
Instituto Politécnico de Leiria

Escola Superior de Tecnologia e Gestão

Departamento de Engenharia Informática

Mestrado em Cibersegurança e Informática Forense

# Proteção de PMEs no Ciberespaço

Aplicação de *CIS Controls* para resposta ao Selo de Maturidade Digital em Cibersegurança

LÚCIO MIGUEL BRITES DOS SANTOS CRESPO

Leiria, julho de 2024


Instituto Politécnico de Leiria

Escola Superior de Tecnologia e Gestão

Departamento de Engenharia Informática

Mestrado em Cibersegurança e Informática Forense

# Proteção de PMEs no Ciberespaço

Aplicação de *CIS Controls* para resposta ao Selo de Maturidade Digital em Cibersegurança

LÚCIO MIGUEL BRITES DOS SANTOS CRESPO

NÚMERO: 2220279

Trabalho de Projeto realizado sob a orientação do Professor Ricardo Gomes (ricardo.p.gomes@ipleiria.pt) e da Professora Doutora Marisa Maximiano (marisa.maximiano@ipleiria.pt)

Leiria, julho de 2024

# Originalidade e Direitos de Autor

O presente relatório de projeto é original, elaborado unicamente para este fim, tendo sido devidamente citados todos os autores cujos estudos e publicações contribuíram para o elaborar.

# Agradecimentos

Este trabalho não representa apenas uma etapa académica, mas uma caminhada pessoal de crescimento e descoberta, que não teria sido possível de concluir, com sucesso sem o apoio de diversas pessoas.

À minha família Luísa, Mafalda e Lucas, por todo o apoio e paciência ao longo dos dois anos do Mestrado, pois sem o apoio e compreensão, a realização do mesmo não seria possível.

Ao professor Ricardo Gomes e à professora Doutora Marisa Maximiano, pela orientação e ensinamentos ao longo deste processo.

Agradeço aos participantes da pesquisa, cuja contribuição foi essencial para a obtenção dos dados necessários.

Ao Miguel que foi o catalisador para decidir embarcar nesta experiência.

Aos colegas de Mestrado, pelo companheirismo e disponibilidade demonstrada ao longo dos dois anos.

A todos aqueles, que de alguma forma, contribuíram para a elaboração deste trabalho, os meus sinceros agradecimentos.

# Resumo

Os ciberataques direcionados a organizações de todos os tamanhos e geografias, aumentam todos os anos. A cibersegurança envolve a utilização de métodos defensivos para detetar e impedir os atacantes de serem bem-sucedidos, centrando-se na tríade CIA. Assim a importância da cibersegurança cresce exponencialmente à medida que a sociedade se digitaliza. As empresas estão cada vez mais interligadas e dependentes umas das outras, aumentando a exposição a riscos e ameaças.

Este trabalho explora diversas *frameworks* e modelos de avaliação de cibersegurança, com o objetivo de compreender e implementar boas práticas adequadas às PMEs portuguesas. O foco está em aumentar a resiliência dessas empresas, protegendo os seus ativos e cadeias de abastecimento, essenciais para a economia. As PMEs muitas vezes possuem recursos limitados, tornando difícil a implementação de práticas robustas de cibersegurança. Muitas destas, também operam em setores regulamentados onde a conformidade com normas de segurança é essencial, mas dispendiosa e complexa.

A falta de acesso à consultoria especializada e a diversidade de normas existentes podem ser desafiantes para as PMEs. Com este trabalho pretende-se disponibilizar um guia prático com instruções claras e executáveis para ajudar as empresas. Este deve ser acompanhado da sensibilização da gestão de topo, pois líderes e executivos desempenham um papel fulcral na definição de prioridades e alocação de recursos.

