegurança irá incluir os recursos do C2M2 para aperfeiçoar, facilitar e ajudar na criação ou melhoria da estratégia, seguindo parte da metodologia apresentada na secção 5 do documento "*ENERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE*" [23].

Por fim, e apesar de na NIST *Framework* existirem apontadores para diversas referências informativas com vários padrões, práticas e controlos de cibersegurança, tais como os da ISO/IEC ("*International Organization for Standardization and the International Electrotechnical Commission*"), do COBIT ("*Control Objectives for Information and Related Technologies*"), da ISA ("*International Society of Automation*"), dos 20 CIS ("*Center for Internet Security*") *Controls* ou até os da própria NIST, nesta estratégia irão ser incluídos os 18 CIS *Critical Security Controls* (2.7). É verdade que originalmente a NIST *Framework* já aponta para controlos da CIS, mas são os controlos antigos (versão 7) que foram recentemente reformulados e passaram a ser só 18, em vez de 20. Além disso, estes controlos fornecem uma visão mais técnica, e não tanto processual como as práticas do C2M2, pelo que completam mais a abordagem apresentada nesta dissertação. Desta forma, na estratégia de cibersegurança são utilizados estes novos controlos da CIS para que as empresas definam aqueles que pretendem ter implementados, havendo talvez a necessidade de serem implementados todos os pertencentes ao grupo 1 ("higiene cibernética básica").

Tendo em conta o que foi referido anteriormente, a estratégia de cibersegurança proposta nesta dissertação tem por objetivo tornar uma empresa mais cibersegura, com processos mais formalizados e organizados, e tendo definido claramente os objetivos ou pilares que regem a sua estratégia. Mais concretamente, os resultados que deverão surgir após percorrer todos os passos do ciclo de vida da estratégia de cibersegurança aqui proposta são:

1. Formalização/Definição do âmbito e prioridades da estratégia de cibersegurança;
2. Melhor compreensão dos sistemas e ativos que devem ser monitorizados e protegidos;
3. Melhor compreensão das normas, leis, requisitos regulamentares e organizacionais, ferramentas, métodos e guias que estão ou devem ser aplicados na empresa;
4. Relatórios que descrevem o nível ou perfil atual em cibersegurança da empresa;

5. Relatórios de avaliação dos riscos atuais que a empresa enfrenta relativos aos processos no âmbito da estratégia;
6. Criação ou revisão do documento formal com as medidas, regras ou políticas de cibersegurança que passaram a estar em vigor na empresa (deverá ser o documento de "Políticas de Cibersegurança" da organização);
7. Relatórios com as lacunas devidamente priorizadas que existem entre o estado atual em cibersegurança e aquilo que se deseja acrescentar para a criação do estado desejado;
8. Documento ou relatório que contém o "plano de ação priorizado" das medidas de cibersegurança adicionais a serem implementadas para se atingir o estado desejado;
9. Relatórios periódicos com o progresso em relação ao "plano de ação priorizado".

4.3 CICLO DE VIDA DA ESTRATÉGIA DE CIBERSEGURANÇA

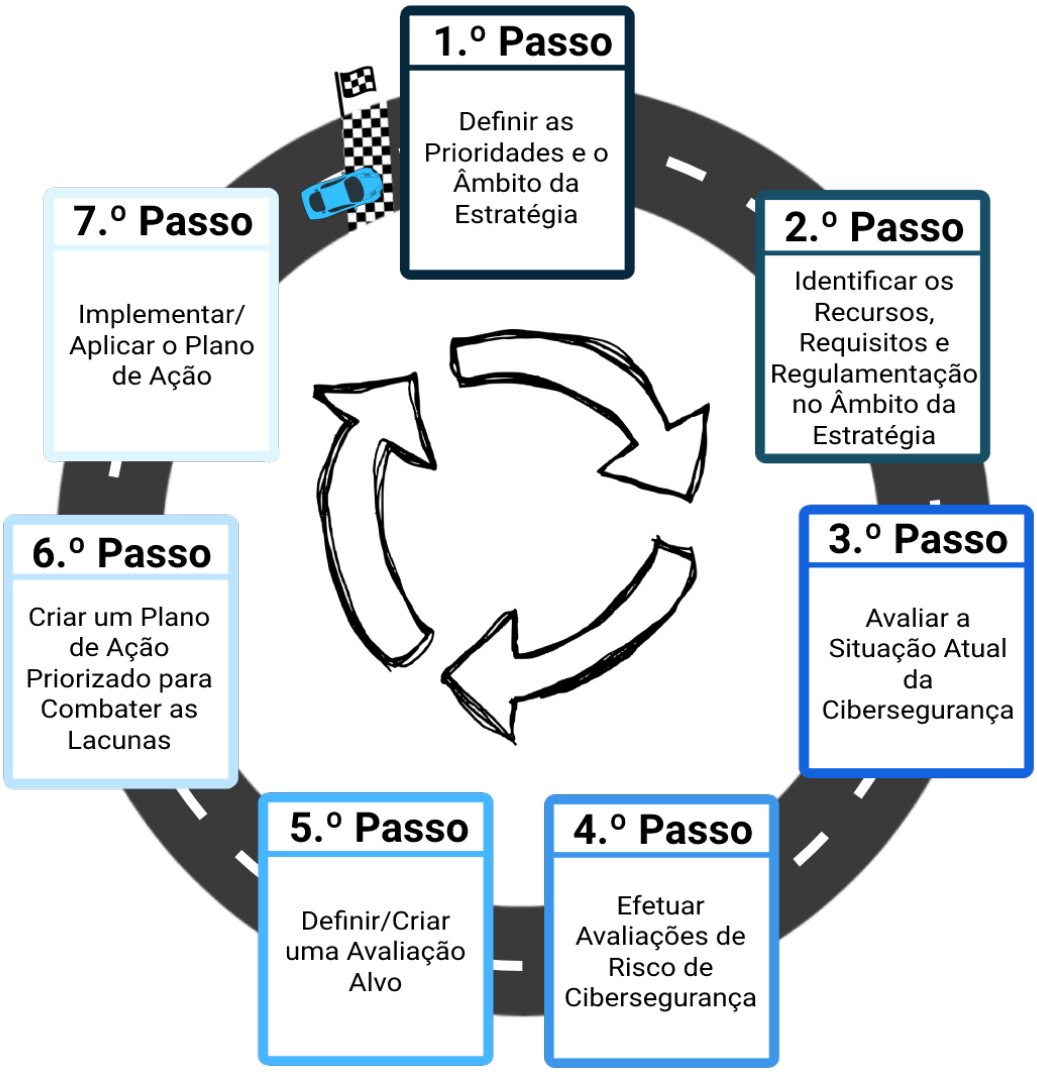


Figura 6: Ciclo de Vida da Estratégia de Cibersegurança

Consoante o referido na secção 4.2, foi concebido um ciclo de vida para a "Estratégia de Cibersegurança", como mostra a Figura 6, onde é evidenciado o seu caráter repetitivo e contínuo. Mas antes de se explicar detalhadamente cada um dos passos da estratégia de cibersegurança, a seguir apresenta-se um resumo de todas as etapas do "*lifecycle*" (ou "*roadmap*") que serão fundamentais para a criação ou melhoria de um "Plano de Cibersegurança".

- **1.º Passo: Definir as Prioridades e o Âmbito da Estratégia**

  Antes de começar a implementação da estratégia de cibersegurança, é fundamental que a empresa que estiver a usar este *"roadmap"* defina quais são as prioridades e o âmbito da sua aplicação. Dentro disto, a organização deve definir o âmbito, os objetivos e visão a longo prazo que tem em cibersegurança tendo em consideração aqueles que são os processos e serviços da empresa.

  A identificação do papel em segurança informática da empresa no seu meio empresarial e em termos nacionais também deve entrar nesta fase, visto que se percebem melhor as ligações que existem com outras organizações e também quais as contribuições em cibersegurança que a organização dá para o seu país. Porém, o aspeto fulcral aqui é entender a organização/estrutura interna da empresa, nomeadamente os seus vários setores/departamentos. Se se conhecer bem as funções de cada setor/departamento da organização e quais as responsabilidades atuais de cada um em cibersegurança, a definição das metas e objetivos a alcançar na estratégia será mais simples e completa, dado que se percebem bem quais são as abordagens atuais de risco e a necessidade de juntar a cibersegurança às prioridades de negócio.

  Assim, neste primeiro passo a organização determina onde quer aplicar a estratégia para orientar a melhoria das capacidades de cibersegurança da organização e definem-se também quais são as prioridades da estratégia e os pilares estratégicos de alto nível que devem guiar a definição das políticas que irão estar em vigor no plano de cibersegurança.

- **2.º Passo: Identificar os Recursos, Requisitos e Regulamentação no Âmbito da Estratégia**

  Após se definirem as prioridades e o âmbito da estratégia, deve-se identificar os ativos e sistemas inseridos no âmbito, bem como os requisitos regulamentares e referências informativas. Basicamente, é neste 2.º passo que se vai orientar ou identificar aquilo que será usado para a elaboração dos passos seguintes do *"roadmap"*. Ou seja, como já foi discutido na fase anterior qual o âmbito ("*scope*") da estratégia, agora deve-se olhar para aquilo que está no raio de ação, identificar tudo o que será necessário para, nos passos seguintes, perceber como a empresa se encontra atualmente em cibersegurança e quais as medidas atualmente aplicadas relativas a processos de cibersegurança.

  Deste modo, além dos ativos e sistemas, devem ser identificados os requisitos organizacionais e a regulamentação apropriada a ter em consideração na estratégia para que as medidas a serem tomadas cumpram com esses requisitos. Por outro lado, é necessário identificar os *standards*, *guidelines*, ferramentas e métodos usados ou considerados na gestão de cibersegurança e de risco da empresa, principalmente os que já estão documentados ou a ser aplicados pela organização.

- **3.º Passo: Avaliar a Situação Atual em Cibersegurança**

  Nesta etapa, o que se pretende é ter uma noção sobre como a empresa se encontra atualmente em cibersegurança e o seu estado em gestão de riscos. Para isso, vai se usar a abordagem de autoavaliação do C2M2 para ser possível avaliar qual a situação atual em cibersegurança para o âmbito escolhido no passo 1.

  Algo que deve ser feito também é identificar o nível de implementação atual em gestão de riscos de cibersegurança segundo a NIST *Framework*, sendo muito útil para isso os resultados do questionário C2M2.

Além disso, para completar o "Perfil-Atual", é proposto que se usem os controlos da CIS v8.0, pelo que através do CIS CSAT será possível identificar o estado de implementação em que o âmbito em questão se encontra nos vários subcontrolos da CIS.

Assim, no final desta etapa deve ser possível obter um "Perfil-Atual" de implementação das práticas da NIST *Framework* e perceber quais partes estão bem implementadas e onde é que existem falhas.

- **4.º Passo: Efetuar Avaliações de Risco de Cibersegurança**

  No 4.º passo são feitas avaliações de risco de cibersegurança para a parte da organização que está no âmbito da estratégia com o intuito de identificar e avaliar quais os riscos de que é alvo e o que está fora das tolerâncias atuais de risco. De salientar que podem ser utilizadas informações de ameaças de cibersegurança internas e externas para perceber a probabilidade e o impacto da ocorrência de eventos de cibersegurança.

  Porém, dependendo da organização, pode já haver um programa de gestão de riscos através da existência de um departamento dedicado aos riscos corporativos, por exemplo. Neste caso, já deve ser uma prática regular da empresa abordar estes riscos e fazer estas avaliações, pelo que os registos e informações necessárias para esta fase podem já existir.

  Relativamente às tolerâncias de risco, devem ser tidos em conta, além da estratégia de gestão de riscos, os *outputs* sobre requisitos ou normas identificados no passo 2 da estratégia. Assim, no final deste passo deve existir um relatório de avaliação de risco para o âmbito da estratégia que será fundamental para definição do perfil desejado no passo 5.

- **5.º Passo: Definir/Criar uma Avaliação Alvo**

  A definição do perfil desejado ou alvo em cibersegurança é feita nesta etapa, sendo uma parte vital para a elaboração ou reestruturação do plano de cibersegurança. Deste modo, a organização que estiver a usar esta estratégia deve pegar na avaliação efetuada no passo 3 e descrever que resultados de cibersegurança pretende ver implementados.

  Todavia, a criação do perfil desejado deve ser feita de uma forma cautelosa e racional, além de ser necessário determinar quais os riscos que podem ser aceites. Ou seja, devem ser percebidas as limitações que a organização tem para implementar certos controlos, seja em termos de negócio, recursos necessários e das prioridades estratégicas da empresa. Por exemplo, se a organização não puder implementar uma certa medida de segurança por causa do investimento envolvido, então o melhor é perceber qual o impacto da sua não implementação para perceber até que ponto é um risco tolerável ou procurar alternativas para mitigar esse risco. Desta forma, a implementação de todos os controlos de segurança ou o alcançar de níveis máximos de implementação de medidas de segurança geralmente não é o ideal para uma organização, visto que é necessário ter sempre em consideração todo o ambiente organizacional, tais como os requisitos organizacionais e regulamentares ou até os objetivos de negócio e de missão.

  Assim, é fundamental que o responsável (ou responsáveis) pela estratégia reúna com as partes executivas da organização com poder de decisão em matéria de cibersegurança para serem decididos os controlos certos para constarem no plano de cibersegurança (ou política, dependendo da vontade da organização). Podem-se ainda considerar influências e requisitos de partes interessadas externas, como entidades setoriais, clientes e parceiros de negócios. Relativamente aos controlos, devem ser observadas as referências informativas presentes nas subcategorias da NIST *Framework*, além dos controlos aconselhados da CIS versão 8.0. Porém, aconselha-se vivamente a selecionar um perfil de destino apropriado na autoavaliação do C2M2.

Todas as razões e análises efetuadas para decidir que certos controlos ou práticas não devem estar no plano devem ficar documentadas num relatório.

No fim deste passo, já será possível ter o "Plano de Cibersegurança" concluído, que pode passar a ser a "Política de Cibersegurança da Empresa" que o usar. Neste documento devem constar os pilares estratégicos definidos no passo 1, os requisitos organizacionais e regulamentares desta área, as responsabilidades de cada área da empresa em cibersegurança e, o mais importante, os controlos/práticas de cibersegurança selecionados neste passo para atingir o "Perfil-Alvo".

- **6.º Passo: Criar um Plano de Ação Priorizado para Combater as Lacunas**

  Após a definição do perfil desejado em cibersegurança, nesta fase pretende-se definir um plano de ação para colmatar as lacunas que existem entre as atuais práticas implementadas pela empresa e as práticas que constam no "Plano de Cibersegurança". Ou seja, neste plano de ação não irão estar todos os controlos, pois alguns já estão implementados, mas apenas os controlos que não estão implementados e fazem parte do "Plano (ou Política) de Cibersegurança".

  Deste modo, a organização compara o "Perfil-Atual" e o "Perfil-Alvo" para determinar as lacunas/falhas e identificar as consequências da existência dessas lacunas ("*gap analysis*"). Depois disso, a empresa deve priorizar, com base nas consequências das lacunas, as ações necessárias para implementar totalmente as práticas da "Política de Cibersegurança" que permitem a obtenção da capacidade desejada nos vários domínios específicos. Nesta parte, deve ser efetuada uma análise custo-benefício (CBA [1]) para cumprir com as medidas presentes na "Política de Cibersegurança", visto que existem muitas opções diferentes para implementar a mesma medida, seja pela variedade de recursos ou ferramentas existentes no mercado, seja pela forma como se vai abordar as medidas.

  No final deste passo é elaborado um plano de ação para abordar/resolver as lacunas selecionadas, sendo necessário determinar todos os recursos, incluindo financiamento e recursos humanos, necessários para resolver as lacunas. Deve ser também identificado um indivíduo com autoridade suficiente para executar o plano e designá-lo como o "dono do plano". Este terá a obrigação de garantir o progresso da implementação das várias ações para as medidas assinaladas como lacunas.

- **7.º Passo: Implementar/Aplicar o Plano de Ação**

  Por último, é necessário dar início à implementação das medidas que estão no plano de ação priorizado para eliminar as lacunas que existem entre a avaliação atual e a avaliação desejada. Como existem medidas mais urgentes que outras, tem de se dar início primeiro à implementação dessas.

  Deve-se também monitorizar o progresso através das KPIs definidas ou de atualizações iterativas da avaliação atual, comparando-a posteriormente com a desejada, para garantir que o progresso desejado seja alcançado.

  Por fim, é fundamental dizer que uma organização deve reavaliar de forma periódica o estado em cibersegurança, ou seja, voltar a iterar a estratégia de cibersegurança. Além disso, é normal que certos pontos não fiquem completamente definidos à primeira, mas com o decorrer do processo as bases irão ficar mais refinadas e sólidas, sendo possível chegar-se a um plano (ou política) de cibersegurança capaz de reforçar a cibersegurança conforme as necessidades da empresa. Por exemplo, a empresa pode pensar que necessita de repetir mais vezes o passo 1 ("Definir as prioridades e o âmbito da estratégia") para ter melhor conhe-

1 CBA significa *"cost-benefit analysis"* (análise custo-benefício)

cimento da situação da empresa e para aperfeiçoar ainda mais as prioridades da estratégia, o que pode originar uma melhor qualidade das avaliações de cibersegurança e de risco.

4.3.1 *Passo 1: Definir as prioridades e o âmbito da estratégia*

Definir as Prioridades e o Âmbito da Estratégia (1.º Passo)		
Inputs	***Outputs***	**Iniciativas**
• Estratégia atual de Gestão de Riscos • Objetivos/Missão de negócio • Prioridades organizacionais • Informação de Ameaças • Contextualização do meio empresarial envolvente • Estrutura/Organograma da empresa (áreas/departamentos/setores, responsabilidades, etc.)	• Objetivo e âmbito de aplicação da estratégia • *"Function List"* • Prioridades alto-nível para a estratégia de cibersegurança (metas/objetivos) • Pilares Estratégicos do "Plano de Cibersegurança" • Responsabilidades alto-nível de cada colaborador/parceiro em cibersegurança na empresa, caso seja efetuado	• Decisão do âmbito da Estratégia. • Criação de uma *"Function List"* com todos os subconjuntos (ou áreas da organização) aos quais irá ser aplicada a Estratégia de cibersegurança. • (Re)Definição das prioridades alto-nível da estratégia de cibersegurança da organização (metas/objetivos). • (Re)Definição dos pilares estratégicos do "Plano de Cibersegurança", ou seja, as áreas com relação à cibersegurança que se pretendem reforçar ou dar destaque e que promovem as prioridades da estratégia. • Criação de uma lista de responsabilidades e deveres de alto-nível em cibersegurança para cada colaborador/parceiro tendo em conta a sua área, setor ou departamento (opcional).

Tabela 20: Resumo dos tópicos abordados no passo 1 da Estratégia de Cibersegurança

Como se pode observar pela Tabela 20, os principais resultados deste passo são a definição da "*Function List*" e a definição das prioridades alto-nível da estratégia e dos pilares do "Plano de Cibersegurança". De certo modo, é por aqui que se começa a delinear o plano de cibersegurança, pelo que é por isso que a estratégia proposta começa com a definição do âmbito de aplicação e a definição das prioridades a serem abrangidas pelo plano.

Primeiro, aquilo que quem está encarregue de desenvolver a estratégia numa organização ("facilitador(es)") deve fazer é recolher as informações necessárias para conseguir definir o âmbito da estratégia, as prioridades estratégicas e os pilares estratégicos do plano. Algumas das informações úteis para estes propósitos são:

- **Estratégia atual de gestão de riscos da empresa**, caso exista, que ajuda a perceber como a empresa lida com os riscos, que objetivos são abordados ou até que tipo de riscos a organização enfrenta e quais os mais preocupantes. Conhecendo isto, é mais fácil definir quais áreas deveriam ser abordadas em primeiro lugar e quais deveriam ser as prioridades da estratégia a criar ou reformular;
- **Informação de ameaças para a empresa**, caso exista, sendo um grande apoio para perceber que áreas devem ser reforçadas primeiro em cibersegurança;
- **Objetivos/missão de negócio**, ou seja, quais os principais objetivos que a organização tem definidos para a sobrevivência do negócio. Neste caso, esta informação é útil porque ajuda a perceber quais as áreas mais críticas e que processos é que são feitos na empresa, o que é fundamental para definir o âmbito e as prioridades;
- **Contextualização do meio empresarial envolvente**, útil para entender os processos empresariais atuais e as ligações que existem com outras organizações externas. Perceber, nem que seja de forma não muito pormenorizada, o funcionamento dos processos internos e externos à empresa dá a capacidade a quem está encarregue de desenvolver este *"roadmap"* de tomar melhores decisões neste passo;
- **Estrutura/Organograma da empresa**, muito útil para perceber as responsabilidades de cada departamento na organização e quais as áreas que poderão estar abrangidas pela estratégia.

Começando pelo âmbito ou objetivo da estratégia, deve ser escolhido quais partes ou áreas é que vão ser alvo de avaliação em cibersegurança. É claro que o ideal é toda a organização estar no âmbito da estratégia e isso pode e deve acontecer em duas situações: ou a empresa é pequena e não possuí muitas áreas distintas, ou então no passado a empresa já usou esta estratégia ou outra semelhante e, desta forma, já tem um conjunto de documentação para suportar este passo. Outro cenário possível seria pegar nesta estratégia e aplicá-la em simultâneo para áreas distintas, o que certamente iria necessitar de mais recursos e também iria gerar vários planos de cibersegurança distintos. Porém, para a maioria das empresas, o recomendável mesmo é que se defina um âmbito menor primeiro e depois numa nova iteração da estratégia ir alargando o *"scope"*.

Por exemplo, numa primeira vez o âmbito decidido poderia ser só a área de administração de sistemas de IT da empresa. Neste caso, só se iriam avaliar os processos dos administradores dos sistemas de tecnologia da informação, ou seja, os sistemas ou ativos que estes coordenam ou gerem, as comunicações existentes com outros colaboradores, os métodos de operação ou estratégias de trabalho que usam, que tipo de monitorização utilizam, quais os métodos de gestão de incidentes, entre outros processos que estejam a cargo deles ou que deveriam estar sob a sua tutela.

Mas em vez desta abordagem, a empresa pode possuir um organograma ou estrutura que possibilite uma separação por áreas ou departamentos. O mais comum é que uma média/grande empresa possua uma estrutura hierárquica com os vários setores distintos e uma atribuição de responsabilidades diferentes a cada, além de atribuições de responsáveis por cada setor. Desta forma, o processo de escolha do âmbito da estratégia de cibersegurança pode ser mais simples, visto que se pode analisar só um subconjunto de departamentos da organização primeiro e posteriormente começar a incluir mais departamentos no âmbito, o que fará com que mais setores estejam abrangidos pelo "Plano de Cibersegurança". Por exemplo, uma determinada organização pode decidir que quer primeiro incluir na estratégia o departamento de sistemas de informação, o de gestão de riscos, o de recursos humanos e o de segurança da informação. Neste caso, o âmbito restringe-se aos processos destes setores, pelo que um ponto de partida interessante seria falar com os responsáveis de cada departamento para delinear os próximos passos a serem feitos e obter as informações necessárias.

Numa estratégia de cibersegurança empresarial claro que o mais importante são os processos internos da organização, porém existem outros aspetos que podem e devem entrar no âmbito da estratégia. Um exemplo disso é a cadeia de fornecimento da empresa ou os parceiros externos que, apesar de não fazerem parte da organização, são uma parte fulcral da empresa e podem constituir um grande risco. Resumindo, todas as ligações internas e externas da empresa que podem constituir perigo em cibersegurança para a organização devem estar a ser consideradas nesta fase como potenciais alvos de uma nova iteração da estratégia.

Esta informação do âmbito irá constar na denominada "*Function List*" ("Lista de funções"), como é explicado no "*Implementation Guidance*" do C2M2 [23]. Uma função, neste caso, refere-se a um conjunto de operações no âmbito que são avaliadas pela estratégia. Deste modo, uma função poderia ser uma linha de negócios, uma zona de segurança de rede ou uma única instalação, dependendo da abordagem a utilizar para definir o âmbito. Assim, uma "*Function List*" contém todas as funções que irão ser alvo de avaliação, podendo dizer-se que o âmbito da estratégia é tudo o que irá estar nessa listagem.

Após definida a "*Function List*" (âmbito), o que se deve fazer é definir (ou redefinir) as prioridades alto-nível da estratégia de cibersegurança, i.e. quais os objetivos ou metas que a estratégia de cibersegurança deve cumprir e alcançar. Para efetuar uma lista de metas e objetivos, devem-se escolher objetivos que apoiem o alcance e a melhoria contínua de uma postura de cibersegurança adequada e apoiem a realização da missão do negócio. As prioridades devem ser de alto-nível para que não se esteja a abordar assuntos demasiado aprofundados da

cibersegurança já nesta fase. Isto porque aquilo que se planeia estabelecer são metas/objetivos necessários a atingir, mas, em simultâneo, também sejam de fácil entendimento e façam com que todas as pessoas percebam a necessidade de se implementar a estratégia na organização.

Desta forma, a empresa deve conseguir definir quais as metas alto-nível a alcançar primeiro e depois, em cada meta, definir quais os objetivos relacionados a cumprir. Para isso, as metas/objetivos da estratégia de cibersegurança devem dar resposta a perguntas como:

- As metas e objetivos suportam a melhoria da capacidade de cibersegurança da empresa, incentivando a mudança das operações, tecnologias, processos e pessoas em torno da organização?
- As metas e objetivos estão em concordância com os objetivos e prioridades organizacionais da empresa?
- As metas e objetivos têm em consideração o ambiente ao redor da empresa e a evolução da tecnologia?
- As metas e objetivos estão atualizadas segundo a evolução das normas ou outras referências de cibersegurança publicadas por instituições, ou outras entidades de interesse em cibersegurança?
- As metas e objetivos são fáceis de perceber?
- As metas e objetivos estão de acordo com as políticas, requisitos e referências sobre cibersegurança?
- As metas e objetivos são úteis para a definição do plano/política de cibersegurança da empresa?
- As metas e objetivos refletem aspetos a serem cumpridos pela estratégia (quase) de forma intemporal?

Com base nas prioridades da estratégia, é possível a seguir começar a delinear a estrutura do "Plano de Cibersegurança", ou seja, definir quais os pilares do plano ou política de cibersegurança da empresa. Claro que, tal como as prioridades da estratégia, podem já existir pilares estratégicos no plano porque, ou já existe um plano efetuado, ou então já se está a efetuar uma nova iteração do *"roadmap"*. Deste modo, só é necessário perceber se houve alterações, por exemplo, nas prioridades estratégicas, que façam com que seja necessário alterar as principais bases ou áreas de atuação do plano de cibersegurança.

Essencialmente, os pilares estratégicos vão de encontro ou promovem as prioridades da estratégia de cibersegurança. O que deve acontecer é que, dependendo dos pilares estratégicos existentes, se definam áreas de cibersegurança distintas que serão as bases do plano. Como exemplo, se as prioridades tiverem muitas metas que se referem a incidentes de cibersegurança, sejam relacionadas, por exemplo, a respostas, recuperações ou impactos, então é natural que um dos pilares do plano seja algo relacionado a "Gestão de incidentes de cibersegurança". Organizando o plano desta forma garante que as medidas que irão constar no plano serão relacionadas às áreas da cibersegurança que são prioridades da estratégia, dando origem a um documento estruturado em capítulos, cada um com medidas associadas. Além disso, o documento fica organizado de forma simples, ficando evidenciados quais os passos que a empresa deve ter em conta para melhorar as suas capacidades de cibersegurança.

Por último, e aproveitando que para se definir o âmbito da estratégia foi necessário perceber a estrutura da organização, pode-se definir em alto-nível quais deveriam ser as responsabilidades de cibersegurança de cada departamento ou cargo na empresa, além dos parceiros. Esta é uma parte opcional, e a empresa pode já possuir documentação para o efeito, sendo só necessário recolhê-la e organizá-la no que à cibersegurança diz respeito. Porém, pode ajudar para o passo 5 ter já essa informação, visto que lá é que se vão redefinir com base na definição do "Perfil-alvo" as novas responsabilidades de cada colaborador e parceiro, tendo em conta a sua função ou cargo na empresa. Na verdade, todos os colaboradores e parceiros externos possuem responsabilidades em cibersegurança,

pelo que se deve definir responsabilidades para todas as pessoas, tendo em conta claro que elas variam consoante a posição ou cargo que ocupam. Todavia, existem várias empresas que não possuem nenhum organograma oficial para distinguir as funções de cada posto, mas mesmo nesses casos devem ser discutidas as responsabilidades de cada um para que todos percebam bem a importância de adotarem medidas para salvaguardar a cibersegurança. Assim, será possível que o "Plano de Cibersegurança" contenha as responsabilidades de cibersegurança para todos os cargos ou funções que fazem parte do âmbito da estratégia.

4.3.2 *Passo 2: Identificar os recursos, requisitos e regulamentação no âmbito da estratégia*

Identificar os Recursos, Requisitos e Regulamentação no Âmbito da Estratégia (2.º Passo)		
Inputs	***Outputs***	**Iniciativas**
• Estratégia atual de Gestão de Riscos • Objetivo e âmbito de uso da estratégia (*"Function List"*) • Prioridades de alto-nível (Pilares Estratégicos) • Inventário de sistemas e ativos da empresa, caso exista • Mapas/Arquiteturas das redes da organização, caso existam • Documentos com requisitos ou referências aplicáveis à empresa, caso existam	• Lista dos sistemas e ativos inseridos no âmbito da estratégia • Mapa/Arquitetura de rede com os sistemas e ativos mais relevantes inseridos no âmbito da estratégia • Lista dos requisitos de cibersegurança (regulamentares e organizacionais) e os de negócio inseridos no âmbito da estratégia • Lista de referências (*standards*, ferramentas, métodos, guias de cibersegurança e gestão de riscos, etc.) inseridas no âmbito da estratégia	• Identificação dos ativos e sistemas (por exemplo, pessoas, informações, tecnologia e instalações) que estão inseridos no âmbito da estratégia. • Criar/Rever o mapa ou arquitetura das redes inseridas no âmbito da estratégia, tendo por base o inventário de sistemas e ativos. • Identificação dos requisitos de cibersegurança regulamentares e organizacionais (por exemplo, leis, regulamentação, certificação, políticas, etc.) e os de negócio (por exemplo, restrições/ limitações da empresa) que estão inseridos no âmbito da estratégia. • Identificação das referências informativas (por exemplo, normas, ferramentas, *frameworks*, boas práticas de cibersegurança e gestão de riscos, etc.) que estão inseridas no âmbito da estratégia.

Tabela 21: Resumo dos tópicos abordados no passo 2 da Estratégia de Cibersegurança

Após definido o âmbito e as prioridades, é preciso orientar ou identificar necessidades para os próximos passos que se irão seguir na estratégia. Como se pode observar na Tabela 21, os resultados deste passo são sobretudo a identificação dos ativos e sistemas, dos requisitos de cibersegurança e das referências inseridas no âmbito. A relevância deste passo prende-se com o facto dos passos seguintes (passos 3, 4 e 5) das avaliações (*"assessments"*) necessitarem das informações aqui recolhidas.

Deve-se começar por fazer uma lista dos sistemas e ativos (físicos e digitais) inseridos no âmbito da estratégia e podem impactar negativamente a organização em caso de incidente de cibersegurança. Ou seja, deve-se percorrer a *"Function List"* e perceber que categorias de ativos e sistemas é que estão associados a cada função. Algo que pode ser útil é a empresa possuir um inventário de ativos, já que pode ajudar a perceber que categorias de ativos estão no âmbito. Este passo não consiste propriamente na inventariação dos ativos e sistemas da organização, mas sim na sua identificação para posteriormente se poder usar esta informação tanto para as avaliações, mas principalmente para o passo 4 de análise de riscos. Contudo, o inventário é algo muito importante numa organização, mesmo para perceber a relevância de cada ativo, pelo que se incentiva a que este esteja construído. Desta forma, neste passo pode-se aproveitar para criar, caso não exista, um inventário com todos os ativos e sistemas que estão no âmbito da estratégia. Caso se opte por construir um inventário, então a lista de sistemas e ativos inseridos no âmbito da estratégia será o próprio inventário.

Porém, uma recomendação para que o processo se torne mais simples é identificar primeiro os ativos e sistemas mais críticos ou prioritários e só depois os menos críticos. Pode-se até chegar a esta fase e chegar-se à conclusão que o âmbito definido no passo 1 é muito "grande", ou seja, que estão muitos ativos no âmbito e não existe capacidade para continuar com eficácia os próximos passos. Nestes casos, o que se deve fazer é mesmo regressar

ao passo 1 e reduzir o âmbito, porém nunca se deve considerar analisar só uma porção dos ativos no âmbito, uma vez que tornará o "Plano/Política de Cibersegurança" incompleto e sem rigor. Por exemplo, uma empresa pode ter implementado controlos de cibersegurança mais avançados para os ativos críticos do que para os menos críticos, o que fará com que essas lacunas não sejam detetadas, caso neste passo 2 não se identifiquem os ativos menos críticos. Isto levará a uma falsa noção de segurança, ou seja, levará a que se pense que os controlos de cibersegurança estão aplicados para todos os ativos do âmbito.

Como forma de exemplo, na Figura 7 pode-se observar uma forma de estruturar a identificação de ativos para o caso específico dos ativos que suportam o trabalho de uma unidade de IT [1].

Category	Type of Asset	Code	Details
Main	Business Process	A1, A2, A3, A4, A5, A6, A7, A8	LMS, Cloud, Zimbra, Form, Chat, Library, SION Lab, SIAP
	Information	A9, A10, A11, A12	SPMB Participant Data, Student Data, Section and Work Unit Data, Email
Supporting	Hardware	A13, A14, A15, A16, A17	Server, Switch, Router, UPS, PC
	Software	A18, A19, A20	ESXi, Proxmox, Windows
	Human Resource	A21, A22, A23, A24	Network Administrator, System Administrator, Data Administrator, Person in charge of operational standards and procedures

Figura 7: Exemplo de como se pode efetuar a identificação de ativos [1]

Além de identificar os ativos e sistemas, algo muito útil principalmente para o passo 4 (secção 4.3.4) é ter um mapa ou diagrama de arquitetura das redes da organização, ou então daquilo que faz parte do âmbito da estratégia. Deste modo, neste passo deve-se construir ou rever a arquitetura da rede, uma vez que sem ela é mais difícil analisar que riscos de cibersegurança podem surgir devido à forma como a rede está organizada, tendo em conta principalmente os pontos de entrada e saída de tráfego para a Internet exterior à organização. Na verdade, um atacante que queira afetar os sistemas internos de uma organização normalmente precisa de aceder do exterior da rede interna da organização. Assim, é importante que a arquitetura contenha a indicação sobre onde se situam ativos como *firewalls*, *switches*, *routers*, servidores (base de dados, email, *backend*/*frontend*, *logs*, etc.), entre outros equipamentos relevantes e com acesso à rede. Além disso, deve conter informações sobre os diferentes sistemas e de que forma é que eles comunicam, tendo em conta também onde é que muda o nível de "confiança" (*"trust boundaries"*).