Através deste trabalho, foi possível mapear os requisitos dos Selo de Maturidade Digital em Cibersegurança (Bronze e Prata), com *safeguards* do *CIS Controls*. Pretende-se que ao serem implementadas as recomendações apresentadas no guia, as empresas se encontrem aptas a se submeterem à certificação de Maturidade Digital em Cibersegurança para a obtenção do nível Prata.

Para uma melhor perceção do panorama real das PMEs, foi realizado um estudo junto de 21 PMEs da Região de Leiria, onde foram avaliadas as suas práticas atuais, perceção de vulnerabilidades e capacidades de resposta a incidentes de cibersegurança. Com a análise dos resultados, destaca-se a necessidade de maior foco na formação e conscientização dos colaboradores, exposto a componente humana como uma das maiores vulnerabilidades identificadas, assim como a necessidade de um maior investimento nas áreas de deteção e resposta a incidentes.

**Palavras-chave:** Cibersegurança, Pequenas e Médias Empresas, Safeguards CIS Controls, Selo de Maturidade Digital em Cibersegurança

# Abstract

Cyberattacks targeting organizations of all sizes and geographies are increasing every year. Cybersecurity involves using defensive methods to detect and prevent attackers from succeeding, focusing on the CIA triad. Thus, the importance of cybersecurity grows exponentially as society digitizes. Companies are increasingly interconnected and dependent on each other, increasing exposure to risks and threats.

This work explores several cybersecurity assessment frameworks and models, with the aim of understanding and implementing good practices suitable for Portuguese SMEs. The focus is on increasing the resilience of these companies, protecting their assets and supply chains, which are essential to the economy. SMBs often have limited resources, making it difficult to implement robust cybersecurity practices. Many of these also operate in regulated sectors where compliance with safety standards is essential, but expensive and complex.

The lack of access to expert advice and the diversity of existing standards can be challenging for SMEs. This work aims to provide a practical guide with clear and executable instructions to help companies. This must be accompanied by awareness among senior management, as leaders and executives play a key role in setting priorities and allocating resources.

Through this work, it was possible to map the requirements of the Digital Maturity Seal in Cybersecurity (Bronze and Silver), with security guards from CIS Controls. It is intended that when the recommendations presented in the guide are implemented, companies will be able to undergo Digital Maturity in Cybersecurity certification to obtain the Silver level.

To better understand the real panorama of SMEs, a study was carried out with 21 SMEs in the Leiria Region, where their current practices, perception of vulnerabilities and response capabilities to cybersecurity incidents were evaluated. With the analysis of the results, the need for greater focus on training and awareness of employees, exposed to the human component as one of the greatest vulnerabilities identified, stands out, as well as the need for greater investment in the areas of detection and response to incidents.

**Keywords:** Cybersecurity, Small and Medium Businesses, Safeguards CIS Controls, Seal of Digital Maturity in Cybersecurity