Neste passo também é importante perceber quais os requisitos regulamentares e organizacionais de cibersegurança que se aplicam ao âmbito da estratégia, tendo em conta também os requisitos de negócio da empresa. Aqui o importante é recolher todas as obrigações que a estratégia deve ter em conta na altura de tomar decisões no passo

5, além de ser útil também para as avaliações do próximo passo. Alguns exemplos de requisitos que poderão ser listados nesta fase são:

- Leis (Lei n.º 46/2018 — Regime Jurídico de Segurança do Ciberespaço [17], Lei n.º 58/2019 [30], etc.) e regulamentos nacionais e europeus (Regulamento n.º 183/2022 [33], Regulamento (UE) 2016/679 [22], etc.);
- Requisitos e regulamentos internos da empresa, como políticas ou instruções técnicas (documentação interna), requisitos setoriais, requisitos normativos e requisitos de negócio;
- Níveis de serviço (SLA) estabelecidos com os clientes, úteis para a análise do impacto dos riscos e para perceber as prioridades de negócio;
- Limitações/restrições da organização, importante para a priorização de ações e tomada de decisão sobre medidas e ações no âmbito da cibersegurança.

Por último, é útil que se identifique as referências informativas sobre cibersegurança mais pertinentes neste âmbito, tais como *standards*, ferramentas, métodos, *guidelines*, entre outras. Para isso deve-se começar por identificar as referências que estão a ser seguidas pela organização sobre cibersegurança e gestão de riscos de cibersegurança. As referências sobre segurança da informação também podem ser úteis, mas o fundamental é conseguir perceber quais são seguidas e até que ponto são seguidas normas, ferramentas ou outros recursos de cibersegurança publicados por organismos normativos, ou por outros organismos internacionais de segurança. Por exemplo, podem estar a ser usadas ferramentas que ajudam a perceber as vulnerabilidades publicadas mais recentes e que se inserem na *framework* OSINT [97].

Além das que são já aplicadas, devem ser consideradas outras referências que o dono ou encarregado da estratégia considere que possam ser incluídas na lista. O objetivo é que esta informação possa ajudar a tomar as melhores decisões nos próximos passos através de aplicação das recomendações que estas referências têm, além de poderem ser úteis na altura de definir um estado desejado e de criar o plano de ação. De referir que a própria NIST *Framework* já apresenta um vasto conjunto de apontadores para referências informativas e que cobrem um grande conjunto de matérias relacionadas à cibersegurança. Geralmente, esta estratégia de cibersegurança já refere um grande conjunto de referências que tocam em um pouco de tudo aquilo que se deve considerar, porém, se existirem outras referências já seguidas, não significa que estas tenham de deixar de ser usadas. O importante é perceber o que é mais relevante para a empresa em causa, lembrando que muitas das referências atualmente seguidas por uma organização podem já não estar atualizadas, tendo em conta o ambiente de rápida evolução e mudança inerente à cibersegurança.

Como nota final, é importante referir que a estratégia de gestão de riscos atual da empresa pode já ter muitas destas informações, seja sobre os ativos e sistemas, seja sobre os requisitos e referências. Além disso, é natural que com o tempo a empresa vá tendo já estas informações acumuladas, caso esta vá aplicando esta estratégia regularmente, o que torna esta fase mais rápida, sendo só necessário verificar novas informações mais atualizadas que possam entrar e outras que já não sejam necessárias constar nas listagens.

4.3.3 *Passo 3: Avaliar a Situação Atual da Cibersegurança*

No 3.º passo, o principal objetivo é o de avaliar o estado atual da empresa em cibersegurança, como mostra a Tabela 22. Esta é uma parte fundamental para perceber em que ponto a empresa se encontra e serve de base para definir no passo 5 um estado para onde planeia evoluir, o que certamente irá despoletar um conjunto de medidas para

Avaliar a Situação Atual da Cibersegurança (3.º Passo)		
Inputs	***Outputs***	**Iniciativas**
• Objetivo e âmbito de aplicação da estratégia (*"Function List"*) • Prioridades (metas/objetivos) da estratégia • Lista dos sistemas e ativos inseridos no âmbito da estratégia • Lista dos requisitos de cibersegurança (regulamentares e organizacionais) e os de negócio inseridos no âmbito da estratégia • Lista de referências (*standards*, ferramentas, métodos, guias de cibersegurança e gestão de riscos, etc.) inseridas no âmbito da estratégia • Abordagem de autoavaliação C2M2 • Mapeamento dos níveis de implementação da NIST *Framework* para as práticas do C2M2 • Ferramenta de avaliação dos CIS *Controls* v8.0 (CIS CSAT)	• Perfil Atual da empresa em cibersegurança • Relatório do C2M2 com o resultado da avaliação atual • Nível de Implementação atual na NIST *Framework* • Estado em implementação das práticas do CIS *Controls* v8.0 (Relatório CIS CSAT)	• Conduzir um *"workshop"* de autoavaliação C2M2 com participantes apropriados (responsáveis pelas áreas, executivos, administradores, etc.). • Identificar, com base no relatório do C2M2 e no mapeamento para os níveis de implementação da NIST *Framework*, qual o nível de implementação das práticas da NIST *Framework* para gestão de riscos. • Identificar quais os subcontrolos do CIS *Controls* v8.0 que a empresa tem implementados atualmente (uso da ferramenta CIS CSAT), sendo que deve ser acordado qual o limite em que um subcontrolo é considerado lacuna (caso se considere aceitável, pode-se usar como base um *score* inferior a 50%).

Tabela 22: Resumo dos tópicos abordados no passo 3 da Estratégia de Cibersegurança

o alcançar. Esta fase fará sem dúvida os responsáveis pelas várias áreas envolvidas refletirem em questões de cibersegurança.

Em primeiro lugar, deve-se realizar a autoavaliação em cibersegurança usando o C2M2 (secção 2.6). Para isso utiliza-se a ferramenta disponibilizada pelo C2M2 [27] que pode ser usada tanto no formato "*online*" como em formato PDF, o que neste último caso necessita de ser pedido por correio eletrónico. A ferramenta é bastante fácil de usar e permite que seja guardado o estado ou as perguntas respondidas até ao momento (em formato JSON, que pode ser exportado e importado para a ferramenta), assim como gerar um relatório final em PDF com uma análise automática às respostas dadas durante a avaliação. É recomendável que se envie um email para o C2M2 a pedir a ferramenta, visto que estes fornecem um conjunto de recursos extra e, além disso, a ferramenta em PDF é mais cómoda para usar.

Após possuir a ferramenta, pode-se dar início a um *"workshop"* com os representantes individuais das funções que constam na *"Function List"*, sendo que algumas dicas para facilitar o processo podem ser observadas no *"Facilitator Guide"* do C2M2 [24]. O recomendável é marcar um dia para efetuar as perguntas a todos os responsáveis pelas áreas em análise e fazer com que cada um responda ao que lhe é destinado, sendo que deve estar também presente o responsável pela implementação da estratégia, para dar ajuda caso seja necessário. O ideal seria o questionário ficar respondido no mesmo dia, mas como são muitas perguntas é natural que não fique logo tudo respondido. Contudo, o fundamental é mesmo garantir que as respostas sejam coerentes com a situação atual.

Ao responder às práticas do C2M2, podem ser dadas as respostas: *"Fully Implemented"* (Completa), *"Largely Implemented"* (Completa, mas existem formas reconhecidas de a melhorar), *"Partially Implemented"* (Incompleta, mas existem várias formas de melhoria) e *"Not Implemented"* (Ausente, a prática não é realizada pela organização). Para efetuar o *"workshop"*, existem duas abordagens que podem ser seguidas:

- Nesta primeira abordagem, aquilo que se espera é que cada um dos representantes responda às perguntas individualmente. Ou seja, são distribuídas as perguntas aos representantes por domínio ou objetivo do C2M2 e cada um responderá aquilo que é da sua competência na empresa. Os responsáveis podem responder às suas perguntas sozinhos, deixando os devidos comentários em cada pergunta para ajudar a complementar as respostas, ou então podem responder em conjunto com o responsável pela estratégia, o que faz com que qualquer dúvida que surja possa ser colocada na hora, além de garantir maior supervisão sobre o que se faz. Esta abordagem é útil para cenários onde não é possível reunir todos os responsáveis num dia só, ou então existe uma separação tal de funções entre eles que não faz sentido todos juntos debaterem as respostas. A grande vantagem desta abordagem é a maior rapidez e simplicidade para os representantes das várias funções em análise. Porém, a desvantagem é que obrigará a um trabalho de divisão em domínios ou

em objetivos por parte do responsável pela estratégia, sendo que esta divisão pode até nem ficar bem-feita, o que trará falhas ou problemas em concluir o questionário. Na primeira vez em que usar a estratégia de cibersegurança, esta pode não ser a melhor abordagem porque ainda pode não haver o conhecimento total das responsabilidades de cada representante e também não há experiência anterior que faça com que já se saiba bem como dividir o questionário em partes.

- Na outra abordagem reúnem-se todos os representantes e, em conjunto, debatem as repostas às perguntas. Ou seja, o responsável pela estratégia reúne todos os representantes num dia, através da marcação de uma reunião com um certo tempo de antecedência para que todos possam estar presentes, e coordena a elaboração do questionário. Na reunião, o responsável pela estratégia lê as perguntas aos representantes e estes debatem e tentam chegar a um consenso sobre qual a resposta mais indicada, sendo que o responsável pela estratégia deve escrever nos comentários notas importantes para não se esquecer do que os representantes dizem. O ideal é que se possua um quadro ou algo similar para projetar as perguntas e os representantes assistirem ao progresso, além de poderem ler as questões por eles próprios. A vantagem disto é que as respostas ficam anotadas e respondidas com consenso entre todos, aumentando a precisão das respostas. A desvantagem é que se pode tornar um processo lento e a reunião demorar muito tempo, uma vez que são muitas perguntas. Isto resolve-se com a marcação de mais reuniões, pelo que é importante que esta abordagem seja bem planeada logo de início para prever estas situações.

Após o questionário ser concluído, pode-se gerar o relatório com o resultado do *"workshop"*. As informações que se podem encontrar no relatório são:

- Respostas dadas às práticas ou perguntas do C2M2, tanto em formato escrito como gráfico;
- Comentários/Notas deixados para complementar as respostas e ajudarem na análise que será feita posteriormente;
- Resumo de como está estruturado o C2M2;
- Resumo dos resultados, nomeadamente os resultados por domínio, onde é dito em que nível de maturidade (MIL) se está em cada domínio;
- Sumário com as lacunas identificadas (todas as práticas respondidas com *"Partially Implemented"* e *"Not Implemented"*).

Através da análise deste relatório é possível perceber em que nível a organização se encontra em cibersegurança, assim como é possível observar as respostas por domínio às perguntas de forma detalhada e os comentários deixados, além de serem ainda apresentadas as lacunas. Este documento gerado é fundamental para os próximos passos, pois contém toda a informação do estado atual em cibersegurança da empresa, pelo que deve ser tratado como informação confidencial.

Este relatório pode também ser usado ainda para identificar qual o nível de implementação conforme a NIST *Framework* (secção 2.5.3). Apesar de o C2M2 já ter um domínio dedicado à gestão de riscos, saber qual o nível de implementação é útil para avaliar o progresso em relação aos recursos de gestão de riscos de cibersegurança recomendados pela NIST *Framework*. Para saber o nível de implementação, pode-se usar os resultados da autoavaliação efetuada, principalmente os do domínio *"Risk Management"*, e efetuar o mapeamento para a NIST *Framework* [23].

Este processo de mapeamento das práticas do C2M2 para níveis de implementação da estrutura está feito no *"Implementation Guidance"* do C2M2 [23], porém, até à data, está só elaborado para a versão 1.1 do C2M2, que não é a usada nesta estratégia (versão 2). Para lidar com esta situação, é apresentada nesta dissertação um novo mapeamento de autoria própria que visa servir para o efeito de determinação do nível de implementação da estrutura, como se pode observar nas tabelas seguintes referenciadas pela Figura 8.

Práticas C2M2 mapeadas para os níveis de implementação da NIST *Framework*					
Nível de Implementação da Estrutura	**Categoria do Nível**	**Características**	**Prática do C2M2**		
			MIL 1	**MIL 2**	**MIL 3**
Nível 1: Parcial (*"Partial"*)	Processo de Gestão de Riscos	As práticas organizacionais de gestão de riscos de cibersegurança não estão formalizadas e os riscos são geridos de forma ad-hoc e às vezes reativa.	THREAT-1c RISK-1a RISK-2a RISK-3a RISK-4a		
		A priorização de atividades de cibersegurança pode não ser informada diretamente pelos objetivos de risco organizacional, pelo ambiente de ameaças ou pelos requisitos de negócios/missão.	ASSET-1a ASSET-2a THREAT-1d THREAT-2c RISK-1a RISK-2a RISK-3a RISK-4a		
	Programa Integrado de Gestão de Riscos	Há uma consciência limitada do risco de cibersegurança no nível organizacional e uma abordagem em toda a organização para gerir o risco de cibersegurança não foi estabelecida.	THREAT-2b RISK-1a RISK-2a RISK-4a		
		A organização implementa a gestão de riscos de cibersegurança de forma irregular, caso a caso, devido à variada experiência ou informações obtidas de fontes externas.	THREAT-1a THREAT-1b THREAT-2a RISK-1a RISK-2a RISK-4a		
		A organização pode não ter processos que permitam que as informações de cibersegurança sejam partilhadas dentro da organização.	THREAT-2a RISK-1a RISK-2a RISK-4a		
	Participação Externa	Uma organização pode não ter os processos implementados para participar na coordenação ou colaboração com outras entidades.	RISK-1a RISK-2a RISK-4a		

Práticas C2M2 mapeadas para os níveis de implementação da NIST *Framework*					
Nível de Implementação da Estrutura	**Categoria do Nível**	**Características**	**Prática do C2M2**		
			MIL 1	**MIL 2**	**MIL 3**
Nível 2: Risco Informado (*"Risk Informed"*)	Processo de Gestão de Riscos	As práticas de gestão de risco são aprovadas pela administração, mas podem não ser estabelecidas como política organizacional.		RISK-5a RISK-5b	
		A priorização das atividades de cibersegurança é informada diretamente pelos objetivos de risco organizacional, pelo ambiente de ameaças ou pelos requisitos de negócio/missão.		ASSET-1c ASSET-1d ASSET-1e ASSET-2c ASSET-2d ASSET-2e RISK-3b RISK-3c RISK-3d RISK-4b THIRD-PARTIES-1c THIRD-PARTIES-1d PROGRAM-1c	
	Programa Integrado de Gestão de Riscos	Existe uma consciência do risco de cibersegurança no nível organizacional, mas uma abordagem em toda a organização para gerir o risco de cibersegurança não foi estabelecida.		RISK-1b RISK-2b RISK-4b	
		Risco informado, processos de gestão aprovados e procedimentos estão definidos e implementados, e a equipa tem recursos adequados para desempenhar as suas funções de cibersegurança.	THIRD-PARTIES-2a THIRD-PARTIES-2b PROGRAM-2a PROGRAM-2b	RISK-2c RISK-5a RISK-5b THIRD-PARTIES-2c THIRD-PARTIES-2d	
		As informações de cibersegurança são partilhadas dentro da organização numa base informativa.		RISK-1c SITUATION-3a SITUATION-3c	
	Participação Externa	A organização conhece o seu papel num ecossistema maior, mas não formalizou a sua capacidade de interagir e partilhar informações externamente.	THIRD-PARTIES-1a	PROGRAM-1c	

Práticas C2M2 mapeadas para os níveis de implementação da NIST *Framework*					
Nível de Implementação da Estrutura	**Categoria do Nível**	**Características**	**Prática do C2M2**		
			MIL 1	**MIL 2**	**MIL 3**
Nível 3: Reproduzível (*"Repeatable"*)	Processo de Gestão de Riscos	As práticas de gestão de riscos da organização são formalmente aprovadas e expressas como política.			RISK-5c
		As práticas de cibersegurança organizacional são atualizadas regularmente com base na aplicação de processos de gestão de riscos para mudanças nos requisitos de negócio/missão e no cenário de ameaças e tecnologia em constante mudança.		RISK-2g	RISK-1e RISK-2h RISK-2i RISK-2j RISK-4c RESPONSE-1e THIRD-PARTIES-1e PROGRAM-1h
	Programa Integrado de Gestão de Riscos	Existe uma abordagem em toda a organização para gerir o risco de cibersegurança.	PROGRAM-1a	RISK-2d RISK-3e	RISK-1e RISK-1f RISK-4d RISK-5e
		Políticas, processos e procedimentos informados sobre riscos são definidos, implementados conforme pretendido e revistos.		THREAT-2d THREAT-2e RISK-1d RISK-2e RISK-3f THIRD-PARTIES-2f WORKFORCE-1d	RISK-4e RISK-5c WORKFORCE-1e PROGRAM-2i PROGRAM-3c
		O pessoal possui o conhecimento e as habilidades para desempenhar as suas funções e responsabilidades designadas	WORKFORCE-2b	RISK-2f THIRD-PARTIES-2g WORKFORCE-2c WORKFORCE-2d	ASSET-5d THREAT-3d RISK-5d ACCESS-4d SITUATION-4d RESPONSE-5d THIRD-PARTIES-3d WORKFORCE-5d ARCHITECTURE-6d PROGRAM-3d
	Participação Externa	A organização entende as suas dependências e parceiros e recebe informações desses parceiros que permitem a colaboração e as decisões de gestão baseadas em riscos dentro da organização em resposta a eventos.		THIRD-PARTIES-3a	RISK-2k

Práticas C2M2 mapeadas para os níveis de implementação da NIST *Framework*					
Nível de Implementação da Estrutura	Categoria do Nível	Características	Prática do C2M2		
			MIL 1	MIL 2	MIL 3
Nível 4: Adaptável ("*Adaptive*")	Processo de Gestão de Riscos	A organização adapta as suas práticas de cibersegurança com base em lições aprendidas e indicadores preditivos derivados de atividades de cibersegurança anteriores e atuais.		RESPONSE-3g	THREAT-1k THREAT-2i RESPONSE-1d RESPONSE-2i
		Através de um processo de melhoria contínua que incorpora tecnologias e práticas avançadas de cibersegurança, a organização adapta-se ativamente a um cenário de cibersegurança em constante mudança e responde a ameaças sofisticadas e em evolução em tempo hábil.			RISK-2l RISK-3g RISK-5f RESPONSE-3h
	Programa Integrado de Gestão de Riscos	Existe uma abordagem em toda a organização para gerir os riscos de cibersegurança que usa políticas, processos e procedimentos informados sobre riscos para abordar possíveis eventos de cibersegurança.		THREAT-1g THREAT-2f SITUATION-2f	THREAT-1k RISK-5c ACCESS-2i SITUATION-2i RESPONSE-2h RESPONSE-3k PROGRAM-2j
		A gestão de riscos de cibersegurança faz parte da cultura organizacional e evolui a partir da consciencialização das atividades anteriores, das informações partilhadas por outras fontes e da consciencialização contínua das atividades nos seus sistemas e redes.			ASSET-1f ASSET-1h ASSET-2f ASSET-2h WORKFORCE-4d WORKFORCE-4e SITUATION-3e SITUATION-3f SITUATION-3g
	Participação Externa	A organização gere os riscos e partilha ativamente informações com parceiros para garantir que informações precisas e atuais sejam distribuídas e consumidas para melhorar a cibersegurança antes que ocorra um evento de cibersegurança.		THREAT-2g RESPONSE-2g	RISK-2m RESPONSE-3i RESPONSE-3j PROGRAM-2l

Figura 8: Práticas do C2M2 mapeadas para os Níveis de Implementação da NIST *Framework* (autoria própria)

Assim, para saber em que nível de implementação a organização se encontra no âmbito da estratégia deve-se olhar para o relatório com as respostas finais da autoavaliação do C2M2 e relacioná-las com o mapeamento mostrado na Figura 8. Basicamente, para que a organização se encontre num determinado nível de implementação, aquilo que deve ser feito é verificar se as práticas do C2M2 que estão nesse nível e para trás deste (os níveis são "acumulativos") estão respondidas com "*Fully Implemented*" ou "*Largely Implemented*". Por exemplo, para uma organização dizer que está no nível 3 ("*Repeatable*"), esta tem de ter as práticas que aparecem de todas as MIL's nesse nível respondidas com "*Fully Implemented*" ou "*Largely Implemented*" e, além disso, tem de ter as dos níveis 1 e 2 também nestas condições. Desta forma, mesmo que só uma prática não esteja respondida desta forma, isso já faz com que a organização não possa estar nesse nível e se encontre no nível imediatamente anterior.

Por último, mas não menos importante, a tarefa que deve ser feita para a avaliação completa da situação atual em cibersegurança é a de identificar as práticas do CIS *Controls* versão 8 (secção 2.7) que a organização tem atualmente implementadas. Usar estes controlos é extremamente útil porque são uma visão diferente priorizada de ações a serem tomadas para reduzir os ciberataques mais comuns e os riscos de cibersegurança. Para essa avaliação, pode-se simplesmente percorrer os controlos apresentados nas tabelas da secção 2.7 e verificar aquilo que está implementado ou não, ou então usar uma abordagem mais sofisticada, completa, cómoda e automatizada através do uso da ferramenta CIS CSAT [36].

O CIS CSAT é uma aplicação *web* que permite às empresas acompanharem o progresso na implementação dos controlos e respetivos subcontrolos da CIS, tanto os da versão 7.1 como os da versão 8.0. É possível registar-se nesta aplicação criando um perfil e inserindo os dados pedidos, nomeadamente o nome da organização à qual se planeia conduzir as autoavaliações. A seguir é só criar uma avaliação nova (*"assessment"*) dando-lhe um nome e escolhendo fazer a avaliação com os controlos da versão 8 da CIS, as utilizadas nesta estratégia. Para este passo, deve-se também selecionar que se quer ver aplicados todos os grupos de implementação (IG's), visto que o objetivo é olhar para todos os controlos e perceber quais é que estão implementados atualmente. Mesmo que não seja a primeira vez a usar esta aplicação, e tenham sido feitas as reavaliações do passo 7 numa iteração anterior da estratégia, é importante que se olhe novamente para todas as práticas, pois pode já ter passado muito tempo desde a última vez que se fez um *"assessment"*.

Após criada uma avaliação para os CIS *Controls* v8.0 com os grupos 1, 2 e 3 selecionados como *"Applicable"*, será apresentada uma *Dashboard* com vários gráficos que ajudam na análise das respostas dadas em cada subcontrolo. Por exemplo, no gráfico *"Spider Web"* pode-se comparar a avaliação atual com a média da indústria. No separador *"Current Assessment"* pode-se encontrar outras formas de constatar o que está a ser feito na avaliação atual, nomeadamente ver todos os controlos em simultâneo e as várias opções de resposta, ver quais as tarefas atribuídas ao utilizador em questão, quais as respostas que necessitam de validação e um calendário com os prazos estabelecidos e alturas das alterações nas respostas a cada subcontrolo. Porém, o objetivo principal é percorrer cada um dos 18 controlos e preencher os respetivos subcontrolos com a informação pedida. De notar que em cada subcontrolo existe uma referência para outras *frameworks* e documentos de referência, nomeadamente a NIST *Framework* ("NIST CSF"), evidenciando ainda mais a compatibilidade com esta (secção 2.5).

As perguntas feitas e as possíveis respostas a dar para cada subcontrolo são:

1. **Política Definida** (A organização tem atualmente uma política definida que indica que o subcontrolo em questão deve ser implementado?) — *"No Policy"*; *"Informal Policy"*; *"Partially Written Policy"*; *"Written Policy"*; *"Approved Written Policy"*; *"Not Applicable"*.

2. **Controlo Implementado** (A organização implementa atualmente o subcontrolo em questão? E até que ponto ele é implementado?) — *"Not Implemented"*; *"Parts of Policy Implemented"*; *"Implemented on Some Systems"*; *"Implemented on Most Systems"*; *"Implemented on All Systems"*; *"Not Applicable"*.

3. **Controlo Automatizado** (A organização atualmente automatiza a implementação deste subcontrolo? E até que ponto ele é automatizado?) — *"Not Automated"*; *"Parts of Policy Automated"*; *"Automated on Some Systems"*; *"Automated on Most Systems"*; *"Automated on All Systems"*; *"Not Applicable"*.

4. **Controlo reportado** (A organização atualmente reporta este subcontrolo aos representantes do negócio? E até que ponto ele é reportado?) — *"Not Reported"*; *"Parts of Policy Reported"*; *"Reported on Some Systems"*; *"Reported on Most Systems"*; *"Reported on All Systems"*; *"Not Applicable"*.

Tendo em conta os requisitos organizacionais como, por exemplo, a tolerância ao risco, deve ser decidido por parte dos responsáveis até que ponto um subcontrolo é considerado uma lacuna para o âmbito da empresa em análise. Como após um subcontrolo ficar respondido é-lhe atribuído um *score*, pode-se usar essa pontuação para definir o que é ou não lacuna. É aconselhável que se considere uma lacuna um subcontrolo com um *score* inferior a 50%, porém a organização pode querer assumir um valor superior abaixo do qual os subcontrolos são considerados lacunas.

Após selecionar as opções que correspondem à situação atual da organização, pode-se ainda colocar documentos de evidência ou de suporte às respostas dadas. Porém, existe ainda a hipótese de adicionar mais pessoas para a organização no menu *"Administration"*, o que faz com que seja possível atribuir a outras pessoas o trabalho de responder a certas perguntas. Depois de todas as respostas dadas, pode-se fazer *download* dos relatórios finais gerados automaticamente e com vários formatos disponíveis, no separador *"Reports"*, sendo que na opção *"Control Summary Report"* é feito um *download* de um *Excel* com um relatório sobre tudo o que foi respondido e feito nessa avaliação.

Pela análise destes relatórios consegue-se rapidamente perceber quais as práticas da CIS implementadas, se existe uma política para o controlo na empresa, se este está automatizado ou se é reportado aos representantes do negócio. De referir ainda que no separador *"Assessment History"* fica guardado um histórico das avaliações feitas ao longo do tempo, o que é muito útil para a empresa verificar a evolução temporal em cibersegurança e poder analisar os *"assessments"* antigos sempre que quiser.

Assim, este passo fica concluído com a total noção da situação atual em cibersegurança para o âmbito da estratégia, sendo gerados muitos relatórios e obtida muita informação que será útil para os próximos passos. Nomeadamente, é reunida a informação suficiente para perceber onde a empresa planeia estar em cibersegurança e quais os riscos que existem com as medidas ou controlos que tem atualmente em prática.

4.3.4 *Passo 4: Efetuar avaliações de risco de cibersegurança*

Efetuar Avaliações de Risco de Cibersegurança (4.º Passo)		
Inputs	***Outputs***	**Iniciativas**
• Objetivo e âmbito de aplicação da estratégia (*"Function List"*) • Lista dos sistemas e ativos inseridos no âmbito da estratégia • Mapa/Arquitetura de rede com os sistemas e ativos mais relevantes inseridos no âmbito da estratégia • Lista dos requisitos de cibersegurança (regulamentares e organizacionais) e os de negócio inseridos no âmbito da estratégia • Lista de referências (*standards*, ferramentas, métodos, guias de cibersegurança e gestão de riscos, etc.) inseridas no âmbito da estratégia • Relatório do C2M2 com o resultado da avaliação atual • Nível de implementação atual na NIST *Framework* • Estado em implementação das práticas do CIS *Controls* versão 8.0 (Relatório CIS CSAT) • Estratégia atual de Gestão de Riscos, incluindo a abordagem de avaliação de risco definida pela organização • Informações de ameaças de cibersegurança internas e externas	• Relatórios de avaliação de risco para cada uma das funções presentes na *"Function List"* (Listagens dos riscos)	• Caso exista, recolher os relatórios de avaliações de risco de cibersegurança já existentes na organização. • Recolher as informações de ameaças de cibersegurança internas e externas. • Perceber as tolerâncias de risco para a organização. • Identificar as vulnerabilidades, ameaças, fontes de ameaças e controlos possíveis para as mitigar nos ativos e sistemas inseridos no âmbito. • Realização de avaliações de risco para cada uma das funções presentes na *"Function List"* efetuando uma listagem de todos os riscos identificados nesta fase.

Tabela 23: Resumo dos tópicos abordados no passo 4 da Estratégia de Cibersegurança

Dado que no passo 3 já se abordou como a empresa lida com os processos de gestão de riscos, é altura de se efetuarem avaliações de riscos de cibersegurança naquilo que faz parte do âmbito da estratégia, como se pode constatar pela tabela resumo 23. Este processo de avaliações de risco deve complementar o atual processo de

gestão de riscos corporativos na organização, caso exista. Deste modo, é um passo crucial e dos mais importantes, dado que é o principal *"input"* para os próximos passos, fornecendo as informações necessárias para tomar decisões nas ações a tomar tanto na decisão do perfil alvo como na priorização de ações no passo 6. Além disso, constitui-se como um reforço complementar à gestão de riscos, garantindo uma análise mais eficaz, rigorosa e completa no que diz respeito a riscos de cibersegurança.

Para ajudar nesta fase, pode-se ter em consideração os documentos, *frameworks* adotadas ou políticas sobre gestão de riscos corporativos já existentes na organização e usar essa informação para ajudar na recolha, análise e avaliação dos riscos de cibersegurança. Outra abordagem é a de usar a abordagem de avaliação de risco proposta nesta dissertação que se baseia não só nas recomendações da NIST [90] e do C2M2 [23], mas também na norma ISO/IEC 27005:2018 [61]. No caso do ISO/IEC 27005:2018 são fornecidas informações sobre como gerir os riscos da segurança da informação em qualquer tipo de organização, sendo que também se pode aproveitar esta abordagem para a cibersegurança. Contém ainda listagens de ameaças típicas, fontes de ameaças e vulnerabilidades. Naquilo que é importante para este passo, esta norma descreve que existem 3 grandes etapas para o processo de levantamento de riscos:

- Identificação do risco (etapa 1):
  - Identificação dos ativos;
  - Identificação das ameaças;
  - Identificação dos controlos existentes;
  - Identificação de vulnerabilidades;
  - Identificação dos cenários de incidentes e as suas consequências.
- Análise do risco (etapa 2):
  - Avaliação do impacto das consequências dos cenários de incidentes;
  - Avaliação da probabilidade dos cenários de incidentes;
  - Nível de determinação do risco.
- Avaliação do risco (etapa 3).

Olhando para as etapas acima, alguns dos pontos já foram efetuados, como a identificação dos ativos e dos controlos existentes (Lista de requisitos e referências, feito no passo 2 (e 3 também, uma vez que com os relatórios da avaliação atual também é possível perceber aquilo que está feito). Além disso, o mapa de rede (obtido no passo 2) também é muito útil para identificar as ameaças. Deste modo, na etapa 1 só fica a faltar a identificação das ameaças, vulnerabilidades e das consequências, sendo depois necessário efetuar aquilo que consta nas etapas 2 e 3. Para tal, deve-se começar por recolher os relatórios ou registos de riscos já efetuados pela organização para o âmbito da estratégia, caso existam oriundos de iterações anteriores da estratégia de cibersegurança ou da gestão de riscos corporativos. A empresa pode já possuir ferramentas ou outros meios de registo de riscos, oriundos do seu programa de gestão de riscos, que podem conter informação útil para a cibersegurança, tais como indicações de ameaças e em que serviços isso pode acontecer. Além destas informações, existem outras fontes tanto internas como externas que ajudam na identificação dos riscos, como as informações de ameaças a que os sistemas informáticos possam estar sujeitos, tais como:

1. **Fontes de Ameaças Internas**: Obtidas a partir de: revisão ou análise de incidentes de cibersegurança; avaliações de ameaças anteriores; proprietários ou utilizadores de ativos ("*resource owners*"); a equipa de recursos humanos; os especialistas em segurança da informação e gestão de instalações; informações dos departamentos legais; entre outras.

2. **Fontes de Ameaças Externas**: Obtidas a partir de: catálogos e estatísticas de ameaças (o ISO/IEC 27005:2018 tem um catálogo de ameaças típicas no anexo C, entre outros catálogos relativos à área em questão); outras organizações (órgãos legais, autoridades meteorológicas, companhias de seguros, instituições públicas de segurança nacional, autoridades governamentais); informação que circula nos meios de comunicação; entre outras.

Assim, é importante que as organizações identifiquem os riscos emergentes e usem informações de ameaças de fontes internas e externas para obter uma melhor compreensão da probabilidade e do impacto dos eventos de cibersegurança [90]. Além das ameaças, é necessário identificar as vulnerabilidades a que o ambiente da empresa possa estar sujeito. Para este processo, podem-se usar ferramentas para o efeito, como *scans* de vulnerabilidades e testes de intrusão em redes ou sistemas (*"pentesting"*). Existem também alguns catálogos de vulnerabilidades mais comuns que podem e devem ser usados para auxiliar neste processo, como, por exemplo, o anexo D do ISO/IEC 27005:2018. No final, obtém-se uma lista com as vulnerabilidades e a sua relação com os ativos, ameaças e controlos implementados. As vulnerabilidades devem ser identificadas para [61]:

- As funções da *"Function List"*;
- Os processos e procedimentos;
- As rotinas de gestão;
- O pessoal da empresa;
- O ambiente físico;
- As configurações dos sistemas de informação;
- O *hardware*, *software* ou equipamento de comunicação;
- As dependências de terceiros.

Após se ter a lista dos ativos, dos controlos atualmente implementados, das ameaças e das vulnerabilidades, identificam-se as consequências que as perdas de confidencialidade, integridade e disponibilidade (CIA) podem ter sobre os ativos. Nesta última tarefa da identificação de riscos, identificam-se os danos ou consequências para a organização que podem ser causados por um cenário de incidente de cibersegurança, que nada mais é que uma ameaça que explorou uma ou mais vulnerabilidades e despoletaram um incidente. Para tal são criados cenários de potenciais incidentes de cibersegurança através da informação das ameaças e das vulnerabilidades, e realizam-se avaliações do impacto desses incidentes, tendo em conta o estado dos controlos atualmente implementados no âmbito. Mas para avaliar o impacto ("grau de sucesso de um incidente") é necessário existir um critério, que pode ser aquele que já está estabelecido pela atual gestão de riscos da organização ou então pode ser baseado em recomendações como as do ISO/IEC 27005:2018. Nessa norma é referido que o impacto possui um efeito imediato (operacional) ou um efeito futuro (negócios) que inclui consequências financeiras e de mercado, além das

consequências poderem ser de natureza temporária ou permanente, como no caso da destruição de um ativo [61]. Como resultado desta tarefa, vai-se obter uma lista com todos os cenários de incidentes e as suas consequências relativas a ativos e processos de negócio. Deste modo, alguns exemplos de consequências úteis para estimar o impacto dos cenários de incidentes criados são:

- Custo e tempo de trabalho perdido até que o serviço prestado pelo(s) ativo(s) seja restabelecido;
- Perda de oportunidades (por exemplo, perda de oportunidades de negócio e de investimento devido aos custos do incidente);
- Potencial uso indevido de informações obtidas através de uma lacuna de segurança;
- Custo financeiro de habilidades específicas para reparar os danos;
- Custo de aquisição, configuração e instalação de um novo ativo ou do *backup*;
- Reputação e imagem da organização;
- Violação das obrigações regulamentares ou de códigos de conduta ética;
- Saúde e segurança.

Tendo concluído a identificação de riscos, deve haver uma lista de cenários de incidentes relevantes com a identificação das ameaças, ativos afetados, vulnerabilidades exploradas e consequências para ativos e processos de negócios, além de listas de todos os controlos existentes e planeados, a sua eficácia, implementação e estado de uso [61].

Pode-se então seguir para a etapa 2, análise dos riscos, devendo-se ter em atenção que existem dois tipos de metodologias que podem ser usadas separadas ou combinadas:

1. **Análise de riscos qualitativa**: É usada uma escala de atributos qualitativos para identificar a magnitude dos potenciais impactos/consequências (por exemplo, Baixo, Médio e Alto) e a probabilidade de tais ocorrências.
    - **Vantagens**: Fácil de entender pelas partes interessadas e ajuda a identificar riscos mais relevantes.
    - **Desvantagens**: Dependência de uma escolha subjetiva, pelo que se deve usar informação e dados factuais se possível.
2. **Análise de riscos quantitativa**: É usada uma escala de valores numéricos para medir o impacto e probabilidade, usando históricos de dados de várias fontes, como dados de incidentes.
    - **Vantagens**: Está diretamente relacionado com os objetivos e preocupações de segurança da informação da empresa.
    - **Desvantagens**: Necessita de dados factuais e/ou auditáveis sobre novos riscos e fraquezas, o que pode ser difícil de obter, criando a ilusão de valor e precisão da avaliação de riscos.

Recomenda-se que se utilize uma análise qualitativa primeiro, que será a usada nesta tese, e só depois introduzir uma análise quantitativa, podendo o processo ter a combinação de ambos. Tendo decidido a metodologia a utilizar, inicia-se a análise do risco com a avaliação do impacto das consequências dos cenários de incidentes (ou riscos) e a probabilidade de estes ocorrerem, tal como apresentado pelo guia de gestão de riscos de segurança de informação e de cibersegurança efetuado pelo CNCS [16], que tem por base o ISO/IEC 27005:2018. O risco

obtém-se pela multiplicação do impacto (da consequência do cenário de incidente) pela probabilidade (da ocorrência desse incidente), sendo representado pela seguinte equação:

$$Risco = (probabilidade\ da\ ocorrência\ do\ incidente) \times (impacto\ do\ incidente) \quad (1)$$

Para definir a probabilidade e o impacto, deve-se olhar para as consequências identificadas na etapa anterior, que tiveram em conta a perda de confidencialidade, integridade e disponibilidade, e usar um conjunto de critérios para atribuir valores à probabilidade e ao impacto. Na Figura 9 pode-se observar os critérios de análise de riscos qualitativos que podem ser usados para atribuir valores ao impacto e à probabilidade, podendo os mesmos ser adaptados pela empresa. Para a análise do risco ficar concluída utiliza-se a equação (1) para determinar o nível de risco para cada um dos cenários de incidentes (riscos).

Critérios de Análise de Riscos

Risco	Probabilidade	Impacto
Muito Alto (5)	Evento tem ocorrido frequentemente. Há registo de várias ocorrências e é provável que venha a ocorrer novamente num intervalo igual ou inferior a 6 meses.	Evento que gera impacto sobre toda a organização ou representa perda de disponibilidade, confidencialidade e/ou integridade causando prejuízos de forma generalizada, inviabilizando todas as funções primárias ou proporcionando percepção negativa
Alto (4)	Evento tem ocorrido frequentemente. Há registo de mais de uma ocorrência e é provável que venha a ocorrer novamente num intervalo de 1 ano.	Evento que gera impacto sobre vários grupos ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções primárias de trabalho de múltiplas áreas da organização.
Médio (3)	Evento tem ocorrido, porém não frequentemente. Há registos de uma ocorrência em intervalos de 1 ano ou superior.	Evento que gera impacto sobre um grupo relevante ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções primárias de trabalho.
Baixo (2)	Evento já ocorreu nesse tipo de atividade e é possível que venha a ocorrer novamente no intervalo de até 3 anos.	Evento que gera impacto sobre um pequeno grupo ou representa perda de disponibilidade, confidencialidade e/ou integridade prejudicando as funções secundárias de trabalho, não sendo o bastante para intervir nas funções principais.
Muito Baixo (1)	Evento nunca ocorreu nesse tipo de atividade e é altamente improvável que venha a ocorrer num intervalo superior a 5 anos.	Evento que gera impacto sobre apenas uma pessoa ou representa perda de disponibilidade, confidencialidade e/ou integridade que não necessita de intervenção ou paralisação imediata.

Figura 9: Critérios de análise de riscos (Fonte: Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança v1.0 [16])

A partir do nível de risco, pode-se efetuar uma avaliação do risco (etapa 3), priorizando cada um dos riscos para um melhor tratamento no passo 5 da estratégia. De referir que este nível é relativo ao risco inerente, ou seja, ao risco que existe no momento em que se efetua o levantamento, e não ao risco residual que será o risco que permanece mesmo após a implementação dos controlos que o mitigam (o risco residual, será abordado no passo 5 da estratégia

de cibersegurança). Nas figuras 10 e 11 apresentam-se duas matrizes de riscos distintas, calculadas com base na equação do risco (1). A interpretação mais conservadora da matriz dos operadores de serviços essenciais (OES) deve-se ao facto de uma falha nos serviços essenciais ter um impacto mais substancial na sociedade.

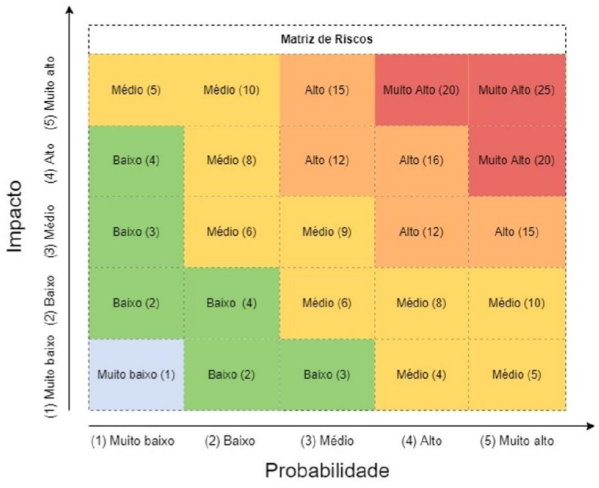


Figura 10: Matriz de riscos (Fonte: Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança v1.0 [16])

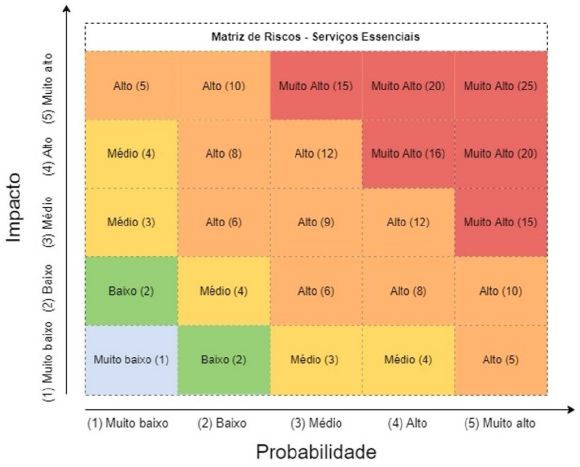


Figura 11: Matriz de riscos para os operadores de serviços essenciais (Fonte: Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança v1.0 [16])

Após se ter determinado um valor para cada cenário de incidente em termos de probabilidade, impacto e nível de risco, é altura de seguir para terceira etapa (avaliação dos riscos), onde se vai avaliar quais os riscos que são aceites ou que necessitam de tratamento para serem mitigados, transferidos ou evitados. É nesta etapa que se vai comparar os níveis de risco com os critérios de avaliação e de aceitação de risco definidos para a organização, identificados no passo 2. Caso não exista um critério na organização formalmente definido, pode-se recorrer à opinião das partes interessadas da organização (donos do risco, responsáveis pela estratégia, etc.) ou então a processos de gestão de risco já publicados, como o que será abordado a seguir (com base no guia de gestão de riscos de segurança de informação e de cibersegurança efetuado pelo CNCS [16]). Os riscos podem então ser avaliados de forma justificada e aprovada em:

1. **Aceitar**: Decisão de aceitar o risco sem ser preciso efetuar ações nenhumas sobre ele;
2. **Evitar**: Se o risco for muito alto e não existirem condições para o tratar, então pode-se decidir evitar o risco eliminando ou alterando as condições onde este risco existe;
3. **Mitigar**: Decisão de reduzir o nível de risco através da seleção de controlos no passo 5 da estratégia para que este se torne aceitável;
4. **Transferir**: Caso não se consiga tratar o risco eficazmente, então pode-se decidir transferir o risco para uma entidade externa, sendo que deve-se ter cuidado porque esta ação pode modificar o risco ou trazer novos riscos para a organização.

Por último, a seguir apresentam-se algumas considerações úteis para ajudar a decidir ou atribuir uma avaliação para cada risco:

- Devem ser consideradas todas as propriedades de segurança da informação (CIA) e as respetivas consequências identificadas nestas propriedades. Além disso, se um critério não for relevante para a organização

(por exemplo, perda de confidencialidade), então todos os riscos que afetem este critério podem não ser relevantes;

- Devem ser consideradas todas as restrições da organização, tais como temporais, custo/benefício, técnicas, operacionais, culturais, éticas, ambientais, legais/regulamentares, facilidade de utilização, restrição de pessoal ou até de integração com os controlos existentes de novos controlos na infraestrutura atual;
- A importância do processo ou da atividade empresarial apoiada por um determinado ativo, ou conjunto de ativos, deve ser considerada. Além disso, pode-se aceitar os riscos mais baixos até que os riscos mais críticos sejam evitados ou mitigados, pelo que depois deve-se voltar a estes riscos para serem abordados. Por exemplo, se existirem dois riscos elevados para tratar, mas um estar no âmbito de um processo mais crítico para a empresa do que o outro, pode ser considerado evitar o risco elevado do processo mais crítico primeiro, aceitando provisoriamente o risco do processo menos importante. Porém, normalmente ao ter riscos elevados, deve-se proceder rapidamente ao tratamento de todos eles;
- A decisão de implementar controlos para o risco vai trazer problemas de desempenho para a atividade envolvida? Esta perda pode fazer com que não seja possível mitigá-lo;
- Considerar também o grau de maturidade dos controlos atualmente implementados, com a ajuda dos relatórios da situação atual do passo 3 da estratégia (secção 4.3.3).

No fim deste passo 4, obtém-se uma listagem dos riscos devidamente priorizados (priorizados no sentido de cada um possuir uma avaliação diferente para tratamento) para cada uma das funções da *"Function List"*, tendo em conta os critérios de avaliação de risco estabelecidos para todos os cenários de incidentes de cibersegurança.

4.3.5 *Passo 5: Definir/Criar uma Avaliação Alvo*

Definir/Criar uma Avaliação Alvo (5.º Passo)		
Inputs	***Outputs***	**Iniciativas**
• Objetivo e âmbito de uso da estratégia (*"Function List"*) • Prioridades alto-nível para a estratégia de cibersegurança (metas/objetivos) • Pilares Estratégicos do "Plano de Cibersegurança" • Responsabilidades alto-nível de cada colaborador/parceiro em cibersegurança na empresa, caso efetuado no passo 1 • Lista de referências (*standards*, ferramentas, métodos, guias de cibersegurança e gestão de riscos, etc.) inseridas no âmbito da estratégia • Lista dos requisitos de cibersegurança (regulamentares e organizacionais) e os de negócio inseridos no âmbito da estratégia • Relatório do C2M2 com o resultado da avaliação atual • Nível de implementação atual na NIST *Framework* • Estado em implementação das práticas do CIS *Controls* versão 8.0 (Relatório CIS CSAT) • Relatórios de avaliação de risco para cada uma das funções presentes na "*Function List*" (Listagens dos riscos) • Estratégia atual de Gestão de Riscos	• Perfil-Alvo da empresa em cibersegurança • Nível de Implementação desejado na NIST *Framework* • Relatório com as análises efetuadas e razões que levaram a que algumas medidas não entrassem para o "Perfil-Alvo" • Documento "Plano (Política) de Cibersegurança"	• Identificação dos controlos/medidas que irão mitigar os riscos relatados nos resultados do passo 4. • Definição das MIL's e escolha das práticas alvo através da análise do relatório do C2M2. • Seleção de um nível de implementação alvo na NIST *Framework*. • Escolha dos controlos ou medidas alvo através dos CIS *Controls* v.8, recomendando que seja selecionado pelo menos todo o "IG1". • Análise da *Framework Core* da NIST para perceber quais as subcategorias relevantes e desta forma incluir potenciais práticas que ainda não estejam selecionadas para a avaliação alvo, de acordo com o mapeamento dos apêndices e as referências informativas. • Possibilidade de escolha de controlos de outras fontes que podem ser relevantes para constarem no "Plano de Cibersegurança" tendo em conta os que estão implementados, os que estão já escolhidos e os que não estão. • Elaboração de um relatório "resumo" com as análises efetuadas (por exemplo, a análise custo-benefício) e com os motivos da não inclusão de certas medidas consideradas aquando da criação da avaliação alvo. • Redefinição das responsabilidades em cibersegurança de cada colaborador, se necessário, através do que foi decidido no novo "Perfil-Alvo" e aprofundando mais as que foram escritas no passo 1. • Escrita ou revisão do documento "Plano (ou Política) de Cibersegurança" inserindo nos vários pilares estratégicos as medidas ou controlos relacionados decididos para implementação no perfil desejado.

Tabela 24: Resumo dos tópicos abordados no passo 5 da Estratégia de Cibersegurança

Este passo tem como objetivo definir uma avaliação alvo ou "Perfil-Alvo" para as funções no âmbito da estratégia, ou seja, definir um estado em cibersegurança onde se planeia estar. Conforme a Tabela 24, é neste passo que fica concluído o "Plano de Cibersegurança" que, dependendo da vontade da organização, pode transformar-se na política de cibersegurança da empresa, tendo só o cuidado de restringir o âmbito da política ao que constar na *"Function List"*.

Ao criar o "Perfil-Alvo", deve ser considerado o seguinte [23]:

- Metas/objetivos definidos para a estratégia de cibersegurança, ou seja, as prioridades identificadas no passo 1;
- Requisitos legais e regulamentares identificados no passo 2;
- Objetivos/missão do negócio identificada no passo 2;
- Restrições organizacionais identificadas no passo 2;
- Práticas atuais de gestão de riscos, espelhadas nos resultados do passo 3 (relatório C2M2, nível de implementação em práticas de gestão de riscos da NIST e o relatório CIS CSAT);
- Ambiente de risco atual, obtido nos relatórios ou listas de riscos efetuadas no passo 4.

Com base nestas informações, neste passo são identificadas as práticas que se desejam ver implementadas no âmbito da estratégia. Esta estratégia tem por base a NIST *Framework* (secção 2.5), mas isso não significa que só se considerem as práticas da NIST CSF, até porque apesar de cobrir amplamente os vários domínios da cibersegurança e gestão de riscos de cibersegurança, não abrange nem especifica completamente tudo o que é relacionado a este tema. Para a completar, devem ser usados outros guias, padrões, ferramentas, métodos e controlos existentes noutras fontes relacionadas a cibersegurança. Nesta estratégia serão seguidas, entre as várias referências informativas que a NIST *Framework* oferece, as práticas do C2M2 v2.0 (secção 2.6) e os controlos da CIS v8.0 (secção 2.7).

Para começar a definir ou criar uma avaliação alvo, o responsável (ou responsáveis) pela implementação da estratégia deve(m) agendar uma ou mais reuniões com os responsáveis/executivos com poderes de decisão em matérias de cibersegurança nas áreas definidas para o âmbito. Para tal, é importante que se analise toda a informação anterior, começando por ver quais as prioridades da estratégia e os pilares do plano. Em seguida, deve-se debater as restrições da organização, requisitos legais e o objetivo ou missão do negócio. Desta forma, parte-se de uma base sólida, fundamental para se decidir as práticas e controlos que irão constar no "Plano de Cibersegurança".

A elaboração do "Plano de Cibersegurança" deve começar pela discussão de quais os controlos que já estão implementados, perceber se vão ou não continuar em vigor no plano e qual o respetivo grau de maturidade desejado. Após isso, é preciso olhar para os relatórios de riscos de cada uma das funções da *"Function List"* e começar o plano de tratamento desses riscos. Tendo em conta a avaliação atribuída a cada risco, é necessário decidir sobre os controlos eficazes que tornem o risco residual aceitável. A eficácia dos controlos pode e deve também ser considerada ou avaliada, sendo que normalmente aqueles que são baseados em documentos técnicos, como normas, ou são publicados por instituições de segurança de relevo, serão mais eficazes dos que aqueles que não estão em qualquer documento e não sofrem nenhum tipo de monitorização. Essas medidas, a par das que já estão e irão continuar implementadas, irão entrar também para o "Perfil-Alvo", constando no "Plano de Cibersegurança".

Após os controlos que mitigam os riscos estarem identificados, é altura de decidir quais as práticas do C2M2 que se aspira ver implementadas no âmbito da estratégia. Para isso, devem ser analisados os resultados do questionário de autoavaliação C2M2 para perceber primeiro quais são as lacunas ou principais fragilidades a resolver. O facto de se identificar primeiro as lacunas presentes no relatório C2M2 é para haver sempre o incentivo de fazer com que estas deixem de ser lacunas, pelo que não podem constar no plano/política de cibersegurança se não tiverem "*Largely Implemented*" ou "*Fully Implemented*". É natural também que existam indicações nos comentários ou notas deixadas por quem respondeu ao questionário e que podem ajudar nesta fase na decisão sobre quais as práticas mais prioritárias ou as que são mais difíceis de concretizar. Adicionalmente, existe ainda a indicação nesse relatório sobre em que MIL é que a empresa se encontra em cada domínio do C2M2, pelo que essa informação deve ser analisada e deve ser decidido em que MIL é que a empresa pretende estar em cada domínio ("MIL-alvo"). Com essa decisão já se tem a noção sobre as práticas que devem estar implementadas em cada domínio para que seja possível atingir a MIL pretendida. Claro que, nesta fase, podia-se dizer que estar na MIL3 em todos os 10 domínios seria o ideal, mas isso pode não ser verdade caso a empresa não tenha condições (financeiras, força de trabalho, objetivos de negócio, viabilidade de implementação, custo/benefício, etc.) para isso ser alcançável. Desta forma, e isto aplica-se a todas as decisões efetuadas, nesta fase deve efetuar-se uma análise custo benefício (CBA) para perceber quais os benefícios e os prejuízos de implementar determinada prática, pelo que se for concluído que irá trazer mais benefícios que prejuízos, então a medida deve ser incluída no "Plano de Cibersegurança". É importante reforçar que no plano devem constar também as práticas do C2M2 que já estão totalmente implementadas, para que tudo fique devidamente documentado e estas sejam reforçadas. Se se achar pertinente, pode-se separar ou evidenciar no plano quais são as novas práticas do C2M2, ou as que são consideradas lacunas segundo a avaliação alvo definida.

Após decidir sobre as práticas do C2M2 desejadas, é necessário definir um nível de implementação alvo em práticas de gestão de risco da NIST *Framework*. Para isso, deve-se olhar para as características de cada nível e escolher o nível que se pretende, tendo em conta o nível atual. Mais uma vez, o ideal para a organização pode não ser subir para o nível máximo ("Adaptável"), tal como já foi explicado para o caso anterior do C2M2, porém "há sempre o incentivo para ir subindo de nível" [90]. Após selecionar o nível de implementação desejado, é necessário identificar quais são as práticas e as atividades de gestão de riscos de cibersegurança necessárias para atingir o objetivo. Por exemplo, tendo em conta o mapeamento da Figura 8, pode-se perceber quais as práticas necessárias do C2M2 para alcançar determinado nível, relembrando que para se estar num determinado nível é necessário ter as práticas todas desse nível implementadas e também as que estão nos níveis anteriores.

Tendo já o nível de implementação alvo na NIST decidido, pode-se avançar para a escolha dos controlos da CIS, mediante as mesmas condições das escolhas anteriores. Para isso, deve-se escolher primeiro qual o grupo de implementação (IG) que deve constar no "Perfil-Alvo", ou seja, que subcontrolos da CIS, pertencentes a um determinado IG, irão constar no plano. Nas recomendações da CIS, tal como já foi referido na secção 2.7, é dito que todas as empresas deveriam ter pelo menos o grupo 1 selecionado ("IG1"), uma vez que este está preparado para que grande parte das empresas os consigam aplicar. Aproveitando então os resultados do CIS CSAT do passo 3, pode-se perceber de entre todos os subcontrolos quais é que estão implementados e quais são lacunas, conforme aquilo que foi definido no passo 3 (secção 4.3.3), sendo que o que for considerado lacuna não pode constar na política se não tiver uma avaliação alvo que a coloque como "não lacuna", tal como acontece para o caso das práticas do C2M2. Outro aspeto interessante é que alguns dos subcontrolos podem estar implementados sem grande sofisticação ou eficácia, o que faz com que seja importante também decidir qual o grau de implementação que se pretende para um determinado subcontrolo. Por exemplo, um subcontrolo pode estar a ser aplicado num

determinado âmbito e até constar já nas políticas, porém este não se encontra automatizado com ferramentas próprias para o efeito e não é reportado à área de negócio da empresa. Por fim, outra informação que pode ser relevante são os gráficos da CIS CSAT, uma vez que permite analisar, tendo em conta a avaliação realizada no passo 3, o desvio que existe em relação à média da indústria. Desta forma, pode-se utilizar esta informação para avaliar como é que a empresa se compara com a média nos vários tipos de controlos da CIS.

Concluída então a escolha dos controlos/subcontrolos da CIS, com o auxílio do CIS CSAT, pode-se então analisar aquela que é a base de referência desta estratégia: a *Framework Core* da NIST CSF. Basicamente, esta parte serve para escolher as subcategorias mais relevantes e incluir no "Perfil-Alvo" as práticas correspondentes que ainda não tenham sido decididas nas iniciativas anteriores deste passo e que estejam presentes ou nas referências informativas, ou no mapeamento apresentado no apêndice A. Por exemplo, se se considerar que a subcategoria PR.IP-1 (subcategoria 1 da categoria IP — "Procedimentos e Processos de Proteção da Informação" pertencente à função PR — "Proteger") é muito relevante para o âmbito e o plano deve conter medidas dessa subcategoria, então devem ser adicionadas as práticas do C2M2 e os subcontrolos da CIS todos correspondentes, além de referências informativas de outras fontes relacionadas. Para ajudar neste processo, aconselha-se vivamente o uso do apêndice A, onde é apresentado um mapeamento da *Framework Core*, com as informações disponibilizadas pela NIST, para as práticas e subcontrolos do C2M2 e da CIS, respetivamente. Estas adições ao "Plano de Cibersegurança" devem ser alvo de análise, tal como já foi explicado para as tarefas anteriores, e também só devem ser adicionadas aquelas práticas que ainda não tiverem sido adicionadas nas tarefas anteriores.

Por último, em termos de escolha da avaliação alvo, podem ser adicionados outros controlos ou práticas de outras fontes e que possam ser relevantes para constarem no "Plano de Cibersegurança". Essa inclusão só deve acontecer caso haja outras medidas importantes a serem adicionadas e que ainda não constam no plano. Tal como nas outras medidas, é importante que se deixe sempre a referência das fontes onde se foi buscar a prática adicionada. Além disso, podem existir práticas que não estejam em nenhuma referência e mesmo assim se considere ser útil incluir. Isto é fundamental porque a avaliação alvo deve ao máximo conter todas as abordagens de cibersegurança aplicáveis, incluindo ferramentas, *standards* e *guidelines*, tudo isto para se conseguir lidar com o risco de cibersegurança de forma proporcional ao risco para os objetivos organizacionais [23]. O objetivo final é que o "Perfil-Alvo" fique totalmente definido e formalmente documentado no plano para haver ao máximo o reforço da cibersegurança e, em simultâneo, se encontre alinhado com os objetivos e restrições da organização.

Para documentação de todas as decisões tomadas neste passo 5, aconselha-se ainda que quem está encarregue de facilitar este processo de tomada de decisões, ou seja, o responsável pela estratégia, crie um relatório "resumo" onde expresse todas as análises efetuadas e razões para as várias medidas de cibersegurança consideradas que não entraram no "Plano (ou Política) de Cibersegurança". Isto significa que as análises custo-benefício, ou outras efetuadas sobre uma determinada medida, devem ser documentadas nesse relatório em conjunto com outras razões que levaram à sua não aceitação (por exemplo, por motivos legais, falta de recursos, pouca relevância no contexto, etc.), podendo até incluir o nome das pessoas que decidiram não aceitar a medida. Este relatório é fundamental porque faz com que as medidas analisadas e que foram rejeitadas fiquem documentadas com as respetivas razões, podendo ser reavaliadas em iterações futuras da estratégia. Por outro lado, se for questionado na organização o porquê de determinada medida não constar no plano, ou até quem foi o responsável (ou responsáveis) por essas decisões, existirá um documento com essa informação toda. O relatório deve então ser assinado por todos os participantes na criação do "Perfil-Alvo".

Após se ter decidido tudo o que constituirá o perfil desejado, passa-se à elaboração do "Plano (ou Política) de Cibersegurança", que deve considerar ou incluir:

- Resultado(s) do passo 1:
  - Âmbito/Destinatários do plano de cibersegurança, que será o mesmo que o âmbito da estratégia (*"Function List"*);
  - Prioridades (objetivos/metas) da estratégia de cibersegurança, caso se ache pertinente;
  - Pilares estratégicos do plano;
  - Responsabilidades alto-nível de cada colaborador/parceiro em cibersegurança na empresa, caso existam.
- Resultado(s) do passo 2:
  - Legislação sobre cibersegurança (leis, regulamentos, requisitos, etc.) que o âmbito possa estar sujeito.
- Resultado(s) deste passo:
  - Avaliação alvo ("Perfil-Alvo"), enumerando e separando as várias práticas ou controlos alvo, que devem estar devidamente explicados, documentados e referenciados, pelos pilares estratégicos que regem o plano. Caso se conclua que os pilares estratégicos não foram bem definidos no passo 1, face ao que consta na avaliação desejada, pode-se voltar ao passo 1 e redefinir os pilares e as prioridades. (Recomendação: o plano pode e deve conter uma visão (ou mapeamento) na *Framework Core* da NIST de todas as práticas do C2M2, dos controlos da CIS e das referências informativas da *Framework Core* que foram escolhidas durante este passo. Para isso, pode-se recorrer ao apêndice A para verificar em que categorias e subcategorias da NIST estão mapeadas essas práticas e controlos);
  - Avaliação alvo ("Perfil-Alvo") deve incluir ainda as decisões dos níveis na NIST CSF e no C2M2 e o grupo de implementação no CIS *Controls* v8.0;
  - Responsabilidades e obrigações em cibersegurança de cada colaborador, tendo em conta o papel na empresa e o âmbito da estratégia.

Deste modo, falta só redefinir as responsabilidades em cibersegurança para cada função atribuída aos colaboradores. No passo 1 já podem ter sido identificadas as responsabilidades alto-nível com base na estrutura e ambiente da organização. Porém, o objetivo, neste passo, é detalhar as responsabilidades mediante aquilo que consta nos pilares estratégicos, ou seja, no "Perfil-Alvo". É natural que o novo perfil contenha novas tarefas, pelo que deve ser decidido quem irá ficar encarregue de as executar, monitorizar e reportar. É importante que a separação de responsabilidades seja bem precisa para que todos os colaboradores saibam aquilo que devem fazer. Deste modo, pode-se decidir separar responsabilidades por áreas, departamentos ou grupos de trabalho, pelo que todos os colaboradores inseridos no âmbito da estratégia devem ter as suas responsabilidades no "Plano (ou Política) de Cibersegurança".

Por fim, tem-se toda a informação necessária para finalizar o documento oficial do "Plano (ou Política) de Cibersegurança". Dependendo da decisão dos responsáveis da organização, o documento pode a qualquer momento transformar-se na política de cibersegurança da organização, fazendo todo o sentido que assim seja. O documento irá certamente sofrer alterações ou revisões ao longo do tempo que até podem fazer com que o âmbito seja ampliado. Se neste passo for realizada a revisão de um plano já existente, é importante que as medidas que já lá constam sejam alvo de análise, para verificar se são para continuar ou remover.

4.3.6 *Passo 6: Criar um Plano de Ação Priorizado para Combater as Lacunas*

Criar um Plano de Ação Priorizado para Combater as Lacunas (6.º Passo)		
Inputs	***Outputs***	**Iniciativas**
• Objetivo e âmbito de uso da estratégia (“*Function List*”) • Lista de referências (*standards*, ferramentas, métodos, guias de cibersegurança e gestão de riscos, etc.) inseridas no âmbito da estratégia • Lista dos requisitos de cibersegurança (regulamentares e organizacionais) e os de negócio inseridos no âmbito da estratégia • Relatório do C2M2 com o resultado da avaliação atual • Nível de Implementação atual na NIST *Framework* • Estado em implementação das práticas do CIS *Controls* versão 8.0 (Relatório CIS CSAT) • Relatórios de avaliação de risco de cada uma das funções presentes na “*Function List*” • Nível de Implementação desejado na NIST *Framework* • Documento “Plano (Política) de Cibersegurança” • Objetivos de negócios e missão • Estratégia atual de Gestão de Riscos	• Lista das lacunas priorizadas com as potenciais consequências associadas • Documento “Plano de Ação Priorizado” com a lista das lacunas e das ações devidamente priorizadas para implementação	• Análise das lacunas entre o perfil atual e o alvo (“gap analysis”). • Avaliação das consequências decorrentes das lacunas existentes. • Determinação das lacunas que necessitam de atenção acrescida. • Identificação das ações que resolvem ou mitigam as lacunas. • Realização de uma análise custo-benefício (CBA) sobre as ações. • Priorização das ações a serem implementadas com base nas consequências das lacunas. • Elaboração de um documento com um plano que irá conter as ações priorizadas para combater as lacunas.

Tabela 25: Resumo dos tópicos abordados no passo 6 da Estratégia de Cibersegurança

Neste passo são identificadas e priorizadas as ações para cumprir com o que foi definido no plano de cibersegurança elaborado no passo anterior, pelo que é necessário comparar o “Perfil-Atual” (elaborado no passo 3) com o “Perfil-Alvo” (elaborado no passo 5) para determinar as lacunas/falhas (“*gap analysis*”). Conforme se pode observar na Tabela 25, o plano de ação a ser criado deve ser priorizado conforme as ações mais relevantes e urgentes para colmatarem as lacunas. Para isso, é importante que os responsáveis da organização e/ou das áreas cobertas pelo plano reúnam para discutirem quais as lacunas mais preocupantes e quais as ações necessárias para as combater.

Para isto ser possível, é necessário identificar todas as lacunas presentes no “Plano (Política) de Cibersegurança”, comparando o plano à avaliação atual efetuada no passo 3. Esse deve ser um processo fácil, uma vez que:

- Para o C2M2, é só verificar as lacunas identificadas no relatório do passo 3 e ver se alguma delas consta no plano de cibersegurança, sendo que para as restantes medidas é só necessário que seja verificada qual a avaliação alvo que lhe foi atribuída e comparar com os resultados do relatório C2M2 (por exemplo, se uma medida na avaliação atual está “*Largely Implemented*” e na avaliação alvo ela está “*Fully Implemented*”, então é considerada também uma lacuna a ser analisada);

- Para o caso do nível de implementação em práticas de gestão de riscos da NIST, é só observar as práticas que fazem parte do nível alvo e perceber quais é que não estão implementadas, o que já deve ficar automaticamente feito através do que foi referido anteriormente para o C2M2;

- Para o CIS *Controls* v8.0, também é simples através do uso do CIS CSAT. Deste modo, é só necessário comparar o que está no “Perfil-Alvo” com o *assessment* efetuado no passo 3. Parecido ao que acontece para o C2M2, para ser mais simples pode-se olhar para as lacunas identificadas conforme o critério definido no passo 3 e verificar se elas constam no plano de cibersegurança, pelo que para as restantes é só verificar se ficou decidido no “Perfil-Alvo” alguma melhoria à classificação obtida no passo 3;

- Para o resto das medidas que possam estar no “Plano (Política) de Cibersegurança” e não pertençam às anteriormente referidas, também não deve ser difícil identificar as que são lacunas, até porque se são de

outras fontes, é provável que sejam lacunas. Porém, as referências informativas recolhidas no passo 2 podem ajudar a perceber se as medidas já estão aplicadas ou foram decididas para aplicação só no passo 5.

Após se ter identificado as lacunas, tem de se atribuir uma prioridade de mitigação a cada lacuna. Para atribuir uma prioridade de mitigação a cada lacuna, deve-se ter em consideração [23]:

- As práticas atuais de gestão de riscos, espelhadas nos resultados do passo 3 (relatório C2M2, nível de implementação em práticas de gestão de riscos da NIST e o relatório CIS CSAT);
- O ambiente de risco atual, visível nos relatórios ou listas de riscos efetuadas no passo 4;
- Os requisitos legais e regulamentares identificados no passo 2;
- Os objetivos e missão de negócio identificada no passo 2;
- As restrições organizacionais ou de negócio aplicáveis identificadas no passo 2.

Por exemplo, se uma lacuna for uma medida que é obrigatória a empresa ter por lei implementada, então certamente a prioridade será maior que uma não obrigatória. Contudo, se uma lacuna tiver consequências muito graves, por exemplo, no âmbito do controlo de acessos da empresa ou for uma lacuna que tenha muitos riscos relacionados, então deve ter uma prioridade elevada. Como último caso, se houver duas lacunas no plano em que uma já está parcialmente implementada e outra não, então pode-se concluir que a que não está sequer começada requer uma atenção maior que a outra, porém depende do critério decidido pelos responsáveis. O objetivo final é que as lacunas fiquem priorizadas segundo a mitigação dos riscos ou consequências que estas apresentam para a organização.

Quando a análise da priorização das lacunas terminar, inicia-se a identificação das atividades de mitigação potenciais e a realização de uma análise custo-benefício (CBA) sobre essas ações potenciais. Aqui o importante é que as razões e análises custo-benefício efetuadas para as ações fiquem bem documentadas, uma vez que fica registado para a posteridade o motivo da escolha de certas ações em vez de outras. Por exemplo, se numa medida falar de cifragem de um certo tipo de dados, então uma das decisões será decidir o algoritmo a usar, pelo que se as razões não ficarem documentadas para a escolha de um algoritmo em vez de outros, será difícil que mais tarde se lembre o porquê dessa decisão.