# Índice

# Lista de Figuras

# Lista de Tabelas

# Lista de Siglas e Acrónimos

| | |
|---|---|
| APCER | Associação Portuguesa de Certificação |
| BSI | *British Standards Institution* |
| C2M2 | *Cybersecurity Capability Maturity Model* |
| CEO | *Chief Executive Officer* |
| CIA | *Confidentiality Integrity Availability* |
| CIS | *Center for Internet Security* |
| CMMC | *Cybersecurity Maturity Model Certification* |
| CMMI | *Capability Maturity Model Integration* |
| CNCS | Centro Nacional de Cibersegurança |
| COBIT | Control Objectives for Information and related Technology |
| CSF | *CyberSecurity Framework* |
| DKIM | *DomainKeys Identified Mail* |
| DMARC | *Domain-based Message Authentication Reporting and Conformance* |
| DNP TS | Documento Normativo Português – Especificação Técnica |
| DNSSEC | *Domain Name System Security Extensions* |
| ENISA | *European Union Agency for Network and Information Security* |
| ESTG | Escola Superior de Tecnologia e Gestão |
| EUA | Estados Unidos da América |
| FFIEC | *Federal Financial Institutions Examination Council* |
| HSTS | *HTTP Strict Transport Security* |
| HTML | *HyperText Markup Language* |
| HTTPS | *Hypertext Transfer Protocol Secure* |
| IGs | *Implementation Groups* |
| INE | Instituto Nacional de Estatística |
| IoT | *Internet of Things* |
| IPAC | Instituto Português de Acreditação |
| IPQ | Instituto Português da Qualidade |
| ISACA | *Information Systems Audit and Control Association* |
| ISMS | *Information Security Management Systems* |
| ISO/IEC | *International Organization for Standardization/International Electrotechnical Commission* |
| MAC | *Media Access Control* |
| MDM | *Mobile Device Management* |
| MIL | *Maturity Indicator Level* |
| NIST | *National Institute of Standards and Technology* |
| NUTS | Nomenclatura das Unidades Territoriais para Fins Estatísticos |
| PDCA | *Plan-Do-Check-Act* |
| PDF | *Portable Document Format* |
| PII | *Personal Identifiable Information* |
| PME | Pequenas e Médias Empresas |
| QNRSC | Quadro Nacional de Referência para a Cibersegurança |
| SGSI | Sistema de Gestão da Segurança da Informação |
| SMD | Selo de Maturidade Digital |
| SPF | *Sender Policy Framework* |

| | |
|---|---|
| SSL | *Secure Sockets Layer* |
| TI | Tecnologia de Informação |
| TIC | Tecnologias de Informação e Comunicação |
| TLS | *Transport Layer Security* |
| TPM | *Trusted Platform Module* |
| UE | União Europeia |
| URL | *Uniform Resource Locator* |

# 1. Introdução

Nos últimos anos, tem-se observado um aumento significativo dos riscos e ataques direcionados a empresas de todos os tamanhos. O último relatório da *ENISA Threat Landscape* 2023 [1], indica que entre o segundo semestre de 2022 e no primeiro semestre de 2023, o cenário de cibersegurança observou um aumento significativo tanto na variedade como na quantidade de ciberataques. O relatório refere a expansão do *hacktivism*, associado ao contexto geopolítico atual, assim como, o surgimento de novas técnicas desenvolvidas com o recurso à Inteligência Artificial, utilizadas em ataques de engenharia social. O *ransomware* continua a ser uma das ameaças mais prevalentes e impactantes no cenário atual, sendo estes ataques cada vez mais direcionados e complexos. Não esquecendo a crescente prevalência de ataques de cadeia de abastecimento, nos quais os atacantes comprometem fornecedores de serviços ou *software* para atingir suas vítimas finais.

A cibersegurança consiste em grande parte em métodos defensivos usados para detetar e impedir possíveis intrusos [2]. No centro desta disciplina está a tríade CIA, que representa os três pilares fundamentais da segurança da informação: Confidencialidade, Integridade e Disponibilidade. A Confidencialidade, garante que a informação está apenas acessível para pessoas autorizadas, protegendo-a contra acessos não autorizados e divulgando apenas o necessário. A Integridade, assegura que a informação não é alterada ou destruída de maneira não autorizada, garantindo a exatidão e a consistência dos dados ao longo do seu ciclo de vida. A Disponibilidade, garante que a informação e os recursos estão acessíveis e utilizáveis quando necessários por quem precisa deles.

A relevância da cibersegurança tem crescido exponencialmente à medida que a sociedade se torna cada vez mais digital. Empresas de todos as dimensões estão mais interligadas, o que aumenta a sua exposição às ameaças. Numa entrevista à CBS [3] em 11 de abril de 2021, Jerome Powell, Presidente da Reserva Federal dos Estados Unido, refere que a cibersegurança não é apenas uma preocupação técnica, é uma questão estratégica que afeta a estabilidade económica, destacando ainda a importância da cibersegurança na manutenção da estabilidade financeira global. Powell afirmou que a cibersegurança é uma das principais ameaças à economia global, onde os ciberataques podem desestabilizar mercados financeiros e infraestruturas críticas.