Por fim, é necessário elaborar um documento com um plano de ações priorizado, com vista à mitigação das lacunas identificadas. O plano para colmatar as lacunas deve ter atribuído um responsável ou dono do plano (normalmente, um responsável com autoridade suficiente em cibersegurança na empresa ou alguém que este designou) que garante a sua concretização [24]. O dono do plano terá também a missão de definir os indicadores-chave de desempenho (KPI), ou seja, as formas de medir se as ações são efetivamente executadas conforme os objetivos que constam no “Plano de Cibersegurança” e no “Plano de Ação Priorizado”. O uso do C2M2 e do CIS CSAT já são uma boa forma de ter KPIs, mas podem ser utilizadas outras ferramentas que consigam abranger todas as medidas ou lacunas que constam no plano de ação. No “Plano de Ação Priorizado” devem estar principalmente elencadas todas as práticas, controlos ou medidas pela prioridade efetuada anteriormente e com as ações respetivas necessárias a serem feitas. Mais concretamente deve estar:

1. Enumeração das medidas por ordem de prioridade de implementação definida na priorização das lacunas;
2. Indicação da medida do “Plano de Cibersegurança” que está identificada como uma lacuna;

3. Apontadores ou referências para os documentos relativos à medida para ajudar na altura da implementação;
4. Descrição das ações decididas para colmatarem a lacuna, nomeadamente os métodos, ferramentas ou abordagens a serem usadas;
5. Identificação de cuidados ou ações extra que sejam necessários ter na aplicação das medidas, nomeadamente as KPIs que vão ser usadas e os motivos para se estar a tomar as ações em questão;
6. Referência à forma como a não implementação das ações pode afetar ou trazer consequências negativas para a empresa (necessária para efeitos de eventual análise/auditoria futura das ações tomadas).

Após a conclusão do "Plano de Ação Priorizado", é importante que este seja aprovado pela empresa, de modo a ser garantida a disponibilização dos recursos necessários (orçamento, pessoas com as competências necessárias para realizar as tarefas planeadas, etc.), eliminando assim potenciais obstáculos à sua implementação. Só depois se pode passar para a sua implementação (passo 7), que leva o estado da cibersegurança na empresa para o que foi definido na avaliação alvo (no "Plano (ou Política) de Cibersegurança"). Caso se considere que tem de haver alterações nas ações a serem efetuadas, pode-se voltar a este passo para redefinir o plano de ação, inclusive mudar a ordem de implementação das ações.

4.3.7 *Passo 7: Implementar/Aplicar o Plano de Ação*

Implementar/Aplicar o Plano de Ação (7.º Passo)		
Inputs	***Outputs***	**Iniciativas**
• Lista das lacunas priorizadas • Lista das potenciais consequências das lacuna • Documento "Plano de Ação Priorizado" com a lista das medidas/lacunas e respetivas ações devidamente priorizadas para implementação	• Dados de acompanhamento da implementação do plano	• Implementação das ações por prioridade. • Ir medindo o progresso das implementações relativamente ao plano, sendo que deve ser usada a ferramenta de autoavaliação C2M2, a ferramenta CIS CSAT, entre outras formas de medir o progresso (KPI's).

Tabela 26: Resumo dos tópicos abordados no passo 7 da Estratégia de Cibersegurança

No último passo desta estratégia de cibersegurança implementa-se o plano de ação, como mostra a Tabela 26. Deste modo, o dono do plano de ação deve garantir que as lacunas são fechadas, à medida que o plano de ação é aplicado, e que os riscos são monitorizados. Além disso, é recomendável que o dono do plano reporte aos executivos da empresa o estado de implementação para estes avaliarem o progresso.

Assim, as ações devem ser implementadas conforme a prioridade definida no passo 6, ou seja, pela ordem em que aparecem enumeradas no plano de ação. Para isso, devem ser atribuídas, por parte do dono do plano, responsabilidades de implementação das ações às pessoas ou equipas adequadas (por exemplo, equipa de cibersegurança, equipa de gestão de riscos corporativos, de gestão da segurança física, de gestão dos sistemas de informação, de programadores de *software*, de gestão de redes, entre outras). Quem tiver atribuída a tarefa de implementar uma ação, tem de cumprir com o estipulado nessa ação e deve reportar o desenvolvimento ou progresso ao dono do plano, sendo que ele próprio deve ter a iniciativa de garantir que está tudo a correr como planeado e validar o que é feito.

Para ajudar a monitorizar o progresso das implementações do "Plano de Ação", devem ser usadas as KPIs definidas no passo 6 e devem ser conduzidas periodicamente autoavaliações do estado atual em cibersegurança. Isto é relevante porque ajuda a perceber se as lacunas são fechadas devidamente, se o plano é seguido e se

as ações tornam a parte da empresa que está no âmbito mais próxima do "Perfil-Alvo". Para isto deve-se usar a ferramenta de autoavaliação C2M2 para, olhando para as lacunas identificadas no plano de ação, se verifique com as partes interessadas se já foram ultrapassadas. Adicionalmente, pode-se usar o CIS CSAT para medir o progresso da implementação dos subcontrolos da CIS versão 8 criando um *assessment* (esse progresso deverá ser adicionado aos subcontrolos por quem teve a responsabilidade de os implementar no âmbito do "plano de ação"). Desta forma, assim que forem concluídas as implementações, podem ser preenchidos os vários campos do subcontrolo em questão e o dono do plano pode validar as respostas dadas. O primordial aqui é que o dono do plano consiga garantir que o "Perfil-Alvo" é alcançado.

4.3.8 *Reavaliação do estado em cibersegurança*

Por fim, é fundamental referir que a qualquer momento pode ser considerado efetuar-se uma reavaliação do estado da cibersegurança, realizando uma nova iteração da presente estratégia de cibersegurança. Essa reavaliação deve ser efetuada periodicamente (prazo a definir pela empresa, mas que não deve ultrapassar os três anos), devendo também ser realizada sempre que ocorrer uma das seguintes situações:

- Grandes mudanças nos objetivos e missão de negócio da empresa;
- Grandes mudanças na tecnologia que possam tornar os controlos atuais inseguros;
- Mudanças no ambiente de ameaças, com o surgimento de novas ameaças que ponham em perigo a função e possam despoletar novos riscos de cibersegurança;
- Mudanças na indústria que podem obrigar a uma ação rápida em cibersegurança para que a empresa não fique para trás e perca vantagem competitiva.

4.4 NOTAS FINAIS

Para terminar, é importante deixar algumas considerações finais sobre a estratégia de cibersegurança apresentada. A estratégia, visível na Figura 6, tanto pode ser chamada *"roadmap"* ou *"lifecycle"*. Isto porque, como a estratégia tem um caráter cíclico, pode ser considerado o ciclo de vida da estratégia. Porém, também é um guia ou um "caminho" que mostra um conjunto de processos e passos necessários para a construção de um plano estratégico.

Esta estratégia baseou-se num conjunto de recomendações de *frameworks*, *standards*, controlos, *guidelines* entre outras recomendações de fontes relevantes em cibersegurança, porque era importante usar algo credível, com referências bastante usadas e internacionalmente aceites pela comunidade. Contudo, existem muitas partes que são de autoria própria por se julgar ser o mais indicado a ser feito, ou então para simplificar ou enriquecer o processo. Teve-se também o cuidado de usar muitas fontes de informação para que não existam informações erradas e para que quem estiver a usar esta estratégia consiga ter a informação que precisa para aplicá-la.

É ainda relevante referir que esta estratégia não necessita de ser tão rígida como parece, ou seja, não precisa de ser seguida exatamente a ordem dos passos sem ser possível recuar uns passos. Deste modo, se quem estiver a seguir o *"roadmap"* acreditar que as coisas não estão bem definidas ou concluídas num determinado passo, então pode regressar ao passo necessário para redefinir o que for necessário. Principalmente, no passo 1 e 2, como são estágios iniciais, é normal que não fique logo tudo definido à primeira, principalmente se for a primeira vez a usar a estratégia.

Um aspeto fundamental a ter em conta são as características da estratégia: periódica, reproduzível, contínua, iterativa, abrangente e com uma estrutura tal que permite a melhoria a cada ciclo das capacidades de cibersegurança e gestão de riscos de cibersegurança. De realçar que se houverem mudanças significativas que alterem completamente o ambiente organizacional, principalmente relativamente a riscos, então em qualquer passo pode ser necessário regressar ao passo 1 para iniciar o processo de novo. Por outro lado, mesmo que não aconteçam mudanças, deve estar definido um período entre iterações do ciclo da estratégia. Consoante aquilo que é aceitável pela comunidade de cibersegurança, o prazo para se iniciar uma nova reavaliação vai de 1 até 3 anos, dependendo dos serviços praticados e do que for decidido pelos executivos da organização.

É importante também reforçar que o tempo que vai desde a avaliação atual até à avaliação alvo não pode ser muito longo, uma vez que com as mudanças que acontecem na tecnologia, na organização, no ambiente de riscos, entre outras, fazem com que, em caso de demora, as avaliações não sejam tão precisas e possam causar o efeito de ilusão da realidade da gestão dos riscos de cibersegurança. Claro que se o responsável (ou responsáveis) pela implementação da estratégia tiverem um grande conhecimento do âmbito em causa, conseguem identificar melhor as eventuais mudanças que possam alterar as avaliações efetuadas até ao momento.

Outro aspeto fundamental no âmbito da estratégia de cibersegurança é a lista de funções da empresa que estão nesse âmbito (*"Function List"*). O objetivo para quem usa esta estratégia é que todas as áreas da empresa sejam cobertas pelo plano ou política de cibersegurança. Porém, dependendo da dimensão da organização, pode ser muito difícil numa primeira iteração da estratégia abordar com precisão todas as áreas da empresa. Nesse caso é preferível começar por uma porção da organização, até pode ser a mais crítica, e depois aumentar o âmbito em sucessivas iterações do plano de cibersegurança, até que se chegue a um ponto em que toda a empresa já faz parte da estratégia. Por outro lado, pode-se usar a estratégia em simultâneo para âmbitos diferentes, o que poderá ser mais simples se estivermos a falar de grandes corporações.

Em relação à possibilidade do plano de cibersegurança se tornar política, isto acontece porque este plano tem todas as condições necessárias para ser uma política empresarial. Como hoje em dia se aconselha a que as empresas tenham políticas de cibersegurança, além das políticas da segurança da informação, mesmo para questões de formalização das práticas aplicadas na organização, esta estratégia oferece também uma forma de se desenvolver uma política de cibersegurança. Além da política, esta estratégia produz vários documentos e relatórios relacionados com a cibersegurança e gestão de riscos de cibersegurança, tornando o processo de análise mais fácil e com evidências daquilo que é feito. Estes documentos são úteis para processos de auditoria, aumento da transparência através da disponibilização do conhecimento das práticas de cibersegurança a todas as partes interessadas, para demonstração das capacidades de cibersegurança, e para uma melhor gestão da cibersegurança e dos riscos associados.

Por último, é muito importante que a cultura de cibersegurança esteja continuamente presente na cabeça de todos os colaboradores, pois, isso é um dos maiores fatores de sucesso desta estratégia. Se todos os colaboradores cooperarem na aplicação da estratégia e no cumprimento das ações espelhadas nos planos, então será mais fácil mitigar os riscos de cibersegurança a que a empresa está sujeita e fazer com que ataques informáticos tenham uma menor probabilidade de terem sucesso. Daí também ser fundamental que a empresa se mantenha sempre informada das tendências nesta área e procure sempre buscar as últimas atualizações. O segredo de qualquer plano estratégico são a união interna, a constante atenção ao mundo que nos rodeia, a paciência e perseverança, a perceção plena do contexto empresarial, o estabelecimento de metas/objetivos e a existência de planos de atuação eficazes.

5

APLICAÇÕES

5.1 INTRODUÇÃO/CONTEXTUALIZAÇÃO

Após apresentada a contribuição teórica desta dissertação (capítulo 4), através da descrição dos passos da estratégia de cibersegurança desenvolvida, neste capítulo descreve-se uma aplicação real do resultado principal desta dissertação numa empresa portuguesa, nomeadamente a Imprensa Nacional — Casa da Moeda (INCM). Esta dissertação insere-se no âmbito da criação de uma estratégia de cibersegurança para a INCM, pelo que serão mostrados alguns exemplos e casos de estudo relativos à implementação dos passos do *"roadmap"* (Figura 6) na INCM.

Desde o início, a implementação da estratégia de cibersegurança foi acompanhada pelo *Chief Information Security Officer* (CISO), e por vários departamentos, entre os quais o da gestão de riscos corporativos e o de sistemas da informação, que deram sempre contributos valiosos para o desenvolvimento da estratégia de cibersegurança assim como para a sua aplicação na INCM.

Numa primeira fase, foram efetuadas um conjunto de reuniões regulares para haver a contextualização necessária do ambiente organizacional da empresa. Depois, a aplicação da estratégia de cibersegurança foi feita de uma forma gradual para que todos se ambientassem a esta nova forma de olhar para a cibersegurança. A ambição inicial da INCM era aplicar a estratégia de cibersegurança a toda a organização, mas rapidamente se concluiu que deveria ter um âmbito menor. Este facto deve-se ao elevado número de serviços geridos e disponibilizados pela INCM, assim como à complexidade de cada um e à sua diversidade.

Durante a implementação da estratégia na INCM, foram produzidos um grande conjunto de documentos e relatórios relativos aos vários passos da estratégia. Esses documentos foram fundamentais na elaboração da estratégia, desde os relatórios do estado atual em cibersegurança até ao "Plano de Cibersegurança" e o "Plano de Ação Priorizado", estando todos os documentos a ser usados atualmente na organização. Inclusive, foi decidido pelos responsáveis da INCM que o plano desenvolvido no passo 5 dever-se-ia tornar na política de cibersegurança da organização, para o âmbito definido. No futuro, o âmbito da estratégia irá ser aumentado, tendo por objetivo ser aplicada a toda a empresa.

Note-se que todos os documentos ou extratos mostrados neste capítulo são atualmente usados e estão em vigor na INCM. O objetivo é que o leitor entenda a utilidade e facilidade do uso desta estratégia, mas também perceba que o seu âmbito poderá começar por alguns serviços e ir aumentado até que se aplique a toda a empresa. Não se pode esperar que algo que é novo seja logo introduzido na empresa de uma vez. O processo deve ser gradual, simplificado, eficaz e iterativo para serem combatidas logo à partida as principais debilidades e com o tempo se alargue a área de ação da estratégia. De salientar que, para o tempo disponível e tendo em conta algumas restrições impostas durante a execução deste projeto, consegui-se obter bons resultados, o que não significa que outras empresas que usem esta estratégia consigam logo obter resultados semelhantes. Facilitou imenso o facto

de a empresa já ter muitos processos desenvolvidos, principalmente na área da segurança da informação, o que permitiu a reutilização de informação que doutro modo teria que ser criada.

Deste modo, a seguir são descritos todos os passos da implementação da estratégia na INCM. Contudo, deve-se referir que não foi permitido a apresentação de informação restrita/confidencial, embora tenha sido permitido utilizarem-se alguns excertos. Todos os excertos divulgados nesta dissertação foram devidamente autorizados pelos responsáveis. A prioridade é mostrar uma aplicação prática como complemento extra à estratégia desenhada nesta tese, estando assegurada que a informação apresentada é mais que suficiente para garantir o objetivo deste capítulo.

5.2 PASSO 1: DEFINIR AS PRIORIDADES E O ÂMBITO DA ESTRATÉGIA

A implementação prática do conteúdo desta dissertação de mestrado na organização supracitada começou pelo passo 1 da estratégia de cibersegurança, seguindo a secção 4.3.1. Neste primeiro passo, foi fundamental conhecer bem o ambiente da instituição, os processos empresariais e principalmente como a empresa lidava com a cibersegurança e geria os seus riscos.

Deste modo, foram analisados vários documentos empresariais que ajudaram a entender o contexto da empresa e quais deveriam ser as prioridades e âmbito da estratégia. Através do organograma da INCM, conseguiu-se perceber quais os vários departamentos que a constituem e de que forma estão distribuídas as responsabilidades por cada área. No topo está o conselho de administração, seguido dos departamentos de coordenação estratégica, auditoria interna, CISO, produção, riscos corporativos, suporte, recursos humanos, entre outros. Além disso, a INCM é uma organização pública que, como atua na área dos serviços de confiança, necessita de ter sempre grandes preocupações não só com a segurança da informação, mas também com a segurança física. Além da cunhagem da moeda e medalhas, possuí mais uma variedade de serviços distintos, tais como:

- As contrastarias;
- A imprensa nacional;
- A biblioteca e as lojas de venda de livros e com áreas numismáticas;
- O museu da casa da moeda;
- As publicações do diário da república (DRE);
- A gráfica de segurança que produz documentos com elevadas preocupações de segurança, tais como os de identificação (cartão de cidadão), hologramas, certificados, cartões bancários, entre outros;
- Gestão de infraestruturas de chave pública (PKI) e outros de serviços qualificados de confiança.

Muito resumidamente, estes são os serviços da INCM, cada um deles com as suas especificidades e complexidades, e todos eles muito diversos. Após esta análise inicial foi decidido que era demasiado complexo elaborar uma estratégia de cibersegurança que abrangesse simultaneamente todos estes serviços, pelo que se optou por reduzir o âmbito desta primeira iteração da estratégia, e aplicá-la ao serviço de PKI do Cartão de Cidadão. Esta decisão foi tomada porque havia por parte da equipa orientadora um elevado conhecimento dos processos desse serviço, para além de ser um serviço essencial da INCM que não pode falhar, conforme os objetivos/missão de negócio, pelo

que a inserção formal (ou formalizada) da cibersegurança nos processos relacionados à PKI é fundamental para o sucesso da infraestrutura.

Assim, após se ter chegado a esta decisão, na *"Function List"* ficou só aquilo que está relacionado com a PKI do CC, nomeadamente as áreas envolvidas e dependências que existem de entidades externas. Para preservar a confidencialidade, as operações no âmbito da estratégia não irão ser muito especificadas nesta tese, mas todas estão relacionadas à PKI do CC.

Definido o alcance ou âmbito da estratégia, passou-se à definição das prioridades alto-nível da estratégia de cibersegurança. Como esta estratégia nunca tinha sido seguida e estávamos na primeira iteração, foi necessário definir as prioridades estratégicas do início. Para isso, foi necessário entender quais os objetivos da organização para a PKI e recolher informações dos responsáveis para perceber aquilo que é mais crítico e se planeia proteger. Toda a informação já existente em documentos como políticas, requisitos e referências informativas também foram fundamentais nesta fase, tais como a política de segurança da informação, a política de riscos da PKI e os vários planos e processos formalmente documentados da infraestrutura. De um modo geral, as metas e objetivos definidos refletem aquilo que são as intenções de melhoria das capacidades de cibersegurança da INCM, mas com foco na PKI do CC. De salientar que são alto-nível, pelo que só servem para relatar de forma clara aquilo que são os objetivos em cibersegurança para a infraestrutura de chave pública do cartão de cidadão.

As metas foram redigidas num documento à parte, uma vez que estes são objetivos relacionados à estratégia de cibersegurança e não propriamente ao "Plano (ou Política) de Cibersegurança". Porém, com o tempo pode ser decidido que seria interessante que houvesse um capítulo no "Plano (ou Política) de Cibersegurança" que enumerasse as prioridades estratégicas. Um conjunto de prioridades da estratégia de cibersegurança foram definidos inicialmente. Como seria extenso colocar todas as prioridades, a seguir será apresentada uma das prioridades alto-nível da estratégia de cibersegurança da INCM, com a respetiva meta e objetivos associados:

- **META**: Proteger a informação e os sistemas de informação relativos à PKI do CC para assegurar que a confidencialidade, integridade e disponibilidade de toda a informação seja proporcional às necessidades da missão, ao valor da informação e às ameaças associadas.
  - **Objetivos**:
    - Reduzir o risco de perda, divulgação não autorizada, acesso de indivíduos não autorizados a dados confidenciais ou modificação não autorizada de informações e sistemas de informação.
    - Garantir a segurança de todos os dados sensíveis (em repouso e em trânsito), através de técnicas avançadas de autenticação, de autorização e de proteção.
    - Garantir que as obrigações e recomendações descritas na "Política de Segurança da Informação" são cumpridas para ser também reforçada a cibersegurança.
    - Estabelecer e manter uma arquitetura de cibersegurança empresarial que proteja a informação.
    - As políticas e as orientações são adaptáveis para atender às necessidades da missão em mudança e alinhadas com as ameaças.
    - Todos os sistemas e redes são capazes de defesa através do reconhecimento dinâmico e resposta a ameaças, vulnerabilidades e anomalias.
    - Garantir a disponibilidade da informação através de mecanismos como cópias de segurança (*backups*) ou redundância de sistemas.
    - Implementar soluções de cibersegurança em toda a INCM.

Com base nestas prioridades, foi possível começar a pensar na estrutura do "Plano de Cibersegurança", tendo-se definido os pilares estratégicos, garantindo que têm por base as várias prioridades que foram redigidas, de tal modo que consigam abranger todas as áreas abordadas nas prioridades. Se as várias metas e objetivos das prioridades forem analisadas com cuidado, é possível distinguir algumas áreas distintas ou que se julgam que devem ter um capítulo próprio no plano. Como é referido na secção 4.3.1, os pilares estratégicos vão de encontro ou promovem as prioridades da estratégia de cibersegurança. Assim, tendo em conta as características dos pilares estratégicos, o âmbito e as prioridades da estratégia, os capítulos da política de cibersegurança que foram decididos nesta primeira iteração da estratégia foram os seguintes:

1. Análise e Gestão de Riscos (Nota: a gestão de riscos de cibersegurança é o pilar base de toda a estratégia);
2. Cultura de Cibersegurança (Formação e Sensibilização);
3. Segurança da Informação (Nota: apesar de ser mais abrangente que a cibersegurança, foi decidido que deveria ser um pilar estratégico porque é relevante para a diminuição de riscos de cibersegurança que a segurança da informação seja garantida);
4. Segurança de Redes;
5. Prevenção contra *Software* Malicioso (*malware*);
6. *Hardening* de Segurança (configuração segura de sistemas, atualização de *software*, etc.);
7. Monitorização (atividades relacionadas a monitorização/deteção de eventos, anomalias, incidentes, vulnerabilidades, ameaças, etc.);
8. Gestão/Controlo de Acessos;
9. Mobilidade Empresarial (BYOD, CYOD, etc.);
10. Gestão de Ativos;
11. Segurança de Aplicações de *Software*;
12. Gestão de Incidentes;
13. Cadeia Logística/de Abastecimento (gestão dos riscos das terceiras partes);
14. Trabalho Remoto/em casa.

Por último neste passo, foi efetuada a definição alto-nível das responsabilidades em cibersegurança de cada departamento da INCM. Esta tarefa, que era opcional, acabou por ser realizada para todas as áreas da INCM, o que não era necessário tendo em conta o âmbito da estratégia. Porém, decidiu-se que era importante fazer esse trabalho para ter já documentadas essas responsabilidades, mesmo que na política só venham a constar, por enquanto, as responsabilidades associadas à PKI do CC. Para isso foi analisado com atenção o organograma da empresa e, como já existem documentadas as responsabilidades de cada departamento, foi necessário recolher aquelas que tinham relação com a cibersegurança e acrescentar outras que se achou serem pertinentes. Para esta tarefa, foi muito relevante contar com o apoio da equipa do CISO que ajudaram a perceber as responsabilidades em cibersegurança de cada uma das áreas. O objetivo final em se ter as responsabilidades de todas as áreas já documentadas foi

o de enfatizar a importância de todos os departamentos no reforço da cibersegurança da INCM, pelo que desta forma nenhum dos departamentos foi excluído desta listagem de responsabilidades. É de referir que, em todas as áreas, existe a responsabilidade de zelar por um ambiente mais ciberseguro na empresa, já que grande parte dos ataques que acontecem nas organizações são oriundos de erros ou descuidos por parte de colaboradores/parceiros da empresa.

Assim, ficou concluído este passo 1 da estratégia, sendo que houve momentos durante a implementação em que foi necessário regressar a este passo porque se julgou que algumas coisas não estavam bem definidas ou então era necessário repensar certos aspetos. Por exemplo, foi necessário regressar após o passo 3 devido às prioridades da estratégia e após o passo 5 devido aos pilares estratégicos.

5.3 Passo 2: Identificar os recursos, requisitos e regulamentação no âmbito da estratégia

No 2.º passo da estratégia, foi necessário identificar os ativos, sistemas, mapas/arquiteturas de rede, requisitos de cibersegurança e as referências informativas no âmbito escolhido no 1.º passo. Neste passo, o responsável da estratégia deve recolher ou juntar o máximo de informações possíveis e que possam ser úteis para o sucesso da estratégia.

Em primeiro lugar, foram analisados todos os documentos associados à PKI do CC, sendo que a documentação é muito extensa e com bastante nível de detalhe. Na verdade, como se reduziu o âmbito para a PKI, foi mais fácil efetuar este passo, pois existe um grande conjunto de documentos formais escritos que fizeram com que só fosse mesmo necessário juntar a informação relevante. Contudo, é de lembrar que isto nem sempre acontece, pelo que poderia ser necessário elaborar essa documentação, principalmente a relacionada com os ativos e sistemas.

No que diz respeito a listar sistemas e ativos na PKI do CC, esta lista já era devidamente elaborada e atualizada com regularidade, sendo já efetuada uma separação por grupos ou tipos de ativos. Existe também uma política de gestão de inventário que define os vários atributos que este deve ter, além dos grupos nos quais os ativos devem ser separados. A separação por grupos de ativos pode, dependendo do grupo, ter atributos adicionais que especificam ou detalham ainda mais cada recurso. A seguir encontram-se alguns dos grupos de ativos mais relevantes para o desenvolvimento da estratégia de cibersegurança que constam no inventário de ativos da infraestrutura de chave pública do cartão de cidadão:

- Ambientes;
- Acessórios de *hardware* criptográfico;
- Acessórios de *hardware*;
- *Hardware* criptográfico;
- *Hardware*;
- *Software*;
- Ficheiros;
- Mídia;
- Recursos humanos;

- Sistemas de suporte.

Após a identificação dos ativos e sistemas, procedeu-se à identificação do mapa/arquitetura de rede da infraestrutura. Essa informação já existia, o que fez com que não fosse necessário elaborar um mapa ou arquitetura para este âmbito da estratégia, sendo constituída por diferentes visões da infraestrutura, onde se pode constatar o posicionamento das *firewalls*, servidores de base de dados, servidores de *frontend* e *backend*, *switches*, entre outros componentes que fazem parte da PKI. São bem visíveis as ligações externas, nomeadamente serviços que acedem à PKI, e pode-se observar a separação existente entre os vários subsistemas (*"trust-boundaries"*), onde muda o grau de confiança entre cada um. A política para a arquitetura de redes, também já existente, detalha as várias obrigações e cuidados que se devem ter nesta matéria.

Por último, juntou-se a documentação mais relevante que pode ajudar na implementação da estratégia de cibersegurança para a PKI do CC. Começando pelos requisitos de cibersegurança (regulamentares e organizacionais) e os de negócio, a INCM já possuí muita documentação, nomeadamente regulamentação (europeia e nacional), assim como políticas, planos, regras e processos organizacionais. A maior dificuldade foi perceber até que ponto todos esses documentos eram relevantes para a cibersegurança ou para o decorrer da estratégia de cibersegurança. Como o serviço da PKI do CC tem por base muitos processos digitais e relacionados aos serviços de confiança, considerou-se que maior parte da documentação é relevante e deve ser identificada para uso nos próximos passos da estratégia. Os documentos de requisitos, que existem na INCM para a PKI, selecionados neste passo da estratégia são os seguintes:

1. **Políticas** — Algumas das políticas mais importantes consideradas neste passo foram: Ambientes, Arquitetura, Controlos Criptográficos, Certificados da EC do CC, Fornecedores, Gestão de Alterações, Recursos Humanos, Segurança de Informação, Gestão de Incidentes, Registo de Auditoria e Monitorização, Gestão de Risco, Gestão de Inventário, Identificadores (OIDs), *Backups*, *Disaster Recovery*, etc.;

2. **Regras** — Nas regras, foram consideradas as regras organizacionais definidas para os vários grupos de trabalho que atuam na infraestrutura, ou seja, a definição de responsabilidades/funções atribuídas a estes;

3. **Planos** — Alguns dos planos que existem documentados e que são úteis durante a implementação da estratégia: Auditoria Interna, Formação, Tratamento de Risco, etc.;

4. **Processos** — Alguns dos processos selecionados foram: Gestão de Riscos, Gestão de Incidentes (Notificação, Resposta, Registo, etc.), Alterações na Infraestrutura, etc.;

5. ***"Compliance"* (regulamentação)** — Foram considerados alguns requisitos regulamentares, tais como, por exemplo, os regulamentos europeus do eIDAS para *Electronic Signatures and Infrastructures* (ESI), a legislação nacional, como o decreto-lei n.º 12/2021 que assegura o cumprimento do regulamento (UE) 910/2014 sobre identificação eletrónica e serviços de confiança para transações eletrónicas no mercado interno e o regulamento geral de proteção de dados (RGPD) [22];

6. ***"Service Level Agreements"* (SLAs)** — Os níveis de serviço considerados foram os relatórios que são efetuados todos os meses para os vários serviços inseridos no âmbito da PKI. Todos estes relatórios são úteis, pois, dão a conhecer as prioridades de negócio associadas à satisfação dos clientes. A tomada das decisões e priorização das ações deverá ter em conta estes SLA's.

A par da documentação, foram também identificadas as referências informativas (normas, ferramentas, *frameworks*, boas práticas de cibersegurança e gestão de riscos, etc.) seguidas e aplicadas à PKI do CC. Basicamente,

são documentos ou publicações de referência seguidos pelo âmbito para haver uma maior segurança, mas que não são um requisito obrigatório ou não são exigidos pela "lei". Alguns exemplos das referências informativas identificadas são:

- IETF — RFC 3647 *Internet* X.509 *Public Key Infrastructure — Certificate Policy and Certification Practices Framework* [81];
- Política de Certificados do SCEE (Sistema de Certificação Eletrónica do Estado) e Requisitos Mínimos de Segurança [103];
- ETSI EN 319 401 V2.3.1, *"Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers"* [38];
- ETSI EN 319 411–2 V2.2.2, *"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates"* [40];
- ETSI EN 319 411–1 V1.2.2, *"Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements"* [39];
- ETSI EN 319 421 V1.1.1, *"Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps"* [37].

No que diz respeito somente a reforço das práticas de cibersegurança, já eram seguidas algumas referências informativas, como, por exemplo, os relatórios da ENISA, o Quadro Nacional de Referência para a Cibersegurança (QNRCS) [11], alguns *standards* do ISO, como o ISO 27002:2013 [46], o ISO 17825:2016 [53], o ISO 27035-1:2016 [56], o ISO 27035-2:2016 [57] e o ISO 31000:2018 [60].

5.4 Passo 3: Avaliar a Situação Atual da Cibersegurança

Após a identificação da informação sobre ativos e documentos existentes no âmbito da estratégia, deu-se início à avaliação da situação atual em cibersegurança. Este passo foi crucial para perceber em que ponto em cibersegurança a PKI do CC se encontrava e quais os processos de gestão de riscos de cibersegurança que estavam a ser aplicados.

Em primeiro lugar, para se começar a decidir qual o "Perfil-Atual", é necessário responder às perguntas do questionário de autoavaliação C2M2. Note-se que antes de abordar somente a PKI do CC, foi feita uma primeira tentativa de resposta ao questionário com várias pessoas diferentes da INCM. Aqui foi usada a abordagem de "entrevistar" em cada domínio do C2M2 as pessoas que tinham as responsabilidades e o conhecimento sobre o assunto. Nessa primeira tentativa, foram analisadas áreas que não atuam diretamente no âmbito, uma vez que o âmbito numa primeira fase era para ser mais abrangente, como já foi referido no passo 1.

Na segunda abordagem ao questionário do C2M2 foi só analisada a PKI do CC, ou seja, o âmbito que se encontrava na *"Function List"*. Neste caso, como o número de responsáveis não era elevado e todos possuíam um grande conhecimento e experiência no âmbito em questão, foram reunidos os principais responsáveis pela PKI e realizado em conjunto a resposta às perguntas, o que diferiu da primeira abordagem. Esta abordagem permitiu houvesse um maior consenso entre todos sobre o estado atual em cibersegurança que era espelhado no questionário, tornando os resultados mais confiáveis e condizentes com a realidade. Note-se que foram feitas reuniões durante aproximadamente duas semanas para que o questionário de autoavaliação ficasse concluído.

Para a resposta às perguntas do questionário, foi usada a versão em PDF, por uma questão de conveniência. Assim que ficaram respondidas todas as práticas do C2M2, foi gerado o relatório final com a análise às respostas dadas durante o *"workshop"*. O resultado, como era expectável desde o início, foi bastante positivo, tendo em conta o nível de segurança existente neste serviço. Nas figuras 12 e 13 são mostrados dois excertos do questionário antes de ser gerado o relatório final e, nas figuras 14 e 15 são apresentados excertos do relatório gerado. Seria interessante mostrar outra informação útil gerada no relatório, como outros gráficos ou os resumos das lacunas, mas esse tipo de informação foi considerada confidencial.

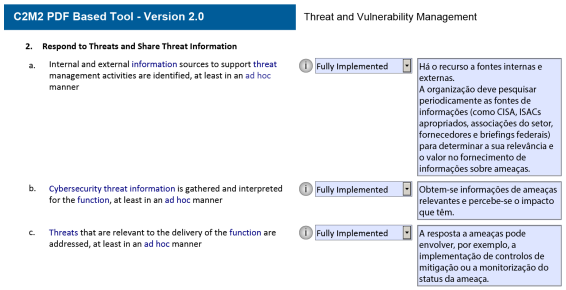


Figura 12: Respostas e notas dadas a algumas das práticas presentes no domínio *THREAT* (Gestão de Ameaças e Vulnerabilidades) do C2M2

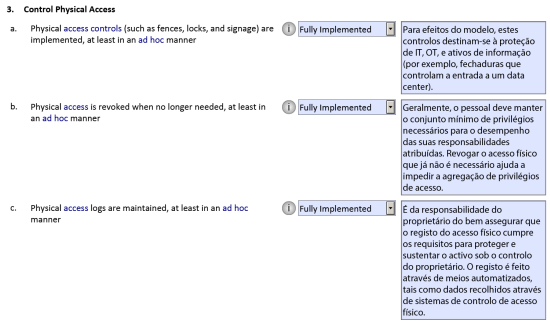


Figura 13: Respostas e notas dadas a algumas das práticas presentes no domínio *ACCESS* (Gestão e Controlo de Acessos) do C2M2

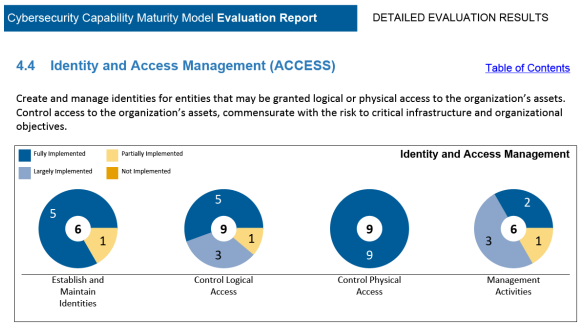


Figura 14: Excerto de um gráfico gerado para o domínio *ACCESS* do C2M2, com um resumo por objetivo das respostas dadas

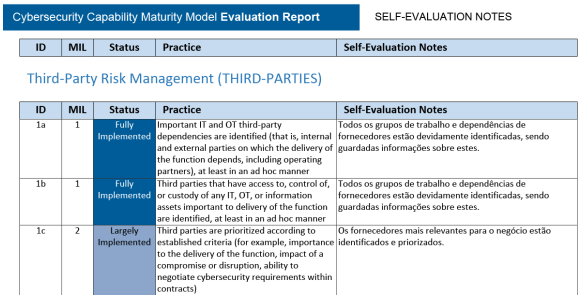


Figura 15: Excerto dos resultados da autoavaliação feita com o C2M2

Após se ter realizado a análise da maturidade em cibersegurança com o C2M2, foi altura de relacionar estes resultados com a NIST *Framework*, mais propriamente com os níveis de implementação das práticas da NIST CSF para gestão de riscos. Com o recurso às tabelas da Figura 8, foi mais simples identificar o nível de implementação, uma vez que foi só comparar os resultados do relatório do C2M2 com o mapeamento feito nessas tabelas. Desta forma, o nível obtido tem por base todas as práticas implementadas de forma "completa" ou "largamente", que estão mapeadas no nível obtido e nos níveis anteriores a esse nível. Claro que a descrição dos vários níveis de implementação também ajuda a perceber em que ponto o âmbito se encontra, mas desta forma consegue-se tornar o processo mais fácil e preciso.

Após se obter o nível de implementação, passou-se à análise de quais as práticas dos CIS *Controls* v8.0 é que eram aplicadas na PKI do CC. Ou seja, seguindo as recomendações da secção 4.3.3, foi usado o CSAT para selecionar todos os grupos de implementação (IGs) para se conseguir analisar cada um dos subcontrolos. Desta forma, consegue-se perceber o grau de implementação de cada subcontrolo tendo em conta os 4 critérios definidos

no CSAT. Esta autoavaliação foi respondida em conjunto pelos responsáveis de segurança da PKI do CC. Mas antes de se responder, foi decidido pelos responsáveis de segurança da PKI que se deveria considerar lacuna um subcontrolo com um *score* inferior a 75%, e não os 50% recomendados na secção 4.3.3. É importante que se responda a este questionário porque dá uma visão mais prática sobre os processos que podem estar implementados na empresa, sendo que são dadas até sugestões de ferramentas a utilizar. Muitos controlos vão ao encontro do que está no C2M2, mas outros diferem, tornando as análises da situação atual e da posterior escolha do "Perfil-Alvo" no passo 5 mais completas e refinadas.

Após se ter respondido aos vários subcontrolos do CIS, é possível gerar vários tipos de relatórios em diferentes formatos (PDF, *Excel* e *PowerPoint*) para uma melhor análise dos resultados. Nesses relatórios, podem ser encontradas as respostas às várias perguntas, análises dos resultados por controlo ou até gráficos com a visão das respostas dadas, além do desvio que existe em relação à média da indústria. Tal como nos casos anteriores, não podem ser mostrados todos os resultados nem esses gráficos, mas o resultado foi muito satisfatório e está acima da média da indústria. Como exemplo, na Figura 16 é apresentado um excerto do relatório PDF com os resultados apresentados para o controlo *"Access Control Management"*, onde é visível o resultado positivo das respostas através da diferença existente entre a percentagem da média dos controlos (88) com a média da indústria (30). Nas figuras 17 e 18 pode-se observar dois exemplos das respostas dadas durante o *assessment* no CIS CSAT.

Figura 16: Excerto do relatório PDF do CIS CSAT para o controlo *"Access Control Management"*

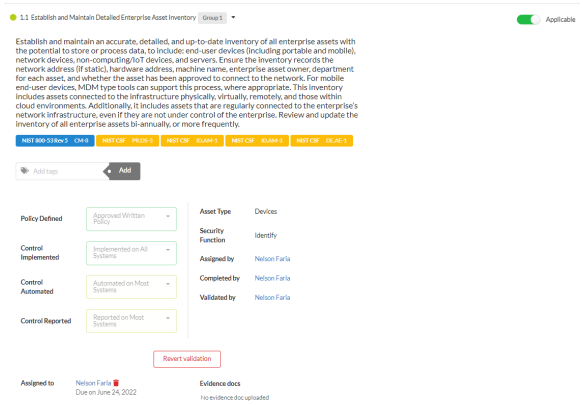


Figura 17: Resultado da análise da situação atual feita para o subcontrolo "Estabelecer e manter um inventário de ativos empresariais detalhado" (CIS *Controls* v8.0 — subcontrolo 1,1)

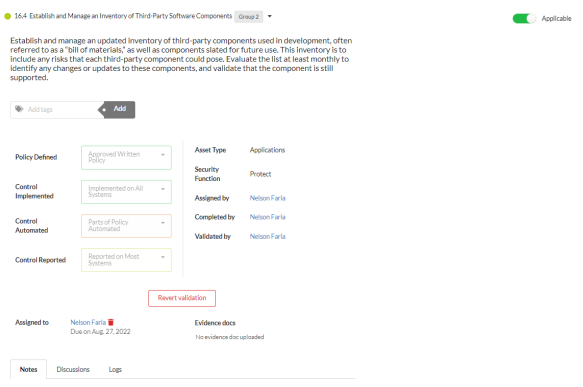


Figura 18: Resultado da análise da situação atual feita para o subcontrolo "Estabelecer e gerir um inventário de componentes de *software* de terceiras partes" (CIS *Controls* v8.0 — subcontrolo 16,4)

Reunindo toda a informação obtida através das várias tarefas deste passo, foi possível obter-se um estado ou perfil atual em cibersegurança e em gestão de riscos de cibersegurança para o âmbito que consta na *"Function List"*.

5.5 PASSO 4: EFETUAR AVALIAÇÕES DE RISCO DE CIBERSEGURANÇA

Neste passo 4, o objetivo foi avaliar os riscos de cibersegurança a que o âmbito poderia estar sujeito. Em cibersegurança, a possibilidade de acontecerem incidentes resultantes de riscos não documentados e/ou não controlados é algo persistente e o mais certo é que maior parte dos riscos nunca desapareçam. Ter os riscos documentados e decidir as melhores medidas e controlos que os mitiguem ou eliminem, é um dos principais objetivos desta estratégia.

Relativamente às iniciativas efetuadas neste passo, como já se conhecia o estado atual em cibersegurança (passo 3) e, por consequência, sabia-se que a gestão de riscos é algo que está bem presente neste âmbito, foi mais fácil desenvolvê-las. Maior parte dos riscos de cibersegurança a que a PKI está ou estava sujeita já se encontravam identificados, pelo que foram extraídos para um documento *Excel* criado para conter só riscos de cibersegurança, conforme o proposto pela estratégia desta dissertação. Este documento *Excel* contém vários campos que fazem parte da estratégia de gestão de riscos utilizada e ainda uns campos extra para conter as ameaças, vulnerabilidades e fontes de risco associadas. Além dos riscos, estão também documentados os controlos atuais que são aplicados para mitigar ou eliminar esses riscos, o que simplificou mais a análise.

Os riscos de cibersegurança foram devidamente revistos e completados de acordo com certos aspetos que foram identificados ao longo da análise, feita em conjunto com os responsáveis pela PKI. Além disso, muitas das ameaças, vulnerabilidades e fontes de riscos foram identificadas segundo o critério descrito no ISO/IEC 27005:2018 [61]. Nesta fase, os resultados do passo 2 foram muito importantes, pois com eles conseguiu-se identificar os riscos a que os ativos e sistemas que constituem a infraestrutura estavam sujeitos através do recurso às características de cada ativo e ainda ao mapa/arquitetura de rede da PKI do CC.

Relativamente à metodologia de gestão de riscos que foi seguida, recorreu-se à estratégia que já era utilizada na PKI do CC, para avaliar riscos. Deste modo, não foi usada a proposta apresentada na secção 4.3.4, uma vez que foi decidido que o mais indicado seria continuar a seguir a mesma metodologia usada para a gestão de riscos da PKI. O facto de se estar a usar outra metodologia também vai ao encontro do que é referido na estratégia, ou seja, é possível usar-se a estratégia de gestão de riscos mais conveniente para o âmbito em questão, havendo essa flexibilidade, sendo o mais relevante que permita identificar completamente os riscos em conjunto com as ameaças e vulnerabilidades correspondentes.

A metodologia usada para gestão de riscos de cibersegurança no âmbito da PKI do CC consiste numa escala de classificação de 4 níveis para impacto, probabilidade e risco, em vez dos 5 propostos na secção 4.3.4. Referindo somente as diferenças para a abordagem dessa secção, são avaliadas a confidencialidade, integridade e disponibilidade com base na classificação de 4 níveis, mas também inclui a autenticidade e o não-repúdio. Porém, o cálculo do impacto é feito com base também na criticidade do risco, ou seja, o impacto que o risco em questão poderia ter no RTO (*"Recovery Time Objective"*) ou RPO (*"Recovery Point Objective"*) de sistemas/aplicações. Desta forma, o impacto é igual à multiplicação da criticidade pelo máximo entre as várias classificações atribuídas à confidencialidade, integridade, disponibilidade, autenticidade e não-repúdio (CIDAN), como se pode constatar na equação (2).

$$Impacto(I) = (Criticidade) \times (MÁXIMO(CIDAN)) \tag{2}$$

Assim, as classificações que podem ser dadas a cada um dos parâmetros do risco são:

- **Confidencialidade**: **0** — Não Aplicável; **1** — Em claro para todos dentro e fora da organização; **2** — Para uso interno; **3** — Acesso restrito numa base de conhecimento dentro de grupos ou equipas de trabalho. A sua divulgação pode causar alguns danos limitados; **4** — Restrito a um indivíduo ou grupo limitado cujo acesso não autorizado pode provocar danos elevados;
- **Integridade**: **0** — Não Aplicável; **1** — Sem impacto — a integridade não tem importância no sentido de que não causa nenhum impacto direto no âmbito de proteção; **2** — Pouco impacto — As modificações têm pouco impacto, por exemplo, afetará apenas documentação, procedimentos internos; **3** — As modificações terão impacto significativo nos processos de trabalho; **4** — As modificações têm impacto sério nos processos de trabalho e na empresa;
- **Disponibilidade**: **0** — Não Aplicável; **1** — Superior a 8 horas — sem impacto negativo para o negócio; **2** — Entre 4 e 8 horas; **3** — Entre 1 e 4 horas; **4** — Inferior a 1 hora — quase imediato;
- **Autenticidade**: **0** — Não Aplicável; **1** — Não precisa de ser autêntica, a origem não é fator obrigatório; **2** — A origem da informação é necessária — causa impacto em processos internos se esta não for verificada; **3** — A origem da informação é relevante — pode causar impacto nos processos internos e externos; **4** — A origem da informação é obrigatória — a sua falta incorre em incumprimento de requisitos contratuais ou legais;
- **Não Repúdio**: **0** — Não Aplicável; **1** — Não necessita de garantia de não repúdio; **2** — Necessita de garantia de não repúdio, quando causa impacto em processos internos; **3** — O não repúdio é relevante quando compromete a atividade de negócio caso essa garantia não seja verificada; **4** — Não repúdio é obrigatório quando a sua falta incorre em incumprimentos de requisitos contratuais ou legais;
- **Criticidade**: **1** — Sem impacto no RTO ou RPO de sistemas/aplicações; **2** — Pouco impacto no RTO ou RPO de sistemas/aplicações. Pode existir indisponibilidade de sistema/aplicação, mas a possibilidade de ser ultrapassado o RTO ou RPO é muito baixa; **3** — Existe algum impacto no RTO ou RPO de sistemas/aplicações. Vai existir indisponibilidade de sistema/aplicação, existindo a possibilidade de ser ultrapassado o RTO ou RPO; **4** — Com impacto no RTO ou RPO de sistemas/aplicações. Vai existir indisponibilidade de sistema/aplicação, sendo ultrapassado o RTO ou RPO;
- **Probabilidade**: **1** — Não é provável que aconteça; **2** — Pode acontecer raras vezes. Aconteceu pelo menos 1 vez nos últimos 3 anos; **3** — Irá acontecer algumas vezes. Aconteceu pelo menos 1 vez no último ano; **4** — De certeza que acontece e que se vai repetir. Aconteceu pelo menos 1 vez nos últimos 6 meses.

Para classificar o risco é usado a seguinte classificação de 4 níveis, conforme a equação da probabilidade (P) a multiplicar pelo impacto (I) (equação (1)).

1. **Baixo**, se $P * I \in \{1, 2\}$;
2. **Médio**, se $P * I \in \{3, 4\}$;

3. **Alto**, se $P * I \in \{6, 8, 9\}$;
4. **Muito Alto**, se $P * I \in \{12, 16\}$.

Por último, de acordo com esta metodologia, os riscos podem ser avaliados consoante os seguintes tipos de tratamento:

1. Reter;
2. Reter após nova análise de risco, com aceitação formal do mesmo;
3. Evitar;
4. Manter ou Aumentar;
5. Remover a fonte do risco;
6. Alterar a probabilidade;
7. Alterar as consequências;
8. Partilhar.

Como exemplo desta metodologia, as figuras 19 e 20 contém duas linhas da tabela utilizada para identificar os riscos de cibersegurança. Note-se que certos campos foram desfocados propositadamente, e os riscos apresentados são riscos que existem na maior parte das empresas.

Desta forma, conseguiu-se obter uma lista de riscos devidamente priorizados segundo a metodologia explicada anteriormente que foram fundamentais para a decisão da avaliação alvo no passo 5. A prática de identificação de riscos de cibersegurança deve ser atenta, proativa e regular na INCM, pelo que o uso contínuo ou periódico desta estratégia de cibersegurança é uma das formas de garantir essas características.

Identificação (Etapa "Identificação do Risco")							Onde Ocorre? (Etapa "Identificação do Risco")		
#ID	Risco Identificado	Descrição do Risco	Ameaça(s)	Vulnerabilidade(s)	Fonte de Risco	Controlos atuais	Processo/Atividade	Recurso(s)	Sistema/Aplicações
[redacted]	Ataque de Distributed Denial of Service (DDoS) à infraestrutura	Um ataque de negação de serviço, que normalmente é distribuído, pode ser direcionado com o objetivo de deitar abaixo e afetar o tráfego normal da infraestrutura.	Ataque a sistemas (por exemplo, ataque distribuído de negação de serviço);	Ponto único de falha	Terroristas; Hackers [intencional]	[redacted]	Serviços de Confiança	Servidores de FrontEnd	FrontEnds
[redacted]	Acesso não autorizado ao centro de processamento de dados	Uma pessoa não autorizada consegue entrar no centro de processamento de dados e ter acesso a dados não autorizados (confidenciais e/ou restritos). Além disso, pode até conseguir introduzir malwares, causar indisponibilidade dos serviços, entre outras consequências que teriam um impacto muito severo para o funcionamento da PKI.	Uso não autorizado de equipamento; Falha de equipamento; Furto de equipamento; Forjamento de direitos; Abuso de direitos	Uso não autorizado de equipamento; Processamento ilegal de dados; Furto de mídia ou documentos; Falha de equipamento; Inexistência de procedimentos de monitorização das instalações de processamento de informações	"Insiders" [acidental, intencional]; Hackers; Criminoso Computacional [intencional]	[redacted]	Gestão e Controlo de Acessos	Infraestrutura da PKI	Servidores, HSMs e outros equipamentos

Figura 19: Exemplo de 2 riscos identificados durante o Passo 4 da Estratégia de Cibersegurança (1/2)

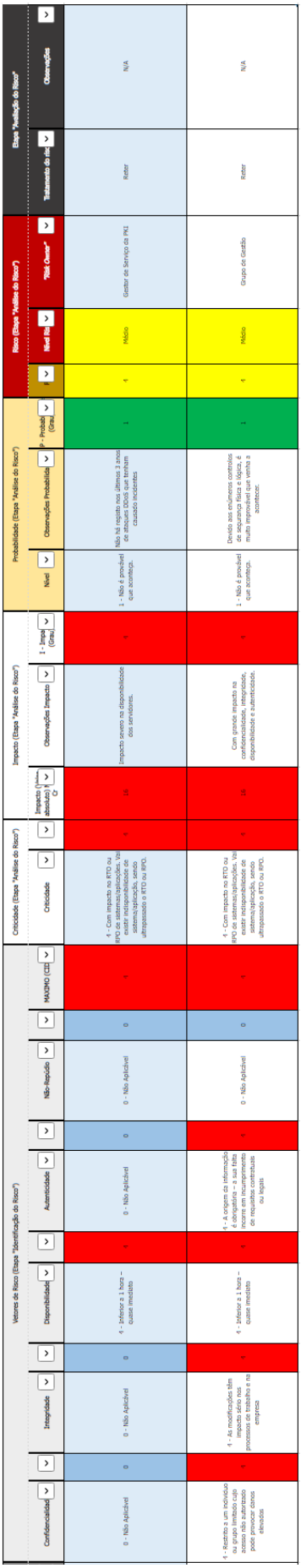


Figura 20: Exemplo de 2 riscos identificados durante o Passo 4 da Estratégia de Cibersegurança (2/2)

5.6 PASSO 5: DEFINIR/CRIAR UMA AVALIAÇÃO ALVO

O 5.º passo da estratégia de cibersegurança é um passo crucial para decidir como o âmbito se vai reforçar em práticas de cibersegurança e gestão de riscos de cibersegurança. A meta, neste passo, é definir qual a avaliação alvo ou desejada nas várias práticas consideradas, sendo que podem até ser consideradas mais práticas do que as abordadas no passo 3.

Foram efetuadas reuniões com os responsáveis pela cibersegurança na PKI do CC para se decidir quais as medidas que iriam fazer parte do "Perfil-Alvo" e, deste modo, iriam constar na política de cibersegurança. Nessas reuniões, começou-se por analisar os riscos identificados no passo 4 e identificar controlos que conseguiriam mitigar ou eliminar esses riscos. Também, aquando da análise e avaliação dos riscos no passo 4, foram identificados controlos ou medidas para diminuir esse risco, sendo que quando se identificava um potencial controlo, ele ia sendo imediatamente documentado. Observando as características dos riscos, é possível arranjar medidas para o tratamento do risco, sejam elas com base em referências informativas ou com base no conhecimento dos participantes. De notar que na Figura 20 existe um campo "Observações" no tratamento que serviu para identificar potenciais controlos que conseguiriam mitigar os riscos, caso a decisão não fosse reter o risco. Claro que esta parte já pertence ao passo 5, contudo dava mais jeito que esta informação ficasse toda junta nesse documento.

Após este trabalho, foi efetuada a análise do relatório final do C2M2 v2.0, obtido no passo 3. Nesta parte, foi identificado o nível de maturidade (MIL) obtido em cada um dos domínios para que se identificasse as áreas onde era necessária mais atenção. Depois disso, foram analisadas as lacunas assinaladas no relatório e mais tarde as restantes medidas. O mesmo foi efetuado também para os controlos da CIS v8.0, onde se identificou as lacunas existentes na autoavaliação efetuada com o CIS CSAT, sendo que neste caso são consideradas lacunas os subcontrolos com classificação inferior a 75%, tal como foi definido no passo 3 (secção 5.4). Aquando da criação da avaliação alvo, foi decidido, para que a primeira iteração fosse mais fácil, que as medidas que não estavam identificadas como lacunas (no C2M2 v2.0 e no CIS *Controls* v8.0) teriam de ser todas incluídas na política de cibersegurança com a mesma classificação obtida na avaliação do passo 3, não sendo necessário serem efetuadas quaisquer análises sobre estas medidas no passo 6. Numa próxima iteração, serão analisadas também as medidas que não são lacunas e será verificado quais é que irão subir em maturidade e as que se mantém com a classificação obtida no passo 3 dessa iteração.

Foi decidido criar dois documentos em *Excel* que contêm as lacunas identificadas e as restantes medidas (i.e., as lacunas identificadas no C2M2, as lacunas identificadas no CIS e os controlos/medidas identificadas no tratamento dos riscos ficam num documento, as restantes medidas ficam no outro). Estes documentos possuem tabelas que estão distribuídas pelos vários pilares estratégicos definidos no passo 1 (secção 5.2), ou seja, cada folha dos documentos contém uma tabela onde irão estar as medidas que estão relacionadas ou pertencem à área de atuação do pilar estratégico em questão. Desta forma, consegue-se facilitar a escrita da política de cibersegurança e, além disso, dar uma melhor noção das áreas que necessitam de mais atenção e das que estão melhor desenvolvidas, de acordo com aquelas que são as prioridades da estratégia. As colunas que cada tabela tem são:

- Descrição da Lacuna ou Medida/Controlo;
- Notas deixadas na avaliação atual (Passo 3);
- Fonte(s)/referência(s) informativa(s);
- Estado de implementação atual;

- Tratamento da Lacuna ou Medida/Controlo (onde se planeia estar numa futura autoavaliação, ou "Avaliação Alvo");
- Incluir na "Política de Cibersegurança"? (Sim/Não);
- Observações sobre a decisão/análise (o porquê de se ter incluído ou não certa lacuna, ou medida/controlo).

Esta forma de organizar as várias medidas permite fazer uma distinção entre o que são lacunas ou não, entre medidas de diferentes pilares estratégicos, ter as referências informativas para as várias lacunas ou medidas (uma medida ou lacuna de determinada fonte de informação pode estar repetida, ou ter relação com outra de uma fonte diferente), saber o tipo de tratamento que é para fazer e se é para incluir ou não na política. Existe também um campo de observações, muito importante para ficarem registadas as decisões tomadas durante a análise das medidas. Por se ter achado mais prático, em vez de se efetuar um relatório à parte com as análises efetuadas e os motivos de se ter incluído ou não certas medidas, decidiu-se aproveitar estes dois documentos *Excel* para que estas decisões lá ficassem documentadas. As decisões rondam questões como a análise custo-benefício (CBA), viabilidade de implementação com os recursos disponíveis, necessidade de implementação, obrigações de negócio ou regulamentares, entre outras.

A avaliação alvo é considerada confidencial, pelo que não é possível transcrevê-la nesta dissertação. Mas para construir essa avaliação, foram então colocadas nos dois documentos anteriormente referidos as práticas do C2M2, do CIS *Controls* v8.0, as práticas/controlos atuais praticados no âmbito, os controlos identificados para mitigar os riscos, as medidas obrigatórias pela legislação, entre outras referências encontradas noutras fontes que se acharam relevantes, incluindo algumas que estavam apontadas nas referências informativas da NIST *Framework*. Além disso, definir o nível de implementação na NIST *Framework* é importante, pois é definido o estado em que se aspira estar em gestão de riscos de cibersegurança. Deste modo, após se definir o nível, verificou-se se existia alguma medida que ainda não fora selecionada para pertencer à política e inclui-se. O mesmo aconteceu na escolha do grupo de implementação do CIS v8.0 em que se planeia estar, ou seja, após se decidir o IG tratou-se de verificar se os subcontrolos estavam todos já incluídos no "Perfil-Alvo".

Por fim, deu-se início à escrita da "Política de Cibersegurança" da INCM, tendo como âmbito a PKI do CC. Note-se que parte da política já tinha sido escrita ao longo da aplicação estratégia (passo 1), nomeadamente algumas introduções teóricas sobre os vários pilares estratégicos da política. Além disso, foram incluídos na política capítulos sobre conceitos gerais de cibersegurança, sobre o papel da INCM em cibersegurança para Portugal e sobre a legislação a que a INCM está sujeita relativamente a cibersegurança. Porém, o capítulo sugerido na estratégia que se deve ter também é o das responsabilidades em cibersegurança definidas para cada um dos grupos de colaboradores com papéis distintos no âmbito. Desta forma, consegue-se alertar mais os colaboradores para a importância que estes têm em garantir um ambiente mais ciberseguro, além de ficarem documentadas as suas responsabilidades em cibersegurança. A definição das responsabilidades seguiu a avaliação alvo, de modo a que as medidas, obrigações e tarefas identificadas fossem distribuídas pelos intervenientes correspondentes.

Assim, a política de cibersegurança incluí tudo aquilo que foi decidido até ao passo 5, nomeadamente:

- Referência ao nível de implementação alvo em práticas de gestão de riscos segundo a NIST *Framework*;
- Nível de maturidade (MIL) esperado obter nos vários domínios do C2M2;
- Grupo de implementação (IG) do CIS *Controls* v8.0 onde se planeia estar;

- Práticas/Controlos/Medidas identificadas para mitigar os riscos de cibersegurança, distribuídas pelos vários pilares estratégicos com que estão relacionadas;
- Práticas do C2M2 distribuídas pelos vários pilares estratégicos com que estão relacionadas;
- Controlos/Subcontrolos da versão 8.0 do CIS distribuídos pelos vários pilares estratégicos com que estão relacionados;
- Práticas/Controlos/Medidas implementadas atualmente distribuídas pelos vários pilares estratégicos com que estão relacionadas;
- Práticas/Controlos/Medidas de outras referências informativas distribuídas pelos vários pilares estratégicos com que estão relacionadas;
- Mapeamento de todas as práticas/controlos/medidas possíveis para as várias subcategorias presentes nas funções (Identificar, Proteger, Detetar, Responder, Recuperar) da NIST *Framework Core* 2.5, com o recurso ao mapeamento apresentado no apêndice A. Esta é uma parte importante para mostrar que existe *compliance* com a *framework* de base desta estratégia (NIST CSF), além de evidenciar também o *compliance* existente com o Quadro Nacional de Referência para a Cibersegurança (QNRCS) [11], visto que este possui as subcategorias idênticas. No âmbito desta estratégia, o QNRCS também foi considerado, e foram vistas as dicas de implementação técnica e processual lá descritas, tendo-se concluído que as várias referências informativas usadas já abordam essas questões.

A política de cibersegurança da PKI do CC foi aprovada pelo CISO e encontra-se em aprovação pela administração da INCM.

5.7 Passo 6: Criar um Plano de Ação Priorizado para Combater as Lacunas

Neste passo é criado um plano de ação priorizado cujo objetivo é colmatar as lacunas existentes entre a situação atual e a desejada, começando por se realizar um *"gap analysis"* entre estas duas situações. Não é possível apresentar o conteúdo das iniciativas efetuadas nesta secção devido a essa informação ter sido considerada confidencial, pelo que é descrito o que foi feito, de forma a se ficar com uma noção sobre como este passo foi aplicado e o tipo de resultados que se obtiveram.

Foram efetuadas reuniões com os responsáveis para se tentar decidir sobre as ações a tomar para cumprir com a política de cibersegurança e quais as mais prioritárias. Como o que importa nesta fase é tentar criar um plano de ação para combater as lacunas, foram identificadas as lacunas entre as avaliações atual e a alvo, sendo que como no passo 5 já foram identificadas as lacunas no documento *Excel*, e uma vez que as restantes medidas não sofreram alterações, avançou-se para a análise. A análise das lacunas começou pela perceção das consequências que estas poderiam trazer para a PKI do CC, sendo tal fundamental para perceber quais as que são mais urgentes de "fechar", ou seja, quais as lacunas que devem ser colmatadas em primeiro lugar.

Foram tidas em conta todas as considerações referidas na secção 4.3.6, sendo que essas consequências associadas a lacunas ficaram documentadas no plano de ação priorizado. Além disso, a responsabilidade da execução do plano de ação ficou atribuída ao responsável de segurança da PKI, que definiu os indicadores-chave de desempenho (KPIs) a serem usados para medir o progresso da implementação/aplicação do plano de ação. Alguns exemplos de KPIs que foram usados foram o prazo para fechar as lacunas, o tempo gasto para fechar as lacunas, o

custo das operações ou alterações efetuadas para combater a lacuna, a quantidade de entregas ou progresso que os executantes das ações forneciam para "fechar" ou cumprir com as ações do plano e, a obtenção da avaliação alvo nas lacunas analisadas.

Para além das consequências das lacunas, foi ainda efetuada ou revista a análise custo-benefício para as várias lacunas, de forma a perceber quais poderiam trazer mais benefícios para a INCM, ou para o âmbito da PKI, caso ficassem mitigadas ou eliminadas. A maior parte das medidas não tiveram necessidade de grandes investimentos, devido à grande variedade de ferramentas, métodos e abordagens já em vigor na organização. Contudo, algumas necessitavam de mais tempo, conhecimento e recursos para ficarem no estado pretendido, ou seja, para ficarem no estado que ficou expresso na política de cibersegurança. Deste modo, estas considerações entraram também para se priorizar a lista de ações com as medidas que eram necessárias ser aplicadas primeiro.

O plano de ação foi feito em formato PDF com a descrição dos vários pontos referidos anteriormente, tendo também sido criado um projeto no *Jira Software* da INCM para colocar as várias ações que constam no plano. Essas ações incluem as tarefas necessárias a serem feitas, com a indicação do prazo para as concluir e quem é que está encarregue de as implementar.

5.8 Passo 7: Implementar/Aplicar o Plano de Ação

No passo 7 o objetivo é implementar o plano de ação priorizado, de forma a cumprir com o perfil-alvo na política de cibersegurança.

Assim, tendo em conta a prioridade definida, foram implementadas as ações que eram mais urgentes primeiro, sendo que o rastreamento de responsabilidades foi feito pelo dono do plano, o responsável de segurança da PKI neste caso. Através de reuniões com os vários intervenientes, foram esclarecidas as várias ações e distribuídas as tarefas através do recurso à plataforma *Jira Software*, como já referido anteriormente. A implementação das ações correu bem, sendo que à data de escrita desta parte da dissertação, a implementação das várias ações decorria conforme o plano estabelecido. Deste modo, é importante referir que, apesar de o plano de ação ainda não ter ficado todo concluído, este irá ficar concluído de acordo com o que está detalhado na política de cibersegurança.

O progresso das implementações é medido através das métricas definidas pelo dono do plano e também através do uso do C2M2 e CIS CSAT. No CIS CSAT, por exemplo, foi escolhido o grupo de implementação alvo e depois foi atribuído a colaboradores a responsabilidade de implementarem os subcontrolos que estavam assinalados como lacunas. Assim, utilizando esta ferramenta existe a facilidade do dono do plano validar as respostas e evidências que são deixadas pelos responsáveis pela implementação.

Apesar de não se poder referir todas as medidas que foram implementadas, há uma que foi executada e será descrita como forma de exemplo. A INCM tem que cumprir com o Regime Jurídico da Segurança do Ciberespaço (Lei n.º 46/2018) [17], pelo que tal foi incluído no plano de ação, e consta na política de cibersegurança. A medida implementada foi elaborar e enviar a informação pedida pelo Decreto-Lei n.º 65/2021 [32] e pelas instruções técnicas do Regulamento n.º 183/2022 [33], que foi concluída com sucesso e passará a ser prática habitual todos os anos de acordo com o que ficou estabelecido na política de cibersegurança.

Por último, é relevante referir que já está a ser planeada uma nova reavaliação do estado em cibersegurança para o mesmo âmbito, de forma a analisar o impacto do novo regulamento eIDAS na PKI do CC, que apesar de a sua publicação só estar prevista para final do ano de 2022, já existe publicada uma primeira proposta [19]. Como referido na secção 4.3.8, as constantes mudanças nos objetivos de negócio, ambiente de ameaças, mercado de trabalho, na tecnologia, entre outras, são um fator decisivo para fazer com que aquilo que hoje é o estado atual em

cibersegurança, amanhã possa já não ser e este ter mudado ou regredido. De certa forma, o adequado é haver um trabalho contínuo por parte da INCM para evoluir em cibersegurança, e ir incluindo mais áreas da empresa ao longo do tempo, até que toda ela esteja no âmbito da estratégia.

6

CONCLUSÕES E TRABALHO FUTURO

Concluído assim o desenvolvimento de uma estratégia de cibersegurança e concluída a demonstração da aplicação deste projeto a um caso real, neste último capítulo são efetuadas as conclusões e apresentadas algumas perspetivas para trabalho futuro.

6.1 CONCLUSÕES

O principal propósito com esta dissertação era o de criar uma estratégia que conseguisse lidar de forma estruturada e formal com a cibersegurança nas empresas em Portugal. Este é efetivamente um tema que preocupa cada vez mais as organizações em todo o mundo, uma vez que o clima de ameaças cibernéticas tem aumentado com a constante evolução e dependência da tecnologia nas empresas. Desta forma, os atacantes veem um alvo atrativo nas empresas para efetuar ataques dos mais variados tipos e com diferentes tipos de finalidades. Contudo, pode-se dizer que estar na defensiva é sempre mais complicado do que na ofensiva, pelo que é necessário que sejam seguidas metodologias geralmente aceites pela comunidade científica para facilitar e tornar eficazes os processos de reforço da cibersegurança.

É neste âmbito que é feita a apresentação do estado da arte (capítulo 2), onde são introduzidos um conjunto de conceitos e referências, tais como *standards*, *frameworks*, *guidelines*, controlos e estratégias de agências governamentais, para demonstrar como é possível lidar com a cibersegurança. Nesta área tão complexa e com uma grande quantidade de investigações já feitas, é evidente que não se poderia começar uma estratégia do zero sem se recorrer a nenhuma referência externa de instituições com trabalho relevante na área da cibersegurança, até mesmo por questões de credibilidade e *compliance*. Assim, em primeiro lugar foram apresentados alguns conceitos-base ou gerais sobre cibersegurança, nomeadamente a necessidade das empresas seguirem uma estratégia, alguns riscos ou ciberataques mais comuns e duas normas relevantes da *International Organization for Standardization* (ISO/IEC 27002:2013 [46] e ISO/IEC 27032 [73]). A seguir foram analisadas as estratégias de cibersegurança publicadas por agências governamentais, nomeadamente da União Europeia, de Portugal, do Departamento de Energia dos Estados Unidos e do *Castle Point Council* do Reino Unido. Porém, era necessário arranjar metodologias para criar a estratégia propriamente dita, pelo que foram estudadas a NIST *Framework* [90], o C2M2 [26] e os controlos da CIS v8.0 [6].

Estas metodologias foram escolhidas para fazerem parte da estratégia de cibersegurança desta dissertação porque são muito referenciadas internacionalmente por organizações especialistas em cibersegurança, além de possuírem ferramentas que ajudam a aplicar a estratégia de uma forma mais simples, completa e eficaz. Desta forma, a estratégia de cibersegurança desta tese tem por base as 7 etapas descritas pela NIST *Framework* (secção 2.5.5), complementadas pela ferramenta de autoavaliação C2M2 [26] e a nova versão de controlos da CIS [6] que

permitiu criar uma estratégia de fácil entendimento para as empresas. Vários foram os documentos, publicações e opiniões de terceiros que foram consultados para que a estratégia englobasse todas as áreas necessárias ao reforço da cibersegurança e a tornasse o mais completa possível, sendo as ferramentas referidas uma ajuda preciosa na análise da situação atual em cibersegurança e na definição de um "Perfil-Alvo" para a organização que siga esta estratégia.