Neste trabalho pretende-se explorar as diversas *frameworks* e modelos de avaliação de cibersegurança disponíveis, para compreender e implementar boas práticas adequadas às necessidades e dimensão das PMEs. De forma a aumentar a sua resiliência, protegendo não apenas os seus ativos, mas também as cadeias de abastecimento das quais muitas

PMEs fazem parte, dada a importância que estas empresas representam para a economia portuguesa.

## 1.1. Motivação e Objetivos

Cada vez mais a cibersegurança está a tornar-se uma preocupação central para as PMEs, que muitas vezes enfrentam desafios importantes devido a recursos limitados, tanto financeiros quanto humanos. Estas limitações tornam difícil a implementação e manutenção de práticas robustas de cibersegurança, deixando-as mais vulneráveis a ataques. Além disso, muitas vezes operam em setores regulamentados onde a conformidade com normas de segurança é indispensável, mas o custo e a complexidade de implementar tais medidas podem ser proibitivos. Este trabalho surge então da importância de fornecer às PMEs ferramentas e estratégias eficazes para melhorar a sua postura de cibersegurança.

As PMEs desempenham papéis essenciais em diversas cadeias de valor e, portanto, uma falha de segurança numa PME pode ter um efeito cascata, afetando outras empresas na cadeia, sendo que uma falha de segurança pode causar disrupções em empresas de maior dimensão. Além disso, investir em cibersegurança pode ser um fator diferenciador competitivo para PMEs que procuram expandir a suas operações globalmente ou estabelecer parcerias estratégicas com outras empresas. A capacidade de demonstrar um compromisso com a proteção de dados e a privacidade dos clientes pode aumentar a confiança do consumidor e abrir novas oportunidades de mercado.

A combinação de sistemas inadequadamente protegidos, falta de conhecimento especializado e orçamentos restritos resulta em vulnerabilidades que podem ter consequências devastadoras para estas empresa. Além disso, a falta de consciencialização sobre cibersegurança entre os utilizadores e a dependência de sistemas *legacy* também são desafios significativos. Estes problemas são agravados por um panorama em rápida evolução, tanto em relação ao tipo quanto à complexidade das ameaças, que exigem uma resposta ágil e adaptável.

A falta de capacidade de acesso a consultoria especializada que possa orientar as PMEs na implementação de práticas de segurança adequadas, assim como, a existência de várias normas e *frameworks*, produzidas por várias entidades nacionais e internacionais, pode ser desafiante. O autor acredita que a ausência de um guia claro e simplificado dificulta a adoção dessas práticas. Portanto, com este trabalho pretende-se também disponibilizar um guia prático que possa orientar as PMEs com instruções práticas e executáveis.

Para aferir a maturidade de um grupo de empresas (PMEs) da Região de Leiria e identificar as áreas com maiores necessidades, foi realizado um estudo, avaliando as suas práticas atuais, a perceção sobre as suas vulnerabilidades e as capacidades de deteção e resposta a incidentes de cibersegurança. Com a análise dos resultados obtidos, podem ser tiradas

conclusões sobre as áreas que necessitam de mais atenção e para as quais as empresas devem orientar mais os seus esforços.

## 1.2. Plano de Trabalho

Para alcançar objetivo deste projeto, foi definida uma sequência de etapas exemplificadas na Figura 1. Estas etapas tiveram o espaço temporal associado ao ano letivo, que teve o seu início em outubro de 2023 e o seu término em julho de 2024.