Claro que são colocados às empresas imensos desafios relacionados com a cibersegurança e mesmo durante a implementação da estratégia, como se pode observar no capítulo 3. Estes desafios foram tidos em conta durante a construção da estratégia de cibersegurança no capítulo 4 e durante a aplicação da estratégia no capítulo 5. Durante o desenvolvimento da estratégia, o maior problema foi criar algo que servisse para todas as empresas portuguesas (principalmente as PMEs), que fosse completo e abrangesse a maioria das matérias da cibersegurança, não tendo a própria estratégia lacunas, e que ao mesmo tempo fosse simples e exequível. Porém, por vezes é difícil aceitar que as coisas podem não ficar logo perfeitas à partida, e ainda para mais numa área como a cibersegurança. Como já referido anteriormente nesta dissertação, na cibersegurança não existem formas perfeitas de proteção, tal como não existem algoritmos criptográficos perfeitos, isto porque, se existissem, então todas as empresas aplicavam essa forma e não seria necessário serem mais debatidas estas questões. Desta forma, os esforços efetuados nesta tese levaram a que a estratégia fosse abrangente e flexível também no sentido de, por exemplo, se duas pessoas tentassem no mesmo âmbito e condições aplicar a estratégia, então os resultados iriam ser certamente diferentes nos dois casos, isto porque depende muito da abordagem e rigor que estes adotaram e das decisões tomadas. Percebe-se então a importância da existência de um facilitador ou responsável pela implementação da estratégia que tenha capacidades e esteja familiarizado com esta estratégia, sendo que este é que dará as orientações daquilo que se deve fazer e de que forma.

Existem, porém, partes menos flexíveis, como, por exemplo, a da avaliação atual e da análise de riscos, uma vez que é importante que estes resultados sejam condizentes com a realidade da organização. Se acontecerem erros nestas fases pode-se ter uma ilusão de falsa proteção, o que tornará as lacunas indetetáveis em fases posteriores. Durante a aplicação da estratégia na Imprensa Nacional — Casa da Moeda (INCM), houve sempre o cuidado de dar a entender primeiro a todos os responsáveis envolvidos aquelas que são as restrições que existem ao se implementar uma estratégia deste género. Conseguiu-se desta forma que o progresso da estratégia fosse gradualmente evoluindo, com a noção que é um trabalho de aperfeiçoamento contínuo.

O maior problema na implementação da estratégia foi o tempo que se demorou a tomar decisões, principalmente por se estar a utilizar uma metodologia que era nova para todos os envolvidos. A adaptação inicial aos processos da empresa, os eventuais assuntos extra que eram necessários resolver, o tempo excessivo nos vários passos da estratégia e a dificuldade em arranjar tempo livre com os responsáveis para se efetuar as correspondentes tarefas, fez com que a primeira iteração da estratégia descrita no capítulo 5 não ficasse concluída no prazo estipulado ou que era previsível terminar. Contudo, é de salientar que o facto de se ter reduzido o âmbito nesta primeira fase para a PKI do CC tornou mais simples a implementação da estratégia e fez com que os resultados sejam considerados ótimos para uma primeira iteração da estratégia. Ajudou ainda o facto de já existirem muitos processos de segurança aplicados a este âmbito e um extenso lote de documentação associada. É importante que se continue a iterar a estratégia e aumentar o âmbito, sendo o objetivo final que a estratégia inclua todas as áreas e serviços da INCM.

Assim, a "Estratégia de Cibersegurança" possui todas as condições para reforçar em vários aspetos a cibersegurança de uma empresa, enfrentando todos os desafios colocados à cibersegurança e, em simultâneo, dando os recursos necessários de várias fontes para conseguir implementar um "Perfil-alvo" conforme as necessidades da empresa e em *compliance* com as normas de cibersegurança aceites pela indústria.

6.2 PERSPETIVA PARA TRABALHO FUTURO

Trabalho futuro irá existir sempre numa área como a cibersegurança, e isso também se percebe pela leitura dos vários capítulos desta dissertação. A própria estratégia apresentada sugere que o trabalho de melhoria e reforço das capacidades em cibersegurança de uma empresa seja contínuo e de constante evolução, percebendo que hoje uma empresa está num determinado estado em cibersegurança, mas no futuro terá certamente que evoluir. Desse modo, é importante que os responsáveis continuamente procurem e investiguem novos métodos, ferramentas, publicações, entre outras fontes atualizadas, para estarem sempre a par das últimas notícias e respondam às mudanças que diariamente surgem no mundo da cibersegurança.

A própria estratégia de cibersegurança aqui apresentada deve ser alvo no futuro de revisão, uma vez que pode-se considerar que existem processos de cibersegurança e gestão de riscos de cibersegurança mais evoluídos e com uma maior eficácia. Desta forma, o mais certo é que em menos de 3 anos a estratégia possa sofrer alterações e seja revisto o conteúdo apresentado nesta dissertação, nem que seja simplesmente mudada a versão dos recursos que são utilizados. Sempre que exista algo na indústria ou alguma publicação que se considere de interesse para incluir na estratégia, seja porque apresenta uma abordagem mais eficaz e simples que a apresentada nesta estratégia, ou seja porque as referências informativas desta estratégia ficaram desatualizadas ou obsoletas, então é incentivada a mudança do atual *"roadmap"* da estratégia de cibersegurança. A lição que se pode tirar da cibersegurança é que nada dura para sempre, pelo que se uma organização não se adaptar às suas mudanças, então irá incorrer no risco de ficar para trás da concorrência.

Relativamente às versões das várias referências informativas, as instituições que publicam artigos sobre cibersegurança têm sempre a preocupação de irem atualizado as suas publicações, ainda por cima no contexto atual de ameaças que o ciberespaço enfrenta. À data que é escrita esta secção, o *Cybersecurity Capability Maturity Model* (C2M2) já publicou a versão 2.1 [28], que além de já possuir novos recursos atualizados para a versão, incluindo a ferramenta de autoavaliação, introduziu mais práticas em alguns dos domínios da antiga versão. Inclusive na INCM já se vai rever a estratégia e passar a usar no futuro esta versão, uma vez que além de existirem mais uns recursos extra disponibilizados pelo C2M2, estão incluídas novas práticas que aperfeiçoam mais a autoavaliação do passo 3 da estratégia de cibersegurança desta dissertação. No que diz respeito aos controlos da CIS, ainda não existem atualizações da versão utilizada nesta tese, mas na NIST *Framework*, apesar de não estar publicada também uma nova versão, já se começou a trabalhar para a criação da versão 2.0, que irá substituir a versão 1.1. Segundo a NIST, "com base no *feedback* das partes interessadas, de modo a refletir o cenário de cibersegurança em constante evolução e ajudar as organizações a gerir os riscos de cibersegurança com mais facilidade e eficácia, está a ser planeada uma atualização nova e mais significativa para a *Framework*: a NIST CSF 2.0" [94]. Deste modo, percebe-se que será sempre necessário no futuro alterar muitas das estratégias e *frameworks* que são atualmente seguidas pela indústria mundial. Certamente, haverá possibilidade no futuro de adaptar esta estratégia a todas essas mudanças que vão surgir, isto se for mantida esta atitude atenta de rever e reformular os métodos usados.

Ainda relativamente aos trabalhos que estão a ser desenvolvidos pela NIST para a versão 2.0 da *Framework*, no dia 17 de agosto de 2022 foi efetuado o primeiro *workshop* para debater melhorias possíveis à infraestrutura, analisar os comentários recebidos à solicitação de informações (RFI) pedida pela NIST e para esta apresentar os planos que tem para o futuro [93]. De entre os vários painéis apresentados, no painel 4 foi referida a necessidade de esta nova versão apresentar mais apoio às PMEs no que diz respeito a processos de governação de cibersegurança. Isto mostra que o tema desta dissertação vai de encontro às necessidades das empresas, uma vez que são necessários mais processos renovados e consistentes para manter uma trajetória de crescimento em cibersegurança nas PMEs.

Exemplificando como as práticas de cibersegurança podem mudar por diversas razões, o diretor-executivo da ENISA, Juhan Lepassaar, alertou que o atual sistema de comunicação de incidentes de cibersegurança é muito burocrático e "não funciona", sendo que na opinião dele deve haver um sistema mais resiliente, bem como um melhor ambiente legislativo e de partilha de informações com os estados-membros da UE [78]. Além disto, o legislador da UE Bart Groothuis disse que, para além do problema de partilha de informações, também as equipas de resposta a incidentes de segurança computacional (CSIRTs) precisam de ser melhoradas através de uma legislação renovada [78]. Para resolver estes problemas, entre outros, está a ser efetuada uma atualização da atual diretiva NIS sobre a Segurança das Redes e dos Sistemas de Informação (Diretiva (UE) 2016/1148) [35]. Ora, o impacto destas potenciais alterações pode ser muito grande em toda a UE, fazendo com que os vários estados-membros tenham que rever as suas leis sobre cibersegurança. No caso português, pode significar a mudança no atual Regime Jurídico de Segurança do Ciberespaço (Lei n.º 46/2018), uma vez que este segue ou 'transpõe' a Diretiva NIS. Assim, a nova Diretiva NIS2 pode revolucionar completamente a maneira como as organizações lidam com os incidentes de cibersegurança, pelo que as práticas que atualmente são aceites e praticadas pelas empresas poderão ter de ser modificadas para atender não só às necessidades regulamentares, mas também às melhores práticas da indústria.

Apesar de tudo, percebe-se que esta estratégia de cibersegurança é flexível o suficiente para conseguir lidar com estas mudanças, podendo ser incluídas novas referências informativas para se considerar nos vários passos da estratégia. No futuro, que pode ser já "amanhã", terá de haver um suporte contínuo à estratégia desta tese para que as medidas (práticas, controlos, *frameworks*, *standards*, *guidelines*, ferramentas, métodos, etc.) de cibersegurança numa empresa sejam sempre, dentro dos possíveis, o mais completas, eficazes, atualizadas e conforme a regulamentação aplicável.

BIBLIOGRAFIA

[1] A. Amiruddin, H. G. Afiansyah, and H. A. Nugroho. Cyber-Risk Management Planning Using NIST CSF V1.1, NIST SP 800-53 Rev.5, and CIS Controls v8. https://ieeexplore.ieee.org/document/9699337, 2021. Accessed: 2022-05-17.

[2] C. Business. How Russian threats in the 2000s turned this country into the go-to expert on cyber defense. https://edition.cnn.com/2021/06/18/tech/estonia-cyber-security-lessons-intl-cmd/index.html, 2021. Accessed: 2022-09-12.

[3] CastlePoint. Cyber Security Strategy. https://www.castlepoint.gov.uk/download.cfm?doc=docm93jijm4n3296, 2021. Accessed: 2021-12-18.

[4] N. C. S. Centre. Cyber Essentials: Requirements for IT infrastructure. https://www.ncsc.gov.uk/cyberessentials/overview, 2021. Accessed: 2021-12-18.

[5] CIS. CIS Critical Security Controls v8 Mapping to NIST CSF. https://www.cisecurity.org/insights/white-papers/cis-controls-v8-mapping-to-nist-csf, 2021. Accessed: 2022-06-05.

[6] CIS. CIS Critical Security Controls (Version 8). https://www.cisecurity.org/controls/cis-controls-list/, 2021. Accessed: 2021-12-17.

[7] CISA. What is Cybersecurity? https://www.cisa.gov/uscert/ncas/tips/ST04-001, 2019. Accessed: 2021-12-12.

[8] Cisco. What Is a Cyberattack? https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html, 2021. Accessed: 2021-12-08.

[9] Cisco. What is Cybersecurity? https://www.cisco.com/c/en/us/products/security/what-is-cybersecurity.html, 2021. Accessed: 2021-12-02.

[10] CNCS. Estratégia Nacional. https://www.cncs.gov.pt/pt/estrategia-nacional/, 2019. Accessed: 2021-12-02.

[11] CNCS. Quadro Nacional de Referência para a Cibersegurança (QNRCS). https://www.cncs.gov.pt/pt/quadro-nacional/, 2019. Accessed: 2021-12-12.

[12] CNCS. Boas práticas em Teletrabalho. https://www.cncs.gov.pt/pt/ciberseguranca-em-teletrabalho/, 2021. Accessed: 2022-01-27.

[13] CNCS. CERT.PT. https://www.cncs.gov.pt/pt/certpt//, 2021. Accessed: 2022-01-24.

[14] CNCS. RFC 2350. https://www.cncs.gov.pt/pt/certpt/rfc-2350/, 2021. Accessed: 2022-01-24.

[15] CNCS. Centro Nacional de Cibersegurança. https://www.cncs.gov.pt/, 2022. Accessed: 2022-01-24.

[16] CNCS. Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança v1.0. https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos.pdf, 2022. Accessed: 2022-07-10.

[17] CNCS. Regime Jurídico. https://www.cncs.gov.pt/pt/regime-juridico/, 2022. Accessed: 2022-01-21.

[18] E. Commission. New EU Cybersecurity Strategy and new rules to make physical and digital critical entities more resilient. https://ec.europa.eu/commission/presscorner/detail/en/IP_20_2391, 2020. Accessed: 2021-12-02.

[19] E. COMMISSION. Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL amending Regulation (EU) No 910/2014 as regards establishing a framework for a European Digital Identity. https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:52021PC0281from=EN, 2021. Accessed: 2022-09-12.

[20] COMPUTERWORLD. Minsait: 56% das empresas colocam em risco o seu futuro por não ter uma estratégia de cibersegurança definida. https://www.computerworld.com.pt/2021/05/04/minsait-56-das-empresas-colocam-em-risco-o-seu-futuro-por-nao-ter-uma-estrategia-de-ciberseguranca-definida/, 2021. Accessed: 2022-09-14.

[21] J. O. da União Europeia. DIRETIVA (UE) 2016/1148 DO PARLAMENTO EUROPEU E DO CONSELHO. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016L1148, 2016. Accessed: 2022-01-21.

[22] J. O. da União Europeia. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32016R0679, 2016. Accessed: 2022-01-24.

[23] U. DOE. ENERGY SECTOR CYBERSECURITY FRAMEWORK IMPLEMENTATION GUIDANCE. https://www.energy.gov/sites/prod/files/2015/01/f19/Energy%20Sector%20Cybersecurity%20Framework%20Implementation%20Guidance_FINAL_01-05-15.pdf, 2015. Accessed: 2022-05-26.

[24] U. DOE. CYBERSECURITY CAPABILITY MATURITY MODEL (C2M2) FACILITATOR GUIDE. https://www.energy.gov/sites/default/files/2017/04/f34/2017-03-21-C2M2%20Facilitator%20Guide%20v1.1a.pdf, 2017. Accessed: 2022-05-26.

[25] U. DOE. Cybersecurity Strategy 2018-2020. https://www.energy.gov/sites/prod/files/2018/07/f53/EXEC-2018-003700%20DOE%20Cybersecurity%20Strategy%202018-2020-Final-FINAL-c2.pdf, 2018. Accessed: 2021-12-18.

[26] U. DOE. Cybersecurity Capability Maturity Model (Version 2.0). https://www.energy.gov/sites/default/files/2021-07/C2M2%20Version%202.0%20July%202021_508.pdf, 2021. Accessed: 2021-12-12.

[27] U. DOE. Cybersecurity Capability Maturity Model — Tools. https://c2m2.doe.gov/, 2021. Accessed: 2021-12-12.

[28] U. DOE. Cybersecurity Capability Maturity Model (Version 2.1). https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf, 2022. Accessed: 2022-09-04.

[29] DRE. Resolução do Conselho de Ministros n.º 36/2015. https://dre.pt/dre/detalhe/resolucao-conselho-ministros/36-2015-67468089, 2015. Accessed: 2021-12-02.

[30] DRE. Lei n.º 58/2019, de 8 de agosto. https://dre.pt/dre/detalhe/lei/58-2019-123815982, 2019. Accessed: 2022-07-12.

[31] DRE. Resolução do Conselho de Ministros n.º 92/2019. https://dre.pt/dre/detalhe/resolucao-conselho-ministros/92-2019-122498962, 2019. Accessed: 2021-12-02.

[32] DRE. Decreto-Lei n.º 65/2021, de 30 de julho. https://dre.pt/dre/detalhe/decreto-lei/65-2021-168697988, 2021. Accessed: 2022-07-20.

[33] DRE. Regulamento n.º 183/2022, de 21 de fevereiro. https://dre.pt/dre/detalhe/regulamento/183-2022-179325870, 2022. Accessed: 2022-07-20.

[34] ekonomista. 9 ataques informáticos que ficaram para a história. https://www.e-konomista.pt/ataques-informaticos-ficaram-para-historia/, 2018. Accessed: 2021-12-02.

[35] ENISA. NIS Directive. https://www.enisa.europa.eu/topics/nis-directive, 2016. Accessed: 2022-01-21.

[36] EthicalHat. CIS CSAT - CIS Controls Self Assessment Tool (v2.0). https://csat.cisecurity.org/, 2021. Accessed: 2022-06-14.

[37] ETSI. ETSI EN 319 421 V1.1.1, Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps. https://www.etsi.org/deliver/etsi_en/319400_319499/319421/01.01.01_60/en_319421v010101p.pdf, 2016. Accessed: 2022-06-12.

[38] ETSI. ETSI EN 319 401 V2.3.1, Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. https://www.etsi.org/deliver/etsi_en/319400_319499/319401/02.03.01_60/en_319401v020301p.pdf, 2021. Accessed: 2022-06-12.

[39] ETSI. ETSI EN 319 411–1 V1.3.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements. https://www.etsi.org/deliver/etsi_en/319400_319499/31941101/01.03.01_60/en_31941101v010301p.pdf, 2021. Accessed: 2022-06-12.

[40] ETSI. ETSI EN 319 411–2 V2.3.1, Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates. https://www.etsi.org/deliver/etsi_en/319400_319499/31941102/02.03.01_60/en_31941102v020301p.pdf, 2021. Accessed: 2022-06-12.

[41] EU. The EU's Cybersecurity Strategy for the Digital Decade. https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0, 2020. Accessed: 2021-12-18.

[42] I. O. for Standardization. *ISO/IEC 27033-3:2010 — Information technology — Security techniques — Network security — Part 3: Reference networking scenarios — Threats, design techniques and control issues*. Geneva, Switzerland, 2010.

[43] I. O. for Standardization. *ISO/IEC 27031:2011 — Information technology — Security techniques — Guidelines for information and communication technology readiness for business continuity*. Geneva, Switzerland, 2011.

[44] I. O. for Standardization. *ISO/IEC 27034-1:2011 — Information technology — Security techniques — Application security — Part 1: Overview and concepts*. Geneva, Switzerland, 2011.

[45] I. O. for Standardization. *ISO/IEC 27033-2:2012 — Information technology — Security techniques — Network security — Part 2: Guidelines for the design and implementation of network security*. Geneva, Switzerland, 2012.

[46] I. O. for Standardization. *ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls*. BSI Standards Limited 2013, Geneva, Switzerland, 2nd edition, 2013. ISBN 978 0 580 63921 0.

[47] I. O. for Standardization. *ISO/IEC 27033-5:2013 — Information technology — Security techniques — Network security — Part 5: Securing communications across networks using Virtual Private Networks (VPNs)*. Geneva, Switzerland, 2013.

[48] I. O. for Standardization. *ISO/IEC 27036-3:2013 — Information technology — Security techniques — Information security for supplier relationships — Part 3: Guidelines for information and communication technology supply chain security*. Geneva, Switzerland, 2013.

[49] I. O. for Standardization. *ISO/IEC 27033-4:2014 — Information technology — Security techniques — Network security — Part 4: Securing communications between networks using security gateways*. Geneva, Switzerland, 2014.

[50] I. O. for Standardization. *ISO/IEC 27017:2015 — Information technology — Security techniques — Code of practice for information security controls based on ISO/IEC 27002 for cloud services*. Geneva, Switzerland, 2015.

[51] I. O. for Standardization. *ISO/IEC 27033-1:2015 — Information technology — Security techniques — Network security — Part 1: Overview and concepts*. Geneva, Switzerland, 2015.

[52] I. O. for Standardization. *ISO/IEC 27034-2:2015 — Information technology — Security techniques — Application security — Part 2: Organization normative framework*. Geneva, Switzerland, 2015.

[53] I. O. for Standardization. *ISO/IEC 17825:2016—Information technology — Security techniques — Testing methods for the mitigation of non-invasive attack classes against cryptographic modules*. Geneva, Switzerland, 2016.

[54] I. O. for Standardization. *ISO/IEC 27033-6:2016 — Information technology — Security techniques — Network security — Part 6: Securing wireless IP network access*. Geneva, Switzerland, 2016.

[55] I. O. for Standardization. *ISO/IEC 27034-6:2016 — Information technology — Security techniques — Application security — Part 6: Case studies*. Geneva, Switzerland, 2016.

[56] I. O. for Standardization. *ISO/IEC 27035-1:2016—Information technology — Security techniques — Information security incident management — Part 1: Principles of incident management*. Geneva, Switzerland, 2016.

[57] I. O. for Standardization. *ISO/IEC 27035-2:2016—Information technology — Security techniques — Information security incident management — Part 2: Guidelines to plan and prepare for incident response*. Geneva, Switzerland, 2016.

[58] I. O. for Standardization. *ISO/IEC 27036-4:2016 — Information technology — Security techniques — Information security for supplier relationships — Part 4: Guidelines for security of cloud services*. Geneva, Switzerland, 2016.

[59] I. O. for Standardization. *ISO/IEC 27034-5:2017 — Information technology — Security techniques — Application security — Part 5: Protocols and application security controls data structure*. Geneva, Switzerland, 2017.

[60] I. O. for Standardization. *ISO 31000:2018—Risk management — Guidelines*. Geneva, Switzerland, 2018.

[61] I. O. for Standardization. *ISO/IEC 27005:2018(E) Information technology — Security techniques — Information security risk management*. Geneva, Switzerland, 2018.

[62] I. O. for Standardization. *ISO/IEC 27034-3:2018 — Information technology — Application security — Part 3: Application security management process*. Geneva, Switzerland, 2018.

[63] I. O. for Standardization. *ISO/IEC 27034-7:2018 — Information technology — Application security — Part 7: Assurance prediction framework*. Geneva, Switzerland, 2018.

[64] I. O. for Standardization. *ISO 22301:2019 — Security and resilience — Business continuity management systems — Requirements*. Geneva, Switzerland, 2019.

[65] I. O. for Standardization. *ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines*. Geneva, Switzerland, 2019.

[66] I. O. for Standardization. *ISO/IEC TR 23187:2020 — Information technology — Cloud computing — Interacting with cloud service partners (CSNs)*. Geneva, Switzerland, 2020.

[67] I. O. for Standardization. *ISO/IEC 27036-1:2021 — Cybersecurity — Supplier relationships — Part 1: Overview and concepts*. Geneva, Switzerland, 2021.

[68] I. O. for Standardization. *ISO/IEC 15408-1:2022 — Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 1: Introduction and general model*. Geneva, Switzerland, 2022.

[69] I. O. for Standardization. *ISO/IEC 15408-2:2022 — Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 2: Security functional components*. Geneva, Switzerland, 2022.

[70] I. O. for Standardization. *ISO/IEC 15408-3:2022 — Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 3: Security assurance components*. Geneva, Switzerland, 2022.

[71] I. O. for Standardization. *ISO/IEC 15408-4:2022 — Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 4: Framework for the specification of evaluation methods and activities*. Geneva, Switzerland, 2022.

[72] I. O. for Standardization. *ISO/IEC 15408-5:2022 — Information security, cybersecurity and privacy protection — Evaluation criteria for IT security — Part 5: Pre-defined packages of security requirements*. Geneva, Switzerland, 2022.

[73] I. O. for Standardization. *ISO/IEC 27032 Information technology — Cybersecurity — Guidelines for Internet security (DIS Stage)*. Geneva, Switzerland, 2022.

[74] I. O. for Standardization. *ISO/IEC 27036-2:2022 — Cybersecurity — Supplier relationships — Part 2: Requirements*. Geneva, Switzerland, 2022.

[75] I. O. for Standardization. *ISO/IEC DIS 27033-7 — Information technology – Network security — Part 7: Guidelines for network virtualization security*. Geneva, Switzerland, 2022.

[76] I. O. for Standardization. *ISO/IEC DIS 27034-4 — Information technology — Security techniques — Application security — Part 4: Validation and verification*. Geneva, Switzerland, 2022.

[77] GeeksforGeeks. Difference between Cyber Security and Information Security. https://www.geeksforgeeks.org/difference-between-cyber-security-and-information-security/, 2022. Accessed: 2022-09-12.

[78] E. Germany. EU's cyber incident reporting mechanism does not work, agency chief warns. https://www.euractiv.com/section/cybersecurity/news/eus-cyber-incident-reporting-mechanism-does-not-work-agency-chief-warns/, 2022. Accessed: 2022-09-04.

[79] W. Hendrickx. NIST's Cybersecurity Framework has become the common language for international cybersecurity. https://www.scmagazine.com/perspective/compliance/nists-cybersecurity-framework-has-become-the-common-language-for-international-cybersecurity-%EF%BF%BC?fbclid=IwAR3m_DbxP-CMtCyddgA6AM5jp_zFWobAvDICmpmHxuRwMq9DiD0Krz4NwZ8, 2022. Accessed: 2022-05-24.

[80] C. S. Hub. IMPLEMENTING A RISK-BASED CYBER SECURITY FRAMEWORK - The NIST CSF quick guide to clarity, readiness, buy-in and risk management for business security leaders. https://www.cshub.com/security-strategy/whitepapers/implementing-a-risk-base-cyber-security-framework, 2019. Accessed: 2022-05-11.

[81] IETF. RFC 3647 Internet X.509 Public Key Infrastructure — Certificate Policy and Certification Practices Framework. https://www.rfc-editor.org/rfc/rfc3647, 2003. Accessed: 2022-06-12.

[82] INFOBLOX. What is DNS Tunneling? https://www.infoblox.com/glossary/dns-tunneling/, 2021. Accessed: 2021-12-15.

[83] kaspersky. What is a Zero-day Attack? - Definition and Explanation. https://www.kaspersky.com/resource-center/definitions/zero-day-exploit, 2021. Accessed: 2021-12-15.

[84] lumin blog. Acesso remoto seguro: controlo de acesso aos funcionários em home office. https://www.lumiun.com/blog/acesso-remoto-seguro-controle-de-acesso-aos-funcionarios-em-home-office/, 2020. Accessed: 2022-01-15.

[85] Malwarebytes. Malware. https://pt.malwarebytes.com/malware/, 2021. Accessed: 2021-12-08.

[86] Microsoft. Microsoft Security Development Lifecycle. https://www.microsoft.com/en-us/securityengineering/sdl, 2021. Accessed: 2021-12-31.

[87] MITRE. Common Weakness Enumeration. https://cwe.mitre.org/, 2021. Accessed: 2021-12-27.

[88] S. Narang. CVE-2021-44228: Proof-of-Concept for Critical Apache Log4j Remote Code Execution Vulnerability Available (Log4Shell). https://www.tenable.com/blog/cve-2021-44228-proof-of-concept-for-critical-apache-log4j-remote-code-execution-vulnerability, 2021. Accessed: 2021-12-27.

[89] P. A. Networks. What is a denial of service attack (DoS) ? https://www.paloaltonetworks.com/cyberpedia/what-is-a-denial-of-service-attack-dos, 2021. Accessed: 2021-12-08.

[90] NIST. Framework for Improving Critical Infrastructure Cybersecurity (Version 1.1). https://doi.org/10.6028/NIST.CSWP.04162018, 2018. Accessed: 2021-12-10.

[91] NIST. NIST Special Publication 800-53 - Security and Privacy Controls for Information Systems and Organizations. https://doi.org/10.6028/NIST.SP.800-53r5, 2020. Accessed: 2021-12-10.

[92] NIST. NATIONAL VULNERABILITY DATABASE. https://nvd.nist.gov/, 2021. Accessed: 2021-12-27.

[93] NIST. Journey to the NIST Cybersecurity Framework (CSF) 2.0 | Workshop 1. https://www.nist.gov/news-events/events/2022/08/journey-nist-cybersecurity-framework-csf-20-workshop-1, 2022. Accessed: 2022-09-04.

[94] NIST. Updating the NIST Cybersecurity Framework – Journey To CSF 2.0. https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20, 2022. Accessed: 2022-09-04.

[95] NIST-NVD. CVE-2021-44228 Detail. https://nvd.nist.gov/vuln/detail/CVE-2021-44228, 2021. Accessed: 2021-12-27.

[96] S. E. of Philosophy. Quantum Computing. https://plato.stanford.edu/entries/qt-quantcomp/#PhysCompComp, 2019. Accessed: 2022-09-12.

[97] OSINT. OSINT Framework. https://osintframework.com/, 2022. Accessed: 2022-08-12.

[98] OWASP. OWASP Top 10 2017 - The Ten Most Critical Web Application Security Risks. *Https://Owasp.Org*, 1(1):1–25, 2017.

[99] PortSwigger. SQL injection. https://portswigger.net/web-security/sql-injection, 2021. Accessed: 2021-12-08.

[100] PurpleBox. What is Apache Log4J Vulnerability and How to Prevent It? https://www.prplbx.com/resources/blog/log4j/, 2021. Accessed: 2021-12-27.

[101] J. V. Rodrigues. Organizações portuguesas sofreram 881 ciberataques por semana em 2021. https://www.dinheirovivo.pt/empresas/tecnologia/organizacoes-portuguesas-sofreram-881-ciberataques-por-semana-em-2021-14476858.html, 2022. Accessed: 2022-09-12.

[102] K. Scarfone. How to develop a cybersecurity strategy: Step-by-step guide. https://searchsecurity.techtarget.com/tip/How-to-develop-a-cybersecurity-strategy-Step-by-step-guide, 2021. Accessed: 2021-12-08.

[103] SCEE. Política de Certificados do SCEE (Sistema de Certificação Eletrónica do Estado) e Requisitos Mínimos de Segurança. https://www.scee.gov.pt/media/7126/pcert-do-scee-v40.pdf, 2020. Accessed: 2022-06-12.

[104] I. SEGURA. Phishing. https://www.internetsegura.pt/Phishing, 2020. Accessed: 2021-12-08.

[105] E. Seguros. Cibercrimes aumentaram no primeiro semestre. https://eco.sapo.pt/2022/07/27/cibercrimes-aumentaram-no-primeiro-semestre/, 2022. Accessed: 2022-09-15.

[106] V. SHESHADRI. NIST FRAMEWORK: 5 PILLARS FOR YOUR CYBER SECURITY STRATEGY. https://riversafe.co.uk/tech-blog/nist-framework-5-pillars-for-your-cyber-security-strategy/, 2021. Accessed: 2021-12-11.

[107] VERACODE. Man in the Middle (MITM) Attack. https://www.veracode.com/security/man-middle-attack, 2021. Accessed: 2021-12-08.

[108] Wikipedia. Ciberataques à Estônia em 2007. https://pt.wikipedia.org/wiki/Ciberataques_à_Estónia_em_2007, 2019. Accessed: 2021-12-30.

[109] Wikipedia. Morris worm. https://en.wikipedia.org/wiki/Morris_worm, 2022. Accessed: 2022-09-12.

[110] C. Woody and R. Ellison. Building a Cybersecurity Strategy. https://doaj.org/article/6fe3379062dd40d18449bdb73ccf3d5b, 2020. Accessed: 2021-12-30.

[111] F. Wortley, C. Thompson, and F. Allison. Log4Shell: RCE 0-day exploit found in log4j 2, a popular Java logging package. https://www.lunasec.io/docs/blog/log4j-zero-day/, 2021. Accessed: 2021-12-27.

Parte III

APÊNDICES

A

MAPEAMENTO DO C2M2 V2.0 & CIS *CONTROLS* V8.0 PARA A NIST CSF V1.1

Neste apêndice, é apresentada uma proposta de mapeamento, de autoria própria, do *Cybersecurity Capability Maturity Model* (C2M2) v2.0 e do CIS *Controls* v8.0 para a NIST *Cybersecurity Framework* (NIST CSF) v1.1. Este mapeamento tem por base os documentos da NIST *Framework* [90], o *Implementation Guidance* do C2M2 [23], o C2M2 v2.0 [26], o mapeamento da CIS v8.0 para a NIST CSF [5] e as indicações do CIS CSAT sobre práticas de referência da NIST CSF [36]. Assim, as práticas do C2M2 e os controlos da CIS são apresentados conforme a seguinte notação:

- No C2M2, aparece a abreviatura do domínio, hífen e o número do objetivo e a letra da prática (por exemplo, ASSET-1a), sendo que as práticas pertencentes a uma determinada MIL estão na coluna respetiva (Nota: se aparecer a prática ASSET-1a na coluna da MIL1, significa que esta prática pertence ao MIL1, contudo também pertence ao MIL2 e MIL3);
  - **(Abreviatura do domínio)-(Número do objetivo nesse domínio)(letra da prática dentro desse domínio)**
- No CIS, aparece o número do controlo, uma vírgula e o número do subcontrolo em questão (por exemplo, o 3.º subcontrolo do controlo 16 é referenciado como: 16,3), sendo que os subcontrolos pertencentes a um determinado IG estão na coluna respetiva (Nota: Se aparecer o subcontrolo 3,10 na coluna do IG2, significa que este subcontrolo pertence ao IG2, mas também pertence ao IG3).
  - **(Número do controlo),(Número do subcontrolo)**

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
IDENTIFICAR (ID)	**Gestão de ativos (ID.AM):** Os dados, pessoal, dispositivos, sistemas e instalações que permitem à organização atingir objetivos empresariais são identificados e geridos de forma consistente com a sua importância relativa para os objetivos organizacionais e a estratégia de risco da organização.	**ID.AM-1** – Os dispositivos e sistemas físicos dentro da organização são inventariados.	· **CIS CSC** 1 · **COBIT 5** BAI09.01, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2 · **NIST SP 800-53 Rev. 4** CM-8, PM-5	ASSET-1a	ASSET-1b ASSET-1c ASSET-2b ASSET-2c	ASSET-1f ASSET-1g ASSET-2f ASSET-2g RISK-2h	1,1		
		ID.AM-2 – As plataformas e aplicações de software dentro da organização são inventariadas.	· **CIS CSC** 2 · **COBIT 5** BAI09.01, BAI09.02, BAI09.05 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISA 62443-3-3:2013** SR 7.8 · **ISO/IEC 27001:2013** A.8.1.1, A.8.1.2, A.12.5.1 · **NIST SP 800-53 Rev. 4** CM-8, PM-5	ASSET-1a	ASSET-1b ASSET-1c ASSET-2b ASSET-2c	ASSET-1f ASSET-1g ASSET-2f ASSET-2g RISK-2h	2,1 2,2	16,4	
		ID.AM-3 – Comunicação organizacional e fluxos de dados são mapeados.	· **CIS CSC** 12 · **COBIT 5** DSS05.02 · **ISA 62443-2-1:2009** 4.2.3.4 · **ISO/IEC 27001:2013** A.13.2.1, A.13.2.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CA-9, PL-8		RISK-3e SITUATION-3a	ASSET-1f ASSET-1g ASSET-2f ASSET-2g	1,1 4,5	3,8	
		ID.AM-4 – As redes e sistemas de informação externos estão identificados e catalogados.	· **CIS CSC** 12 · **COBIT 5** APO02.02, APO10.04, DSS01.02 · **ISO/IEC 27001:2013** A.11.2.6 · **NIST SP 800-53 Rev. 4** AC-20, SA-9	THIRD-PARTIES-1a THIRD-PARTIES-1b	THIRD-PARTIES-1c THIRD-PARTIES-1d	THIRD-PARTIES-1e		12,4 13,5 16,4	
		ID.AM-5 – Os recursos (por exemplo, hardware, dispositivos, dados, tempo, pessoal e software) são priorizados com base na sua classificação, criticidade e valor comercial.	· **CIS CSC** 13, 14 · **COBIT 5** APO03.03, APO03.04, APO12.01, BAI04.02, BAI09.02 · **ISA 62443-2-1:2009** 4.2.3.6 · **ISO/IEC 27001:2013** A.8.2.1 · **NIST SP 800-53 Rev. 4** CP-2, RA-2, SA-14, SC-6	ASSET-1a ASSET-2a ARCHITECTURE-3a	ASSET-1b ASSET-1c ASSET-1d ASSET-1e ASSET-2b ASSET-2c ASSET-2d ASSET-2e ARCHITECTURE-2b ARCHITECTURE-2d ARCHITECTURE-3b	RISK-2h	3,2	3,7	
		ID.AM-6: São estabelecidas funções e responsabilidades de cibersegurança para toda a força de trabalho e terceiros interessados (por exemplo, fornecedores, clientes, parceiros).	· **CIS CSC** 17, 19 · **COBIT 5** APO01.02, APO07.06, APO13.01, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1 · **NIST SP 800-53 Rev. 4** CP-2, PS-7, PM-11	WORKFORCE-1a WORKFORCE-1b	RISK-2f THIRD-PARTIES-2f THIRD-PARTIES-3a WORKFORCE-1c WORKFORCE-1d WORKFORCE-3e WORKFORCE-5a	ASSET-5e THREAT-3e THIRD-PARTIES-2h THIRD-PARTIES-3c THIRD-PARTIES-3e WORKFORCE-5e	14,1		

Figura 21: Mapeamento para a categoria "Gestão de Ativos" da função "Identificar" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
IDENTIFICAR (ID)	**Ambiente da Organização (ID.BE):** A missão, objetivos, partes interessadas e atividades da organização são compreendidas e priorizadas; esta informação é utilizada para informar as funções de cibersegurança, responsabilidades e decisões de gestão de risco.	**ID.BE-1** – O papel da organização na cadeia logística é identificado e comunicado.	· **COBIT 5** APO08.01, APO08.04, APO08.05, APO10.03, APO10.04, APO10.05 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** CP-2, SA-12	THIRD-PARTIES-1a	RISK-1c THIRD-PARTIES-1d	RISK-2k THIRD-PARTIES-1e			
		ID.BE-2: O lugar da organização em infraestruturas críticas e no seu setor industrial é identificado e comunicado.	· **COBIT 5** APO02.06, APO03.01 · **ISO/IEC 27001:2013** Clause 4.1 · **NIST SP 800-53 Rev. 4** PM-8	THIRD-PARTIES-1a	RISK-1c THIRD-PARTIES-1d PROGRAM-1c	RISK-1e RISK-1f RISK-2k RISK-2m THIRD-PARTIES-1e			
		ID.BE-3: As prioridades da missão, objetivos e atividades organizacionais são estabelecidas e comunicadas.	· **COBIT 5** APO02.01, APO02.06, APO03.01 · **ISA 62443-2-1:2009** 4.2.2.1, 4.2.3.6 · **NIST SP 800-53 Rev. 4** PM-11, SA-14		RISK-1c SITUATION-3a	RISK-1e RISK-1f RISK-2h			
		ID.BE-4: São estabelecidas dependências e funções críticas para a prestação de serviços críticos.	· **COBIT 5** APO10.01, BAI04.02, BAI09.02 · **ISO/IEC 27001:2013** A.11.2.2, A.11.2.3, A.12.1.3 · **NIST SP 800-53 Rev. 4** CP-8, PE-9, PE-11, PM-8, SA-14	ASSET-1a ASSET-2a THIRD-PARTIES-1a THIRD-PARTIES-1b	ASSET-1c ASSET-1d ASSET-1e ASSET-2c ASSET-2d ASSET-2e THIRD-PARTIES-1c THIRD-PARTIES-1d ARCHITECTURE-2b ARCHITECTURE-3h	ASSET-1f ASSET-1g ASSET-1h ASSET-2f ASSET-2g ASSET-2h RISK-2m THIRD-PARTIES-1e			
		ID.BE-5: São estabelecidos requisitos de resiliência para apoiar a prestação de serviços críticos para todos os estados operacionais (por exemplo, sob dureza/ataque, durante a recuperação, operações normais).	· **COBIT 5** BAI03.02, DSS04.02 · **ISO/IEC 27001:2013** A.11.1.4, A.17.1.1, A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-11, SA-13, SA-14	RESPONSE-4a RESPONSE-4b RESPONSE-4c	RESPONSE-4e RESPONSE-4f RESPONSE-4j RESPONSE-4k RESPONSE-4n ARCHITECTURE-1e	ARCHITECTURE-2l			

Figura 22: Mapeamento para a categoria "Ambiente da Organização" da função "Identificar" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
IDENTIFICAR (ID)	**Governação (ID.GV):** As políticas, procedimentos e processos para gerir e monitorizar os requisitos regulamentares, legais, de risco, ambientais e operacionais da organização são compreendidos e informam a gestão do risco de cibersegurança.	**ID.GV-1:** A política de cibersegurança organizacional é estabelecida e comunicada.	· **CIS CSC** 19 · **COBIT 5** APO01.03, APO13.01, EDM01.01, EDM01.02 · **ISA 62443-2-1:2009** 4.3.2.6 · **ISO/IEC 27001:2013** A.5.1.1 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families	PROGRAM-1a PROGRAM-2b	SITUATION-3a SITUATION-4a ARCHITECTURE-6a PROGRAM-2c PROGRAM-2e PROGRAM-2f PROGRAM-2h PROGRAM-3a	ASSET-5c THREAT-3c RISK-5c ACCESS-4c SITUATION-4c RESPONSE-5c THIRD-PARTIES-3c WORKFORCE-5c ARCHITECTURE-6c PROGRAM-2j PROGRAM-3c	14,1		
		ID.GV-2: As funções e responsabilidades de cibersegurança são coordenadas e alinhadas com as funções internas e os parceiros externos.	· **CIS CSC** 19 · **COBIT 5** APO01.02, APO10.03, APO13.02, DSS05.04 · **ISA 62443-2-1:2009** 4.3.2.3.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.15.1.1 · **NIST SP 800-53 Rev. 4** PS-7, PM-1, PM-2	WORKFORCE-1a WORKFORCE-1b ARCHITECTURE-1a	RISK-1d RISK-2f THIRD-PARTIES-2f THIRD-PARTIES-3a WORKFORCE-1c WORKFORCE-3d ARCHITECTURE-1b ARCHITECTURE-1c ARCHITECTURE-1d PROGRAM-1d PROGRAM-2g	THREAT-3e RISK-5e SITUATION-4e THIRD-PARTIES-2h THIRD-PARTIES-3c THIRD-PARTIES-3e WORKFORCE-1e WORKFORCE-1f WORKFORCE-5e ARCHITECTURE-6e PROGRAM-2i PROGRAM-3e		15,2 17,4	
		ID.GV-3: Os requisitos legais e regulamentares relativos à cibersegurança, incluindo as obrigações em matéria de privacidade e liberdades civis, são compreendidos e geridos.	· **CIS CSC** 19 · **COBIT 5** BAI02.01, MEA03.01, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.7 · **ISO/IEC 27001:2013** A.18.1.1, A.18.1.2, A.18.1.3, A.18.1.4, A.18.1.5 · **NIST SP 800-53 Rev. 4** -1 controls from all security control families		THIRD-PARTIES-2f ARCHITECTURE-1e PROGRAM-1g	ASSET-5c ASSET-5f THREAT-3c RISK-5c ACCESS-4c SITUATION-4c RESPONSE-3i RESPONSE-5c THIRD-PARTIES-2h THIRD-PARTIES-3c WORKFORCE-5c PROGRAM-2k			
		ID.GV-4: Os processos de governação e gestão de risco abordam os riscos de cibersegurança.	· **COBIT 5** EDM03.02, APO12.02, APO12.05, DSS04.02 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.3, 4.2.3.8, 4.2.3.9, 4.2.3.11, 4.3.2.4.3, 4.3.2.6.3 · **ISO/IEC 27001:2013** Clause 6 · **NIST SP 800-53 Rev. 4** SA-2, PM-3, PM-7, PM-9, PM-10, PM-11	RISK-2a RISK-3a RISK-4a	RISK-1d RISK-2c RISK-2d RISK-3e THIRD-PARTIES-2c	RISK-1e RISK-1f RISK-4d RISK-4e RISK-5c ARCHITECTURE-1i			

Figura 23: Mapeamento para a categoria "Governação" da função "Identificar" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
IDENTIFICAR (ID)	**Avaliação de risco (ID.RA):** A organização compreende o risco da cibersegurança para as operações organizacionais (incluindo missão, funções, imagem, ou reputação), bens organizacionais, e indivíduos.	**ID.RA-1:** As vulnerabilidades dos bens são identificadas e documentadas.	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04, DSS05.01, DSS05.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.7, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.12.6.1, A.18.2.3 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CA-8, RA-3, RA-5, SA-5, SA-11, SI-2, SI-4, SI-5	THREAT-1a THREAT-1b THREAT-1c RISK-2a	THREAT-1e THREAT-1f THREAT-1g THREAT-1h RISK-2c RISK-2e	THREAT-1j THREAT-1k RISK-2i	7,1 7,2 7,4		
		ID.RA-2: A informação sobre ameaças cibernéticas é recebida de fóruns e fontes de partilha de informação.	· **CIS CSC** 4 · **COBIT 5** BAI08.01 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15, PM-16	THREAT-1a THREAT-1b THREAT-2a THREAT-2b	THREAT-1e RISK-2c	RISK-2j RISK-2k SITUATION-3f SITUATION-3g			
		ID.RA-3: As ameaças, tanto internas como externas, são identificadas e documentadas.	· **CIS CSC** 4 · **COBIT 5** APO12.01, APO12.02, APO12.03, APO12.04 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-3, SI-5, PM-12, PM-16	THREAT-2a THREAT-2b RISK-2a	THREAT-2d THREAT-2e RISK-2c RISK-2e	THREAT-2h THREAT-2i RISK-2h RISK-2j RISK-2k			
		ID.RA-4: São identificados os potenciais impactos e probabilidades de negócio.	· **CIS CSC** 4 · **COBIT 5** DSS04.02 · **ISA 62443-2-1:2009** 4.2.3, 4.2.3.9, 4.2.3.12 · **ISO/IEC 27001:2013** A.16.1.6, Clause 6.1.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-14, PM-9, PM-11	RISK-3a	THREAT-2d THREAT-2f RISK-2e RISK-3b RISK-3c RISK-3f	THREAT-2h THREAT-2i ARCHITECTURE-1g			
		ID.RA-5: Ameaças, vulnerabilidades, probabilidades e impactos são utilizados para determinar o risco.	· **CIS CSC** 4 · **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, PM-16	RISK-2a RISK-3a	RISK-2c RISK-2e RISK-3b RISK-3f	THREAT-1k RISK-2h RISK-2i RISK-2j		3,7 7,6	
		ID.RA-6: As respostas ao risco são identificadas e priorizadas.	· **CIS CSC** 4 · **COBIT 5** APO12.05, APO13.02 · **ISO/IEC 27001:2013** Clause 6.1.3 · **NIST SP 800-53 Rev. 4** PM-4, PM-9	RISK-2a RISK-3a RISK-4a	THREAT-2d RISK-2b RISK-2e RISK-3b RISK-3c RISK-3d RISK-4b	THREAT-2h THREAT-2i RISK-3g RISK-4d RISK-4e RESPONSE-2h			

Figura 24: Mapeamento para a categoria "Avaliação de Risco" da função "Identificar" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
IDENTIFICAR (ID)	**Estratégia de Gestão de Risco (ID.RM):** As prioridades, restrições, tolerâncias de risco e pressupostos da organização são estabelecidos e utilizados para apoiar decisões de risco operacional.	**ID.RM-1:** Os processos de gestão de risco são estabelecidos, geridos e acordados pelos intervenientes organizacionais.	· **CIS CSC** 4 · **COBIT 5** APO12.04, APO12.05, APO13.02, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3, Clause 9.3 · **NIST SP 800-53 Rev. 4** PM-9	RISK-1a RISK-2a RISK-3a RISK-4a	RISK-1b RISK-1c RISK-1d RISK-2b RISK-2c RISK-2d RISK-2e RISK-2f RISK-2g RISK-3b RISK-3c RISK-3d RISK-3e RISK-3f RISK-4b RISK-5a RISK-5b	RISK-1e RISK-1f RISK-2h RISK-2i RISK-2j RISK-2k RISK-2l RISK-2m RISK-3g RISK-4c RISK-4d RISK-4e RISK-5d RISK-5e RISK-5f			
		ID.RM-2: A tolerância ao risco organizacional é determinada e claramente expressa.	· **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.2.6.5 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** PM-9		RISK-1c RISK-3b RISK-3c	RISK-4d			
		ID.RM-3: A determinação da tolerância ao risco da organização é informada pelo seu papel na infraestrutura crítica e na análise de risco específica do setor.	· **COBIT 5** APO12.02 · **ISO/IEC 27001:2013** Clause 6.1.3, Clause 8.3 · **NIST SP 800-53 Rev. 4** SA-14, PM-8, PM-9, PM-11		RISK-3b RISK-3c	RISK-1e RISK-1f RISK-4d			

Figura 25: Mapeamento para a categoria "Estratégia de Gestão de Risco" da função "Identificar" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
IDENTIFICAR (ID)	**Gestão do Risco da Cadeia Logística (ID.SC):** As prioridades, restrições, tolerâncias de risco e suposições da organização são estabelecidas e utilizadas para apoiar decisões de risco associadas à gestão do risco da cadeia logística. A organização estabeleceu e implementou os processos para identificar, avaliar e gerir os riscos da cadeia de fornecimento.	**ID.SC-1:** Os processos cibernéticos de gestão de risco da cadeia de logística são identificados, estabelecidos, avaliados, geridos e acordados pelos intervenientes organizacionais.	· **CIS CSC** 4 · **COBIT 5** APO10.01, APO10.04, APO12.04, APO12.05, APO13.02, BAI01.03, BAI02.03, BAI04.02 · **ISA 62443-2-1:2009** 4.3.4.2 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3, A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** SA-9, SA-12, PM-9	THIRD-PARTIES-2a THIRD-PARTIES-2b	THIRD-PARTIES-2c THIRD-PARTIES-2d THIRD-PARTIES-2e THIRD-PARTIES-2f THIRD-PARTIES-3a ARCHITECTURE-4b	RISK-2k RISK-2m THIRD-PARTIES-2h THIRD-PARTIES-2i THIRD-PARTIES-2j THIRD-PARTIES-3c THIRD-PARTIES-3e THIRD-PARTIES-3f ARCHITECTURE-4e		15,2	
		ID.SC-2: Os fornecedores e terceiras partes de sistemas de informação, componentes e serviços são identificados, priorizados e avaliados utilizando um processo de avaliação de risco da cadeia de fornecimento cibernética.	· **COBIT 5** APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** RA-2, RA-3, SA-12, SA-14, SA-15, PM-9	THIRD-PARTIES-1a THIRD-PARTIES-1b THIRD-PARTIES-2a THIRD-PARTIES-2b	THIRD-PARTIES-1c THIRD-PARTIES-1d THIRD-PARTIES-2c THIRD-PARTIES-2d THIRD-PARTIES-2e THIRD-PARTIES-2g	RISK-2k RISK-2m THIRD-PARTIES-1e THIRD-PARTIES-2i THIRD-PARTIES-2j THIRD-PARTIES-2k THIRD-PARTIES-3d THIRD-PARTIES-3f	15,1	15,3	15,5
		ID.SC-3: Os contratos com fornecedores e terceiras partes são utilizados para implementar medidas apropriadas concebidas para cumprir os objetivos do programa de cibersegurança de uma organização e do Plano de Gestão de Riscos da Cadeia de Fornecimento Cibernética.	· **COBIT 5** APO10.01, APO10.02, APO10.03, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.6.4, 4.3.2.6.7 · **ISO/IEC 27001:2013** A.15.1.1, A.15.1.2, A.15.1.3 · **NIST SP 800-53 Rev. 4** SA-9, SA-11, SA-12, PM-9		THIRD-PARTIES-2f	THIRD-PARTIES-2h THIRD-PARTIES-3c THIRD-PARTIES-3e PROGRAM-2l		15,4	
		ID.SC-4: Os fornecedores e terceiras partes são rotineiramente avaliados utilizando auditorias, resultados de testes, ou outras formas de avaliação para confirmar que estão a cumprir as suas obrigações contratuais.	· **COBIT 5** APO10.01, APO10.03, APO10.04, APO10.05, MEA01.01, MEA01.02, MEA01.03, MEA01.04, MEA01.05 · **ISA 62443-2-1:2009** 4.3.2.6.7 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.15.2.1, A.15.2.2 · **NIST SP 800-53 Rev. 4** AU-2, AU-6, AU-12, AU-16, PS-7, SA-9, SA-12		THIRD-PARTIES-2d THIRD-PARTIES-2g THIRD-PARTIES-3b	THIRD-PARTIES-2k THIRD-PARTIES-3d THIRD-PARTIES-3f			15,5
		ID.SC-5: O planeamento e testes de resposta e recuperação são conduzidos com fornecedores e fornecedores terceiros.	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 2.8, SR 3.3, SR.6.1, SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-4, IR-3, IR-4, IR-6, IR-8, IR-9			RESPONSE-3i RESPONSE-3j	11,1		

Figura 26: Mapeamento para a categoria "Gestão do Risco da Cadeia Logística" da função "Identificar" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
PROTEGER (PR)	**Gestão de Identidades, Autenticação e Controlo de Acessos (PR.AC):** O acesso a bens físicos e lógicos e instalações associadas é limitado a utilizadores, processos e dispositivos autorizados, gerido de forma consistente com o risco avaliado de acesso não autorizado a atividades e transações autorizadas.	**PR.AC-1:** As identidades e credenciais são emitidas, geridas, verificadas, revogadas e auditadas para dispositivos, utilizadores e processos autorizados.	· **CIS CSC** 1, 5, 15, 16 · **COBIT 5** DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.5.1 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.7, SR 1.8, SR 1.9 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.2, A.9.2.3, A.9.2.4, A.9.2.6, A.9.3.1, A.9.4.2, A.9.4.3 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, IA-1, IA-2, IA-3, IA-4, IA-5, IA-6, IA-7, IA-8, IA-9, IA-10, IA-11	ACCESS-1a ACCESS-1b ACCESS-1c	ACCESS-1d ACCESS-1e ACCESS-1f ACCESS-4a THIRD-PARTIES-1b ARCHITECTURE-1f	RISK-2l ACCESS-4e ARCHITECTURE-1h	4,7 5,1 5,3 6,1 6,2	5,5 6,6 6,7	13,9 15,7
		PR.AC-2: O acesso físico aos bens é gerido e protegido.	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.2, 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2, A.11.1.3, A.11.1.4, A.11.1.5, A.11.1.6, A.11.2.1, A.11.2.3, A.11.2.5, A.11.2.6, A.11.2.7, A.11.2.8 · **NIST SP 800-53 Rev. 4** PE-2, PE-3, PE-4, PE-5, PE-6, PE-8	ACCESS-3a ACCESS-3b ACCESS-3c	ACCESS-3d ACCESS-3e ACCESS-3f ACCESS-3g ARCHITECTURE-3h	ACCESS-3h			
		PR.AC-3: O acesso remoto é gerido.	· **CIS CSC** 12 · **COBIT 5** APO13.01, DSS01.04, DSS05.03 · **ISA 62443-2-1:2009** 4.3.3.6.6 · **ISA 62443-3-3:2013** SR 1.13, SR 2.6 · **ISO/IEC 27001:2013** A.6.2.1, A.6.2.2, A.11.2.6, A.13.1.1, A.13.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-17, AC-19, AC-20, SC-15	ACCESS-2a ACCESS-2b	ACCESS-2c ACCESS-2d ACCESS-2e ACCESS-2f ACCESS-2g ARCHITECTURE-3h	RISK-2l ACCESS-2h ARCHITECTURE-1h ARCHITECTURE-2j	6,4	4,11 6,6 12,7 13,5	
		PR.AC-4: As permissões e autorizações de acesso são geridas, incorporando os princípios do privilégio mínimo e da separação de responsabilidades.	· **CIS CSC** 3, 5, 12, 14, 15, 16, 18 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.7.3 · **ISA 62443-3-3:2013** SR 2.1 · **ISO/IEC 27001:2013** A.6.1.2, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24		ACCESS-2c ACCESS-2d ACCESS-2e ACCESS-3d ACCESS-3e ACCESS-4a THIRD-PARTIES-1b ARCHITECTURE-1f ARCHITECTURE-2c ARCHITECTURE-3c ARCHITECTURE-3h	RISK-2l ACCESS-4c ACCESS-4e ARCHITECTURE-1h ARCHITECTURE-2j	3,3 5,4		6,8
		PR.AC-5: A integridade da rede é protegida (por exemplo, segregação da rede, segmentação da rede).	· **CIS CSC** 9, 14, 15, 18 · **COBIT 5** DSS01.05, DSS05.02 · **ISA 62443-2-1:2009** 4.3.3.4 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8 · **ISO/IEC 27001:2013** A.13.1.1, A.13.1.3, A.13.2.1, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-10, SC-7	ARCHITECTURE-2a	RESPONSE-4i ARCHITECTURE-1f ARCHITECTURE-2b ARCHITECTURE-2d	RISK-2l ARCHITECTURE-1h ARCHITECTURE-2g ARCHITECTURE-2h ARCHITECTURE-2i ARCHITECTURE-2l	9,2	3,12 9,3 9,6 12,2 13,4	12,8 16,14
		PR.AC-6: As identidades são revistas, vinculadas a credenciais e confirmadas em interações.	· **CIS CSC**, 16 · **COBIT 5** DSS05.04, DSS05.05, DSS05.07, DSS06.03 · **ISA 62443-2-1:2009** 4.3.3.2.2, 4.3.3.5.2, 4.3.3.7.2, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.4, SR 1.5, SR 1.9, SR 2.1 · **ISO/IEC 27001:2013**, A.7.1.1, A.9.2.1 · **NIST SP 800-53 Rev. 4** AC-1, AC-2, AC-3, AC-16, AC-19, AC-24, IA-1, IA-2, IA-4, IA-5, IA-8, PE-2, PS-3	ACCESS-1b	ACCESS-1d ACCESS-4a	ACCESS-4c ACCESS-4f			13,9
		PR.AC-7: Os utilizadores, dispositivos e outros ativos são autenticados (por exemplo, single-factor, multi-factor) proporcional ao risco da transação (por exemplo, riscos de segurança e privacidade dos indivíduos e outros riscos organizacionais).	· **CIS CSC** 1, 12, 15, 16 · **COBIT 5** DSS05.04, DSS05.10, DSS06.10 · **ISA 62443-2-1:2009** 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.5, SR 1.7, SR 1.8, SR 1.9, SR 1.10 · **ISO/IEC 27001:2013** A.9.2.1, A.9.2.4, A.9.3.1, A.9.4.2, A.9.4.3, A.18.1.4 · **NIST SP 800-53 Rev. 4** AC-7, AC-8, AC-9, AC-11, AC-12, AC-14, IA-1, IA-2, IA-3, IA-4, IA-5, IA-8, IA-9, IA-10, IA-11		ACCESS-1f ACCESS-4a ARCHITECTURE-1f ARCHITECTURE-3h	RISK-2l ACCESS-4c ARCHITECTURE-1h ARCHITECTURE-2j ARCHITECTURE-2k	6,3 6,4 6,5	12,3 12,6 12,7 13,5	

Figura 27: Mapeamento para a categoria "Gestão de Identidades, Autenticação e Controlo de Acessos" da função "Proteger" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
PROTEGER (PR)	**Formação e Sensibilização (PR.AT):** Os colaboradores e os parceiros da organização recebem educação sobre cibersegurança sendo formados para desempenhar as suas funções e responsabilidades relacionadas com a cibersegurança de forma consistente com as políticas, procedimentos e acordos relacionados.	**PR.AT-1:** Todos os utilizadores estão informados e formados.	· **CIS CSC** 17, 18 · **COBIT 5** APO07.03, BAI05.07 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.7.2.2, A.12.2.1 · **NIST SP 800-53 Rev. 4** AT-2, PM-13	WORKFORCE-2a WORKFORCE-2b WORKFORCE-4a	WORKFORCE-2c WORKFORCE-2d WORKFORCE-3e WORKFORCE-4b WORKFORCE-4c WORKFORCE-5b ARCHITECTURE-4a	ASSET-5d THREAT-3d RISK-5d ACCESS-4d SITUATION-4d RESPONSE-5d THIRD-PARTIES-3d WORKFORCE-2e WORKFORCE-2f WORKFORCE-4d WORKFORCE-4e WORKFORCE-5d ARCHITECTURE-4d ARCHITECTURE-6d PROGRAM-3d	14,1 14,2 14,3 14,4 14,5 14,6 14,7 14,8 17,3	14,9 16,9	
		PR.AT-2: Os utilizadores privilegiados compreendem os seus papéis e responsabilidades.	· **CIS CSC** 5, 17, 18 · **COBIT 5** APO07.02, DSS05.04, DSS06.03 · **ISA 62443-2-1:2009** 4.3.2.4.2, 4.3.2.4.3 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13	WORKFORCE-1a WORKFORCE-1b	WORKFORCE-1c WORKFORCE-1d WORKFORCE-3e	THREAT-3e ACCESS-4e WORKFORCE-1e WORKFORCE-1f		14,9 16,9	
		PR.AT-3: Os terceiros interessados (por exemplo, fornecedores, clientes, parceiros) compreendem as suas funções e responsabilidades.	· **CIS CSC** 17 · **COBIT 5** APO07.03, APO07.06, APO10.04, APO10.05 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** PS-7, SA-9, SA-16	WORKFORCE-1a WORKFORCE-1b	THIRD-PARTIES-2f THIRD-PARTIES-3a WORKFORCE-1c WORKFORCE-1d WORKFORCE-3e	THIRD-PARTIES-2h THIRD-PARTIES-3c THIRD-PARTIES-3e WORKFORCE-1e WORKFORCE-1f		15,4	
		PR.AT-4: Os altos executivos compreendem as suas funções e responsabilidades.	· **CIS CSC** 17, 19 · **COBIT 5** EDM01.01, APO01.02, APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, PM-13	WORKFORCE-1a WORKFORCE-1b	WORKFORCE-1c WORKFORCE-1d WORKFORCE-3e	WORKFORCE-1e WORKFORCE-1f		14,9	
		PR.AT-5: O pessoal da segurança física e da segurança da informação compreendem as suas funções & responsabilidades.	· **CIS CSC** 17 · **COBIT 5** APO07.03 · **ISA 62443-2-1:2009** 4.3.2.4.2 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** AT-3, IR-2, PM-13	WORKFORCE-1a WORKFORCE-1b	RISK-2f WORKFORCE-1c WORKFORCE-1d WORKFORCE-3e	ASSET-5e WORKFORCE-1e WORKFORCE-1f		14,9	

Figura 28: Mapeamento para a categoria "Formação e Sensibilização" da função "Proteger" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
PROTEGER (PR)	**Segurança de Dados (PR.DS):** A informação e os registos (dados) são geridos conforme a estratégia de risco da organização para proteger a confidencialidade, integridade, e disponibilidade da informação.	**PR.DS-1:** Os dados em repouso estão protegidos.	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, BAI02.01, BAI06.01, DSS04.07, DSS05.03, DSS06.06 · **ISA 62443-3-3:2013** SR 3.4, SR 4.1 · **ISO/IEC 27001:2013** A.8.2.3 · **NIST SP 800-53 Rev. 4** MP-8, SC-12, SC-28	THREAT-1d THREAT-2c ARCHITECTURE-5a	ARCHITECTURE-1f ARCHITECTURE-5b ARCHITECTURE-5d ARCHITECTURE-5e	RISK-2l ARCHITECTURE-1h	11,3 11,4	3,11 16,11	
		PR.DS-2: Os dados em trânsito são protegidos.	· **CIS CSC** 13, 14 · **COBIT 5** APO01.06, DSS05.02, DSS06.06 · **ISA 62443-3-3:2013** SR 3.1, SR 3.8, SR 4.1, SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** SC-8, SC-11, SC-12	THREAT-1d THREAT-2c	ARCHITECTURE-1f ARCHITECTURE-5c ARCHITECTURE-5d ARCHITECTURE-5e	RISK-2l ARCHITECTURE-1h		3,10 12,3 12,6 12,7 16,11	
		PR.DS-3: Os bens são formalmente geridos durante a remoção, transferências, e disposição.	· **CIS CSC** 1 · **COBIT 5** BAI09.03 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.4.4.1 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.8.3.3, A.11.2.5, A.11.2.7 · **NIST SP 800-53 Rev. 4** CM-8, MP-6, PE-16	ASSET-4a ASSET-4b ARCHITECTURE-3a	ASSET-4c ASSET-4d ASSET-5a ASSET-5b ARCHITECTURE-1f ARCHITECTURE-3b ARCHITECTURE-3h	ASSET-4f ASSET-5c ASSET-5f RISK-2l ARCHITECTURE-1h	1,1 1,2 3,5		
		PR.DS-4: Capacidade adequada para assegurar a manutenção da disponibilidade.	· **CIS CSC** 1, 2, 13 · **COBIT 5** APO13.01, BAI04.04 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.12.1.3, A.17.2.1 · **NIST SP 800-53 Rev. 4** AU-4, CP-2, SC-5	THREAT-1d THREAT-2c	ARCHITECTURE-1f	THREAT-2j RISK-2l ARCHITECTURE-1h	3,4	8,9	
		PR.DS-5: As proteções contra fugas de dados são implementadas.	· **CIS CSC** 13 · **COBIT 5** APO01.06, DSS05.04, DSS05.07, DSS06.02 · **ISA 62443-3-3:2013** SR 5.2 · **ISO/IEC 27001:2013** A.6.1.2, A.7.1.1, A.7.1.2, A.7.3.1, A.8.2.2, A.8.2.3, A.9.1.1, A.9.1.2, A.9.2.3, A.9.4.1, A.9.4.4, A.9.4.5, A.10.1.1, A.11.1.4, A.11.1.5, A.11.2.1, A.13.1.1, A.13.1.3, A.13.2.1, A.13.2.3, A.13.2.4, A.14.1.2, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-5, AC-6, PE-19, PS-3, PS-6, SC-7, SC-8, SC-13, SC-31, SI-4	THREAT-1d THREAT-2c	ARCHITECTURE-1f ARCHITECTURE-5f	THREAT-1l RISK-2l ARCHITECTURE-1h ARCHITECTURE-5g	2,2		3,13 16,14
		PR.DS-6: Os mecanismos de verificação da integridade são utilizados para verificar o software, firmware e integridade da informação.	· **CIS CSC** 2, 3 · **COBIT 5** APO01.06, BAI06.01, DSS06.02 · **ISA 62443-3-3:2013** SR 3.1, SR 3.3, SR 3.4, SR 3.8 · **ISO/IEC 27001:2013** A.12.2.1, A.12.5.1, A.14.1.2, A.14.1.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** SC-16, SI-7		SITUATION-2d ARCHITECTURE-1f ARCHITECTURE-3h ARCHITECTURE-4b	RISK-2l SITUATION-2h ARCHITECTURE-1h ARCHITECTURE-3i ARCHITECTURE-4e ARCHITECTURE-4f ARCHITECTURE-4g ARCHITECTURE-4h ARCHITECTURE-5h		2,5 2,6 11,5	2,7 3,14
		PR.DS-7: O(s) ambiente(s) de desenvolvimento e teste são separados do(s) ambiente(s) de produção.	· **CIS CSC** 18, 20 · **COBIT 5** BAI03.08, BAI07.04 · **ISO/IEC 27001:2013** A.12.1.4 · **NIST SP 800-53 Rev. 4** CM-2		ASSET-4c ARCHITECTURE-1f ARCHITECTURE-4a	ASSET-4e RISK-2l ARCHITECTURE-1h ARCHITECTURE-4d ARCHITECTURE-4h		16,8	
		PR.DS-8: Os mecanismos de verificação da integridade são utilizados para verificar a integridade do hardware.	· **COBIT 5** BAI03.05 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISO/IEC 27001:2013** A.11.2.4 · **NIST SP 800-53 Rev. 4** SA-10, SI-7		ARCHITECTURE-1f ARCHITECTURE-3h	RISK-2l ARCHITECTURE-1h			16,14

Figura 29: Mapeamento para a categoria "Segurança de Dados" da função "Proteger" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
PROTEGER (PR)	**Procedimentos e Processos de Proteção da Informação (PR.IP):** As políticas de segurança (que abordam o objetivo, âmbito, funções, responsabilidades, compromisso de gestão e coordenação entre entidades organizacionais), processos e procedimentos são mantidos e utilizados para gerir a proteção dos sistemas e bens de informação.	**PR.IP-1:** É criada e mantida uma configuração de base de tecnologia de informação/sistemas de controlo industrial incorporando princípios de segurança (por exemplo, conceito de menor funcionalidade).	· **CIS CSC** 3, 9, 11 · **COBIT 5** BAI10.01, BAI10.02, BAI10.03, BAI10.05 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9, SA-10	ASSET-3a	ASSET-3b ARCHITECTURE-1e ARCHITECTURE-2c ARCHITECTURE-3d ARCHITECTURE-3e ARCHITECTURE-3f	ASSET-3c ASSET-3d ASSET-3e ASSET-3f THREAT-2j SITUATION-3h ARCHITECTURE-1j	4,1 4,2 4,3 7,3 9,1	9,4 9,5 10,5 16,1 16,7	2,7
		PR.IP-2: É implementado um ciclo de vida de desenvolvimento de sistemas para gerir os sistemas.	· **CIS CSC** 18 · **COBIT 5** APO13.01, BAI03.01, BAI03.02, BAI03.03 · **ISA 62443-2-1:2009** 4.3.4.3.3 · **ISO/IEC 27001:2013** A.6.1.5, A.14.1.1, A.14.2.1, A.14.2.5 · **NIST SP 800-53 Rev. 4** PL-8, SA-3, SA-4, SA-8, SA-10, SA-11, SA-12, SA-15, SA-17, SI-12, SI-13, SI-14, SI-16, SI-17	ARCHITECTURE-3a	ASSET-4d ARCHITECTURE-3b ARCHITECTURE-3h ARCHITECTURE-4a ARCHITECTURE-4c	ARCHITECTURE-3i ARCHITECTURE-4d ARCHITECTURE-4h		16,5 16,10	16,12
		PR.IP-3: Os processos de controlo de alteração de configuração estão em vigor.	· **CIS CSC** 3, 11 · **COBIT 5** BAI01.06, BAI06.01 · **ISA 62443-2-1:2009** 4.3.4.3.2, 4.3.4.3.3 · **ISA 62443-3-3:2013** SR 7.6 · **ISO/IEC 27001:2013** A.12.1.2, A.12.5.1, A.12.6.2, A.14.2.2, A.14.2.3, A.14.2.4 · **NIST SP 800-53 Rev. 4** CM-3, CM-4, SA-10	ASSET-4a ASSET-4b	ASSET-4c ASSET-4d ASSET-5a	ASSET-4e ASSET-4f ASSET-5c ASSET-5f	4,2		
		PR.IP-4: São realizados, mantidos e testados os backups de informação.	· **CIS CSC** 10 · **COBIT 5** APO13.01, DSS01.01, DSS04.07 · **ISA 62443-2-1:2009** 4.3.4.3.9 · **ISA 62443-3-3:2013** SR 7.3, SR 7.4 · **ISO/IEC 27001:2013** A.12.3.1, A.17.1.2, A.17.1.3, A.18.1.3 · **NIST SP 800-53 Rev. 4** CP-4, CP-6, CP-9	RESPONSE-4b RESPONSE-4c	RESPONSE-4e RESPONSE-4f RESPONSE-4h RESPONSE-4i RESPONSE-4j		11,2 11,3		
		PR.IP-5: A política e os regulamentos relativos ao ambiente físico operacional para bens organizacionais são cumpridos.	· **COBIT 5** DSS01.04, DSS05.05 · **ISA 62443-2-1:2009** 4.3.3.3.1 4.3.3.3.2, 4.3.3.3.3, 4.3.3.3.5, 4.3.3.3.6 · **ISO/IEC 27001:2013** A.11.1.4, A.11.2.1, A.11.2.2, A.11.2.3 · **NIST SP 800-53 Rev. 4** PE-10, PE-12, PE-13, PE-14, PE-15, PE-18			ASSET-5c ASSET-5f RISK-2l RISK-5c ARCHITECTURE-1h			
		PR.IP-6: Os dados são destruídos consoante a política.	· **COBIT 5** BAI09.03, DSS05.06 · **ISA 62443-2-1:2009** 4.3.4.4.4 · **ISA 62443-3-3:2013** SR 4.2 · **ISO/IEC 27001:2013** A.8.2.3, A.8.3.1, A.8.3.2, A.11.2.7 · **NIST SP 800-53 Rev. 4** MP-6		ASSET-4d	ASSET-1i ASSET-2i	3,1 3,5		