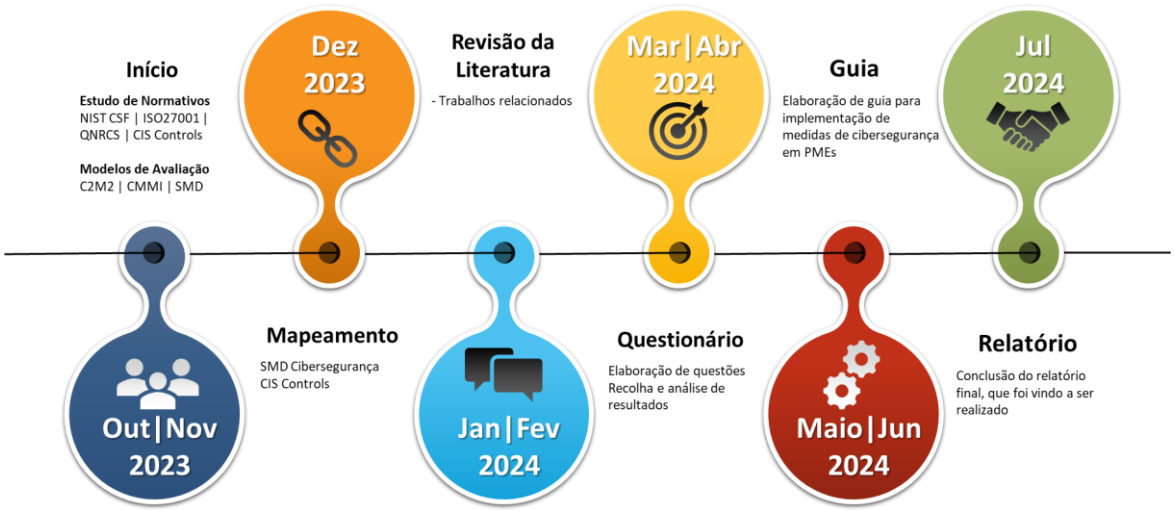



**Figura 1 – Diagrama temporal da realização do projeto**

Estando o objetivo final, definido logo desde o início do projeto, este foi iniciado com a obtenção de uma base sólida para o poder desenvolver e sustentar. Para tal, foram analisados normativos e modelos de avaliação de cibersegurança, que se poderiam adequar ao fim. Destacam-se então o: *NIST Cybersecurity Framework* [4], ISO/IEC 27001 [5], QNRCS [6] e o *CIS Controls* [7], por seu lado para a avaliação de maturidade foram analisados modelos como o: C2M2 [8], CMMI [9] e o Selo de Maturidade Digital (SMD) em Cibersegurança [10]. Com esta etapa foi possível criar uma base de conhecimento e compreensão de boas práticas e escolha da que mais se adequava ao objetivo pretendido.

Na etapa seguinte foi realizada uma revisão da literatura académica e trabalhos relacionados para perceber o que já foi efetuado na área, de forma a identificar oportunidades para diferenciação. Nos trabalhos avaliados, existem vários que analisam a relação entre a cibersegurança e as PMEs, mas não no mesmo contexto deste projeto. Neste trabalho pretende-se a integração de controlos técnicos disponibilizados pelo *CIS Controls* com um modelo de avaliação que permitisse aferia a vantagem da implementação desses mesmos controlos.

Seguidamente o esforço foi centrado no mapeamento entre os requisitos do Selo de Maturidade Digital em Cibersegurança e as *safeguards* do *CIS Controls* com vista à identificação das práticas adaptadas às necessidades de uma PME, mas que no caso

específico de Portugal, se possam submeter-se a uma avaliação que lhe confere uma distinção reconhecida, com 3 níveis. Além disso, foi definido um perfil de PME ao qual o trabalho se adequa.

Com base no trabalho de preparação efetuado foi elaborado um questionário estruturado para investigar as práticas atuais de cibersegurança num conjunto de 21 PMEs. Os dados recolhidos foram analisados de forma a perceber quais as maiores necessidades por parte das empresas.

Através da investigação efetuada e os resultados do questionário, foi elaborado um guia de implementação, que se pretende que ofereça orientações e soluções práticas para ajudar as PMEs a implementar medidas de cibersegurança.