Figura 30: Mapeamento para a categoria "Procedimentos e Processos de Proteção da Informação" da função "Proteger" da NIST *Framework Core* (1/2)

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
PROTEGER (PR)	**Procedimentos e Processos de Proteção da Informação (PR.IP):** As políticas de segurança (que abordam o objetivo, âmbito, funções, responsabilidades, compromisso de gestão e coordenação entre entidades organizacionais), processos e procedimentos são mantidos e utilizados para gerir a proteção dos sistemas e bens de informação.	**PR.IP-7:** Os processos de proteção são melhorados.	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.1, 4.4.3.2, 4.4.3.3, 4.4.3.4, 4.4.3.5, 4.4.3.6, 4.4.3.7, 4.4.3.8 · **ISO/IEC 27001:2013** A.16.1.6, Clause 9, Clause 10 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-8, PL-2, PM-6	ARCHITECTURE-1a PROGRAM-1a PROGRAM-2a	RISK-1b SITUATION-4b ARCHITECTURE-1b ARCHITECTURE-6b PROGRAM-1b PROGRAM-1e PROGRAM-1f PROGRAM-2d PROGRAM-3b	SITUATION-4f RESPONSE-4m ARCHITECTURE-6f PROGRAM-1h PROGRAM-3f		18,1	16,14
		PR.IP-8: A eficácia das tecnologias de proteção é partilhada.	· **COBIT 5** BAI08.04, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4** AC-21, CA-7, SI-4		SITUATION-3a SITUATION-3c	SITUATION-3d			
		PR.IP-9: Planos de resposta (Resposta a incidentes e continuidade dos negócios) e planos de recuperação (Recuperação de Incidentes e Recuperação de Catástrofes) estão em vigor e são geridos.	· **CIS CSC** 19 · **COBIT 5** APO12.06, DSS04.03 · **ISA 62443-2-1:2009** 4.3.2.5.3, 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.1, A.17.1.1, A.17.1.2, A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-2, CP-7, CP-12, CP-13, IR-7, IR-8, IR-9, PE-17	RESPONSE-4a	THREAT-2d RESPONSE-3d RESPONSE-3e RESPONSE-4d RESPONSE-4g RESPONSE-5a	THREAT-2h THREAT-2j RESPONSE-3h RESPONSE-3k RESPONSE-4m RESPONSE-4o RESPONSE-4q RESPONSE-5c RESPONSE-5d RESPONSE-5e RESPONSE-5f	11,1 17,1 17,3	17,4	
		PR.IP-10: Os planos de resposta e recuperação são testados.	· **CIS CSC** 19, 20 · **COBIT 5** DSS04.04 · **ISA 62443-2-1:2009** 4.3.2.5.7, 4.3.4.5.11 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.17.1.3 · **NIST SP 800-53 Rev. 4** CP-4, IR-3, PM-14		RESPONSE-3f RESPONSE-4g	RESPONSE-3h RESPONSE-3j RESPONSE-4o RESPONSE-4q		17,7	
		PR.IP-11: A cibersegurança está incluída nas práticas de recursos humanos (por exemplo, desprovisionamento, rastreio de pessoal).	· **CIS CSC** 5, 16 · **COBIT 5** APO07.01, APO07.02, APO07.03, APO07.04, APO07.05 · **ISA 62443-2-1:2009** 4.3.3.2.1, 4.3.3.2.2, 4.3.3.2.3 · **ISO/IEC 27001:2013** A.7.1.1, A.7.1.2, A.7.2.1, A.7.2.2, A.7.2.3, A.7.3.1, A.8.1.4 · **NIST SP 800-53 Rev. 4** PS-1, PS-2, PS-3, PS-4, PS-5, PS-6, PS-7, PS-8, SA-21	WORKFORCE-3a WORKFORCE-3b WORKFORCE-4a	WORKFORCE-3c WORKFORCE-3d WORKFORCE-3e WORKFORCE-4b WORKFORCE-4c WORKFORCE-5b	WORKFORCE-3f WORKFORCE-3g WORKFORCE-4d WORKFORCE-4e WORKFORCE-5f	6,2		
		PR.IP-12: É desenvolvido e implementado um plano de gestão de vulnerabilidades.	· **CIS CSC** 4, 18, 20 · **COBIT 5** BAI03.10, DSS05.01, DSS05.02 · **ISO/IEC 27001:2013** A.12.6.1, A.14.2.3, A.16.1.3, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** RA-3, RA-5, SI-2		THREAT-1h THREAT-3a THREAT-3b ARCHITECTURE-4a	THREAT-1l THREAT-3c THREAT-3e THREAT-3f RISK-2i ARCHITECTURE-4d ARCHITECTURE-4h		7,6	

Figura 31: Mapeamento para a categoria "Procedimentos e Processos de Proteção da Informação" da função "Proteger" da NIST *Framework Core* (2/2)

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
PROTEGER (PR)	**Manutenção (PR.MA):** A manutenção e reparação dos componentes do sistema de controlo industrial e de informação são executadas conforme as políticas e procedimentos.	**PR.MA-1:** Manutenção e reparação de bens organizacionais são executados e registados, com ferramentas aprovadas e controladas.	· **COBIT 5** BAI03.10, BAI09.02, BAI09.03, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.7 · **ISO/IEC 27001:2013** A.11.1.2, A.11.2.4, A.11.2.5, A.11.2.6 · **NIST SP 800-53 Rev. 4** MA-2, MA-3, MA-5, MA-6	ASSET-4b ACCESS-3a ACCESS-3b ACCESS-3c SITUATION-1a	ASSET-5b ACCESS-3d ACCESS-3g ACCESS-4b SITUATION-1b	ASSET-4f ACCESS-3h SITUATION-1e			
		PR.MA-2: A manutenção remota de bens organizacionais é aprovada, registada e executada de forma a impedir o acesso não autorizado.	· **CIS CSC** 3, 5 · **COBIT 5** DSS05.04 · **ISA 62443-2-1:2009** 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8 · **ISO/IEC 27001:2013** A.11.2.4, A.15.1.1, A.15.2.1 · **NIST SP 800-53 Rev. 4** MA-4	ACCESS-2a ACCESS-2b SITUATION-1a RESPONSE-1a	ACCESS-2c ACCESS-2d ACCESS-2e ACCESS-2f ACCESS-2g SITUATION-1b	ACCESS-2h ACCESS-4f SITUATION-1e ARCHITECTURE-2j ARCHITECTURE-2k		13,5	

Figura 32: Mapeamento para a categoria "Manutenção" da função "Proteger" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
PROTEGER (PR)	**Tecnologia de Proteção (PR.PT):** As soluções técnicas de segurança são geridas para garantir a segurança e resiliência dos sistemas e bens, de acordo com as políticas, procedimentos e acordos relacionados.	**PR.PT-1:** Os registos de auditoria/log são determinados, documentados, implementados e revistos de acordo com a política.	· **CIS CSC** 1, 3, 5, 6, 14, 15, 16 · **COBIT 5** APO11.04, BAI03.05, DSS05.04, DSS05.07, MEA02.01 · **ISA 62443-2-1:2009** 4.3.3.3.9, 4.3.3.5.8, 4.3.4.4.7, 4.4.2.1, 4.4.2.2, 4.4.2.4 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.2, A.12.4.3, A.12.4.4, A.12.7.1 · **NIST SP 800-53 Rev. 4** AU Family	ACCESS-3c SITUATION-1a SITUATION-2a	SITUATION-1b SITUATION-1c SITUATION-1d SITUATION-2c SITUATION-2d SITUATION-3b SITUATION-4a	SITUATION-1e SITUATION-3e SITUATION-4c SITUATION-4f	8,2	8,4 8,8 8,11	
		PR.PT-2: Os meios amovíveis são protegidos e a sua utilização restringida de acordo com a política.	· **CIS CSC** 8, 13 · **COBIT 5** APO13.01, DSS05.02, DSS05.06 · **ISA 62443-3-3:2013** SR 2.3 · **ISO/IEC 27001:2013** A.8.2.1, A.8.2.2, A.8.2.3, A.8.3.1, A.8.3.3, A.11.2.9 · **NIST SP 800-53 Rev. 4** MP-2, MP-3, MP-4, MP-5, MP-7, MP-8	ACCESS-2a ACCESS-2b	ACCESS-2c ACCESS-4a ARCHITECTURE-1f ARCHITECTURE-3g	RISK-2l ACCESS-4c ARCHITECTURE-1h	10,3	3,9	
		PR.PT-3: O princípio da menor funcionalidade é incorporado através da configuração de sistemas para fornecer apenas capacidades essenciais.	· **CIS CSC** 3, 11, 14 · **COBIT 5** DSS05.02, DSS05.05, DSS06.06 · **ISA 62443-2-1:2009** 4.3.3.5.1, 4.3.3.5.2, 4.3.3.5.3, 4.3.3.5.4, 4.3.3.5.5, 4.3.3.5.6, 4.3.3.5.7, 4.3.3.5.8, 4.3.3.6.1, 4.3.3.6.2, 4.3.3.6.3, 4.3.3.6.4, 4.3.3.6.5, 4.3.3.6.6, 4.3.3.6.7, 4.3.3.6.8, 4.3.3.6.9, 4.3.3.7.1, 4.3.3.7.2, 4.3.3.7.3, 4.3.3.7.4 · **ISA 62443-3-3:2013** SR 1.1, SR 1.2, SR 1.3, SR 1.4, SR 1.5, SR 1.6, SR 1.7, SR 1.8, SR 1.9, SR 1.10, SR 1.11, SR 1.12, SR 1.13, SR 2.1, SR 2.2, SR 2.3, SR 2.4, SR 2.5, SR 2.6, SR 2.7 · **ISO/IEC 27001:2013** A.9.1.2 · **NIST SP 800-53 Rev. 4** AC-3, CM-7	ACCESS-2a ACCESS-2b ACCESS-3a ACCESS-3b	ACCESS-2c ACCESS-2d ACCESS-2f ACCESS-2g ACCESS-3d ACCESS-3e ARCHITECTURE-1f ARCHITECTURE-2c ARCHITECTURE-3d ARCHITECTURE-3e	RISK-2l ACCESS-2h ACCESS-3h ARCHITECTURE-1h			2,7 13,10
		PR.PT-4: As redes de comunicação e controlo estão protegidas.	· **CIS CSC** 8, 12, 15 · **COBIT 5** DSS05.02, APO13.01 · **ISA 62443-3-3:2013** SR 3.1, SR 3.5, SR 3.8, SR 4.1, SR 4.3, SR 5.1, SR 5.2, SR 5.3, SR 7.1, SR 7.6 · **ISO/IEC 27001:2013** A.13.1.1, A.13.2.1, A.14.1.3 · **NIST SP 800-53 Rev. 4** AC-4, AC-17, AC-18, CP-8, SC-7, SC-19, SC-20, SC-21, SC-22, SC-23, SC-24, SC-25, SC-29, SC-32, SC-36, SC-37, SC-38, SC-39, SC-40, SC-41, SC-43	ARCHITECTURE-2a	ARCHITECTURE-1f ARCHITECTURE-2b ARCHITECTURE-2d	RISK-2l ARCHITECTURE-1h ARCHITECTURE-2g ARCHITECTURE-2h ARCHITECTURE-2i ARCHITECTURE-2j ARCHITECTURE-2k			
		PR.PT-5: Mecanismos (por exemplo, failsafe, balanceamento de carga, hot swap) são implementados para alcançar requisitos de resiliência em situações normais e adversas.	· **COBIT 5** BAI04.01, BAI04.02, BAI04.03, BAI04.04, BAI04.05, DSS01.05 · **ISA 62443-2-1:2009** 4.3.2.5.2 · **ISA 62443-3-3:2013** SR 7.1, SR 7.2 · **ISO/IEC 27001:2013** A.17.1.2, A.17.2.1 · **NIST SP 800-53 Rev. 4** CP-7, CP-8, CP-11, CP-13, PL-8, SA-14, SC-6		RESPONSE-4f RESPONSE-4j ARCHITECTURE-1f	ARCHITECTURE-2l	11,4		

Figura 33: Mapeamento para a categoria "Tecnologia de Proteção" da função "Proteger" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
DETETAR (DE)	**Anomalias e Eventos (DE.AE):** Deteta-se atividade anómala e compreende-se o impacto potencial dos acontecimentos.	**DE.AE-1:** É estabelecida e gerida uma linha de base de operações de rede e fluxos de dados esperados para os utilizadores e sistemas.	· **CIS CSC** 1, 4, 6, 12, 13, 15, 16 · **COBIT 5** DSS03.01 · **ISA 62443-2-1:2009** 4.4.3.3 · **ISO/IEC 27001:2013** A.12.1.1, A.12.1.2, A.13.1.1, A.13.1.2 · **NIST SP 800-53 Rev. 4** AC-4, CA-3, CM-2, SI-4	SITUATION-2a	SITUATION-3a	SITUATION-3d	1,1	3,8	
		DE.AE-2: Os eventos detetados são analisados para compreender os alvos e métodos de ataque.	· **CIS CSC** 3, 6, 13, 15 · **COBIT 5** DSS05.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1, SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.1, A.16.1.4 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, SI-4		RISK-3d ARCHITECTURE-2e	RISK-3g RESPONSE-1d RESPONSE-2i RESPONSE-3h		8,11	
		DE.AE-3: Os dados dos eventos são recolhidos e correlacionados a partir de múltiplas fontes e sensores.	· **CIS CSC** 1, 3, 4, 5, 6, 7, 8, 11, 12, 13, 14, 15, 16 · **COBIT 5** BAI08.02 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, IR-8, SI-4		SITUATION-2c RESPONSE-1c RESPONSE-2f	RESPONSE-1d RESPONSE-2i	8,2	8,5 8,6 8,7 8,8	8,12
		DE.AE-4: O impacto dos eventos é determinado.	· **CIS CSC** 4, 6 · **COBIT 5** APO12.06, DSS03.01 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, RA-3, SI-4	RISK-3a RESPONSE-2b	THREAT-2d RISK-2e RISK-3b RISK-3c RISK-3f RESPONSE-2c RESPONSE-2d RESPONSE-4d	THREAT-2h RESPONSE-2h			
		DE.AE-5: São estabelecidos limiares de alerta de incidentes.	· **CIS CSC** 6, 19 · **COBIT 5** APO12.06, DSS03.01 · **ISA 62443-2-1:2009** 4.2.3.10 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** IR-4, IR-5, IR-8	RISK-3a RESPONSE-2a	THREAT-2d RISK-2e RISK-3b SITUATION-2e RESPONSE-2c RESPONSE-2d RESPONSE-2e	THREAT-2h SITUATION-2j RESPONSE-2h			13,11

Figura 34: Mapeamento para a categoria "Anomalias e Eventos" da função "Detetar" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	Categoria	Subcategoria	Referências Informativas	MIL1	MIL2	MIL3	IG1	IG2	IG3
DETETAR (DE)	**Monitorização Contínua de Segurança (DE.CM):** O sistema de informação e os bens são controlados para identificar eventos de cibersegurança e verificar a eficácia das medidas de proteção.	**DE.CM-1:** A rede é monitorizada para detetar potenciais eventos de cibersegurança.	· **CIS CSC** 1, 7, 8, 12, 13, 15, 16 · **COBIT 5** DSS01.03, DSS03.05, DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, CA-7, CM-3, SC-5, SC-7, SI-4	SITUATION-2a SITUATION-2b	THREAT-2d SITUATION-2d SITUATION-2f ARCHITECTURE-2e ARCHITECTURE-2f	THREAT-2h THREAT-2k ACCESS-2i SITUATION-2g SITUATION-2h RESPONSE-1f		8,5 13,2 13,3 13,6	13,7 13,8 13,10
		DE.CM-2: O ambiente físico é monitorizado para detetar potenciais eventos de cibersegurança.	· **COBIT 5** DSS01.04, DSS01.05 · **ISA 62443-2-1:2009** 4.3.3.3.8 · **ISO/IEC 27001:2013** A.11.1.1, A.11.1.2 · **NIST SP 800-53 Rev. 4** CA-7, PE-3, PE-6, PE-20	SITUATION-2a SITUATION-2b	SITUATION-2d	THREAT-2k ACCESS-3i SITUATION-2h RESPONSE-1f			
		DE.CM-3: A atividade do pessoal é monitorizada para detetar potenciais eventos de cibersegurança.	· **CIS CSC** 5, 7, 14, 16 · **COBIT 5** DSS05.07 · **ISA 62443-3-3:2013** SR 6.2 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3 · **NIST SP 800-53 Rev. 4** AC-2, AU-12, AU-13, CA-7, CM-10, CM-11	SITUATION-2a SITUATION-2b	SITUATION-2d ARCHITECTURE-2e ARCHITECTURE-2f	THREAT-2k ACCESS-2i ACCESS-3i SITUATION-2h RESPONSE-1f			
		DE.CM-4: Código malicioso é detetado.	· **CIS CSC** 4, 7, 8, 12 · **COBIT 5** DSS05.01 · **ISA 62443-2-1:2009** 4.3.4.3.8 · **ISA 62443-3-3:2013** SR 3.2 · **ISO/IEC 27001:2013** A.12.2.1 · **NIST SP 800-53 Rev. 4** SI-3, SI-8	SITUATION-2a SITUATION-2b	SITUATION-2d ARCHITECTURE-2f ARCHITECTURE-3j	SITUATION-2h RESPONSE-1f	10,1 10,2	10,4 10,5 10,6 10,7	9,7
		DE.CM-5: Código móvel não autorizado é detetado.	· **CIS CSC** 7, 8 · **COBIT 5** DSS05.01 · **ISA 62443-3-3:2013** SR 2.4 · **ISO/IEC 27001:2013** A.12.5.1, A.12.6.2 · **NIST SP 800-53 Rev. 4** SC-18, SI-4, SC-44	SITUATION-2a SITUATION-2b	SITUATION-2d ARCHITECTURE-3j	SITUATION-2h RESPONSE-1f			
		DE.CM-6: A atividade dos prestadores de serviços externos é monitorizada para detetar potenciais eventos de cibersegurança.	· **COBIT 5** APO07.06, APO10.05 · **ISO/IEC 27001:2013** A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** CA-7, PS-7, SA-4, SA-9, SI-4	SITUATION-2a SITUATION-2b	SITUATION-2d THIRD-PARTIES-2d THIRD-PARTIES-3b	THREAT-2k RISK-2k RESPONSE-1f THIRD-PARTIES-2j THIRD-PARTIES-2k			15,6
		DE.CM-7: Monitorização para pessoal não autorizado, conexões, dispositivos e software é realizada.	· **CIS CSC** 1, 2, 3, 5, 9, 12, 13, 15, 16 · **COBIT 5** DSS05.02, DSS05.05 · **ISO/IEC 27001:2013** A.12.4.1, A.14.2.7, A.15.2.1 · **NIST SP 800-53 Rev. 4** AU-12, CA-7, CM-3, CM-8, PE-3, PE-6, PE-20, SI-4	SITUATION-2a SITUATION-2b	THREAT-2d SITUATION-2d SITUATION-2f	THREAT-2h THREAT-2k RISK-2j SITUATION-2g SITUATION-2h RESPONSE-1f ARCHITECTURE-2k ARCHITECTURE-4h	2,3	1,3 1,4 2,4 2,5 2,6 9,6 13,5	1,5 2,7 13,10
		DE.CM-8: São efetuados scans de vulnerabilidades.	· **CIS CSC** 4, 20 · **COBIT 5** BAI03.10, DSS05.01 · **ISA 62443-2-1:2009** 4.2.3.1, 4.2.3.7 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** RA-5	THREAT-1c	THREAT-1f RISK-2c	THREAT-1j THREAT-1k RISK-2i	4,2	7,5	

Figura 35: Mapeamento para a categoria "Monitorização Contínua de Segurança" da função "Detetar" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
DETETAR (DE)	**Processos de Deteção (DE.DP):** Os processos e procedimentos de deteção são mantidos e testados para assegurar o conhecimento de eventos anómalos.	**DE.DP-1:** Os papéis e responsabilidades de deteção estão bem definidos para assegurar a responsabilização.	· **CIS CSC** 19 · **COBIT 5** APO01.02, DSS05.01, DSS06.03 · **ISA 62443-2-1:2009** 4.4.3.1 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PM-14	WORKFORCE-1a	WORKFORCE-1d	SITUATION-4e WORKFORCE-1e	17,1	17,4	
		DE.DP-2: As atividades de deteção cumprem todos os requisitos aplicáveis.	· **COBIT 5** DSS06.01, MEA03.03, MEA03.04 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISO/IEC 27001:2013** A.18.1.4, A.18.2.2, A.18.2.3 · **NIST SP 800-53 Rev. 4** AC-25, CA-2, CA-7, SA-18, SI-4, PM-14	RISK-3a	THREAT-2d RISK-2e RISK-3b SITUATION-2c RESPONSE-1b RESPONSE-5a	THREAT-2h RESPONSE-1e RESPONSE-5c			
		DE.DP-3: Os processos de deteção são testados.	· **COBIT 5** APO13.02, DSS05.02 · **ISA 62443-2-1:2009** 4.4.3.2 · **ISA 62443-3-3:2013** SR 3.3 · **ISO/IEC 27001:2013** A.14.2.8 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, PE-3, SI-3, SI-4, PM-14		RESPONSE-3f RESPONSE-3g	SITUATION-2j RESPONSE-3j			
		DE.DP-4: São comunicadas informações de deteção de eventos às partes apropriadas.	· **CIS CSC** 19 · **COBIT 5** APO08.04, APO12.06, DSS02.05 · **ISA 62443-2-1:2009** 4.3.4.5.9 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.16.1.2, A.16.1.3 · **NIST SP 800-53 Rev. 4** AU-6, CA-2, CA-7, RA-5, SI-4	RESPONSE-1a RESPONSE-3c	THREAT-1i THREAT-2g RISK-3e SITUATION-3a SITUATION-3c RESPONSE-2g RESPONSE-4d	THREAT-2k SITUATION-3d RESPONSE-3i		17,5	
		DE.DP-5: Os processos de deteção são continuamente melhorados.	· **COBIT 5** APO11.06, APO12.06, DSS04.05 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6 · **NIST SP 800-53 Rev. 4**, CA-2, CA-7, PL-2, RA-5, SI-4, PM-14		RESPONSE-2e RESPONSE-3g RESPONSE-5b ARCHITECTURE-2e ARCHITECTURE-2f	SITUATION-2i SITUATION-3f SITUATION-3g RESPONSE-1f RESPONSE-3h			

Figura 36: Mapeamento para a categoria "Processos de Deteção" da função "Detetar" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
RESPONDER (RS)	**Planeamento da Resposta (RS.RP):** Os processos e procedimentos de resposta são executados e mantidos, para assegurar a resposta a incidentes de cibersegurança detetados.	**RS.RP-1:** O plano de resposta é executado durante ou após um incidente.	· **CIS CSC** 19 · **COBIT 5** APO12.06, BAI01.10 · **ISA 62443-2-1:2009** 4.3.4.5.1 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-2, CP-10, IR-4, IR-8		RESPONSE-3d RESPONSE-3e RESPONSE-5a				

Figura 37: Mapeamento para a categoria "Planeamento da Resposta" da função "Responder" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
RESPONDER (RS)	**Comunicações (RS.CO):** As atividades de resposta são coordenadas com os intervenientes internos e externos (por exemplo, apoio externo das agências de aplicação da lei).	**RS.CO-1:** O pessoal conhece as suas funções e a ordem das operações quando é necessária uma resposta.	· **CIS CSC** 19 · **COBIT 5** EDM03.02, APO01.02, APO12.03 · **ISA 62443-2-1:2009** 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 · **ISO/IEC 27001:2013** A.6.1.1, A.7.2.2, A.16.1.1 · **NIST SP 800-53 Rev. 4** CP-2, CP-3, IR-3, IR-8	RESPONSE-3a	RESPONSE-5b		17,2	17,4	
		RS.CO-2: Os incidentes são comunicados de acordo com os critérios estabelecidos.	· **CIS CSC** 19 · **COBIT 5** DSS01.03 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** A.6.1.3, A.16.1.2 · **NIST SP 800-53 Rev. 4** AU-6, IR-6, IR-8	RESPONSE-2a RESPONSE-3c	RESPONSE-2g			17,5	
		RS.CO-3: A informação é partilhada de forma consistente com os planos de resposta.	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.2 · **ISO/IEC 27001:2013** A.16.1.2, Clause 7.4, Clause 16.1.2 · **NIST SP 800-53 Rev. 4** CA-2, CA-7, CP-2, IR-4, IR-8, PE-6, RA-5, SI-4	RESPONSE-3c	SITUATION-3a SITUATION-3c SITUATION-4a RESPONSE-2g RESPONSE-3d RESPONSE-3e	SITUATION-3d RESPONSE-3i		17,5	
		RS.CO-4: A coordenação com as partes interessadas ocorre de forma consistente com os planos de resposta.	· **CIS CSC** 19 · **COBIT 5** DSS03.04 · **ISA 62443-2-1:2009** 4.3.4.5.5 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8		RESPONSE-3d RESPONSE-3e	RESPONSE-3i		17,5	
		RS.CO-5: A partilha voluntária de informação ocorre com intervenientes externos para alcançar uma maior consciência da situação de cibersegurança.	· **CIS CSC** 19 · **COBIT 5** BAI08.04 · **ISO/IEC 27001:2013** A.6.1.4 · **NIST SP 800-53 Rev. 4** SI-5, PM-15		THREAT-1i THREAT-2g RESPONSE-2g	THREAT-2k SITUATION-3d SITUATION-3f SITUATION-3g			

Figura 38: Mapeamento para a categoria "Comunicações" da função "Responder" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
RESPONDER (RS)	**Análise (RS.AN):** A análise é conduzida para assegurar uma resposta eficaz e apoiar as atividades de recuperação.	**RS.AN-1:** Notificações de sistemas de deteção são investigadas.	· **CIS CSC** 4, 6, 8, 19 · **COBIT 5** DSS02.04, DSS02.07 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISA 62443-3-3:2013** SR 6.1 · **ISO/IEC 27001:2013** A.12.4.1, A.12.4.3, A.16.1.5 · **NIST SP 800-53 Rev. 4** AU-6, CA-7, IR-4, IR-5, PE-6, SI-4		RESPONSE-1c RESPONSE-2f	RESPONSE-1d		8,11 16,3 16,6	
		RS.AN-2: O impacto do incidente é compreendido.	· **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 · **ISO/IEC 27001:2013** A.16.1.4, A.16.1.6 · **NIST SP 800-53 Rev. 4** CP-2, IR-4	RISK-3a	THREAT-2d RISK-2e RISK-3b RISK-3c RISK-3f RESPONSE-2c	RESPONSE-2h			
		RS.AN-3: As análises forenses são realizadas.	· **COBIT 5** APO12.06, DSS03.02, DSS05.07 · **ISA 62443-3-3:2013** SR 2.8, SR 2.9, SR 2.10, SR 2.11, SR 2.12, SR 3.9, SR 6.1 · **ISO/IEC 27001:2013** A.16.1.7 · **NIST SP 800-53 Rev. 4** AU-7, IR-4		RESPONSE-3d RESPONSE-3e	RESPONSE-3h RESPONSE-3i			
		RS.AN-4: Os incidentes são categorizados de acordo com os planos de resposta.	· **CIS CSC** 19 · **COBIT 5** DSS02.02 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISO/IEC 27001:2013** A.16.1.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-5, IR-8	RESPONSE-2a	RESPONSE-1b RESPONSE-1c				17,9
		RS.AN-5: São estabelecidos processos para receber, analisar e responder a vulnerabilidades reveladas à organização a partir de fontes internas e externas (por exemplo, testes internos, boletins de segurança, ou investigadores de segurança).	· **CIS CSC** 4, 19 · **COBIT 5** EDM03.02, DSS05.07 · **NIST SP 800-53 Rev. 4** SI-5, PM-15	THREAT-1a THREAT-1b THREAT-1c THREAT-1d RISK-3a RISK-4a	THREAT-1e THREAT-1f THREAT-1g THREAT-1i RISK-2e RISK-3b RISK-3d RISK-4b	THREAT-1j THREAT-1k THREAT-1l RISK-2i RISK-3g RISK-4c RISK-4e SITUATION-3f SITUATION-3g		16,2 16,3	

Figura 39: Mapeamento para a categoria "Análise" da função "Responder" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
RESPONDER (RS)	**Mitigação (RS.MI):** São realizadas atividades para prevenir a expansão de um evento, mitigar os seus efeitos, e resolver o incidente.	**RS.MI-1:** Os incidentes são contidos.	· **CIS CSC** 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6 · **ISA 62443-3-3:2013** SR 5.1, SR 5.2, SR 5.4 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4	RESPONSE-3b		ARCHITECTURE-2l			
		RS.MI-2: Os incidentes são mitigados.	· **CIS CSC** 4, 19 · **COBIT 5** APO12.06 · **ISA 62443-2-1:2009** 4.3.4.5.6, 4.3.4.5.10 · **ISO/IEC 27001:2013** A.12.2.1, A.16.1.5 · **NIST SP 800-53 Rev. 4** IR-4	RESPONSE-3b	RESPONSE-4e RESPONSE-4f	ARCHITECTURE-2l			
		RS.MI-3: Vulnerabilidades recentemente identificadas são mitigadas ou documentadas como riscos aceites.	· **CIS CSC** 4 · **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** A.12.6.1 · **NIST SP 800-53 Rev. 4** CA-7, RA-3, RA-5	THREAT-1d RISK-3a	THREAT-1g RISK-2e RISK-3b RISK-3d	THREAT-1k THREAT-1l RISK-2i RISK-3g		7,6	

Figura 40: Mapeamento para a categoria "Mitigação" da função "Responder" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
RESPONDER (RS)	**Melhorias (RS.IM):** As atividades de resposta organizacional são melhoradas através da incorporação de lições aprendidas de atividades de deteção/resposta atuais e anteriores.	**RS.IM-1:** Planos de resposta incorporam lições aprendidas.	· **COBIT 5** BAI01.13 · **ISA 62443-2-1:2009** 4.3.4.5.10, 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8		RESPONSE-3g	RESPONSE-2i RESPONSE-3h		17,8	
		RS.IM-2: As estratégias de resposta estão atualizadas.	· **COBIT 5** BAI01.13, DSS04.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8		RESPONSE-3f RESPONSE-3g	RESPONSE-3h		17,8	

Figura 41: Mapeamento para a categoria "Melhorias" da função "Responder" da NIST *Framework Core*

NIST Framework Core				Práticas do C2M2			Controlos da CIS versão 8		
Função	**Categoria**	**Subcategoria**	**Referências Informativas**	**MIL1**	**MIL2**	**MIL3**	**IG1**	**IG2**	**IG3**
RECUPERAR (RC)	**Plano de Recuperação (RC.RP):** Os processos e procedimentos de recuperação são executados e mantidos para assegurar a restauração dos sistemas ou bens afetados por incidentes de cibersegurança.	**RC.RP-1:** O plano de recuperação é executado durante ou após um incidente de cibersegurança.	· **CIS CSC** 10 · **COBIT 5** APO12.06, DSS02.05, DSS03.04 · **ISO/IEC 27001:2013** A.16.1.5 · **NIST SP 800-53 Rev. 4** CP-10, IR-4, IR-8	RESPONSE-3b RESPONSE-4a	RESPONSE-3d RESPONSE-3e RESPONSE-4l	RESPONSE-3k			
	Melhorias (RC.IM): O planeamento e os processos de recuperação são melhorados através da incorporação das lições aprendidas em atividades futuras.	**RC.IM-1:** Planos de recuperação incorporam lições aprendidas.	· **COBIT 5** APO12.06, BAI05.07, DSS04.08 · **ISA 62443-2-1:2009** 4.4.3.4 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8		RESPONSE-3g	RESPONSE-3h RESPONSE-4o			
		RC.IM-2: As estratégias de recuperação estão atualizadas.	· **COBIT 5** APO12.06, BAI07.08 · **ISO/IEC 27001:2013** A.16.1.6, Clause 10 · **NIST SP 800-53 Rev. 4** CP-2, IR-4, IR-8		RESPONSE-3g	RESPONSE-3h RESPONSE-4p RESPONSE-4q			
	Comunicações (RC.CO): As atividades de restauração são coordenadas com partes internas e externas (por exemplo, centros de coordenação, fornecedores de serviços de Internet, proprietários de sistemas de ataque, vítimas, outros CSIRT, e vendedores).	**RC.CO-1:** As relações públicas estão geridas.	· **COBIT 5** EDM03.02 · **ISO/IEC 27001:2013** A.6.1.4, Clause 7.4		RISK-1c	RESPONSE-3i			
		RC.CO-2: A reputação é reparada após um incidente.	· **COBIT 5** MEA03.02 · **ISO/IEC 27001:2013** Clause 7.4		RESPONSE-3d RESPONSE-3e				
		RC.CO-3: As atividades de recuperação são comunicadas às partes interessadas internas e externas, bem como às equipas executivas e de gestão.	· **COBIT 5** APO12.06 · **ISO/IEC 27001:2013** Clause 7.4 · **NIST SP 800-53 Rev. 4** CP-2, IR-4		SITUATION-3a SITUATION-3c RESPONSE-3d RESPONSE-3e RESPONSE-4l RESPONSE-4m	SITUATION-3d			

Figura 42: Mapeamento para a função "Recuperar" da NIST *Framework Core*

A presente dissertação foi proposta pela empresa *Devise Futures, Lda.* e realizada na Imprensa Nacional — Casa da Moeda, S.A. (INCM)