## 1.3. Estrutura do Documento

No Capítulo 2 são abordados diversos tópicos fundamentais para a compreensão do contexto e da relevância da cibersegurança para as empresas. Neste, são abordados os conceitos e limites para uma empresa ser considerada como PME. Fazendo as PMEs, muitas vezes fazem parte de cadeias de abastecimento, fala-se da importância destas, e abordam-se os riscos de cibersegurança nestas cadeias. A transformação digital, é aborda pelo seu impacto paras as empresas continuarem competitivas no meio em que se inserem. Tendo em conta a integração de Portugal na União Europeia (EU) são analisadas as diretrizes e políticas da UE, que são de transposição obrigatória e tratam da cibersegurança num espectro mais alargado, com impacto na cibersegurança das empresas em toda a União. É abordada a análise efetuada de algumas *frameworks* de cibersegurança. Por fim fala-se da avaliação de maturidade, onde se analisa alguns os modelos de avaliação de maturidade em cibersegurança que servem para aferir o estado com critérios reconhecidos ou normalizados.

No Capítulo 3, é apresentada uma revisão da literatura existente sobre cibersegurança em PMEs. São exploradas pesquisas onde são abordados os desafios de Cibersegurança das PMEs, Gestão de Riscos, Estratégias e Mitigação de Riscos, Desenvolvimento de Competências, Formação e Implementação de medidas práticas de Segurança.

No Capítulo 4, é detalhada a abordagem da metodologia adotada, tendo sido divida em 4 fases, correspondendo às etapas da preparação do trabalho e objetivos a atingir.

O Capítulo 5, apresenta o principal trabalho desenvolvido, como o processo de mapeamento dos SMD em Cibersegurança e *CIS Controls.* Neste é detalhamento a correlação entre os requisitos do SMD em Cibersegurança, dos níveis Bronze e Prata e as *safeguards* dos *CIS Controls*. Com base nesta correlação é aborda a estratégia seguida para a elaboração e aplicação de um questionário para avaliar a implementação de cibersegurança nas PMEs. É ainda feita uma análise comparativa da divisão da estrutura do

questionário por funções de segurança do *CIS Controls* e Áreas dos SMD em Cibersegurança.

No Capítulo 6, são tratados e analisados os resultados obtidos com o questionário realizado a 21 PMEs, onde são apuradas as principais tendências observadas e implicações dos resultados para as PMEs.

Por fim, no Capítulo 7, são apresentadas as conclusões do trabalho, com o *input* obtido pelo estudo realizado junto das PMEs, assim como as sugestões de trabalho futuro a ser realizado.

# 2. Contextualização

Este capítulo apresenta os conceitos fundamentais que constituem o contexto do presente trabalho. Inicialmente, aborda-se o foco do projeto: as Pequenas e Médias Empresas (PME). Em seguida, são discutidos os conceitos essenciais de cibersegurança, delineando a importância e os desafios enfrentados nesse campo. Além disso, examina-se a estratégia da União Europeia (UE) para promover a cibersegurança, destacando iniciativas e políticas relevantes. Por último, são analisados os componentes críticos das normas de cibersegurança e dos métodos de avaliação do nível de maturidade das organizações neste contexto, visando compreender as melhores práticas e diretrizes para garantir a segurança digital das PMEs.

## 2.1. PMEs

A categoria das Micro, Pequenas e Médias Empresas é constituída por empresas que empregam menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de euros, ou cujo balanço total anual não excede 43 milhões de euros [11].

De acordo com dados do Instituto Nacional de Estatística (INE)[1], referentes ao ano de 2022 (atualizados a 15 de dezembro de 2023), em Portugal existiam 1.437.254 empresas. Das quais 1.345.818 eram consideradas PMEs, existindo um total de 1.436 Grandes empresas, como é possível verificar na Figura 2.

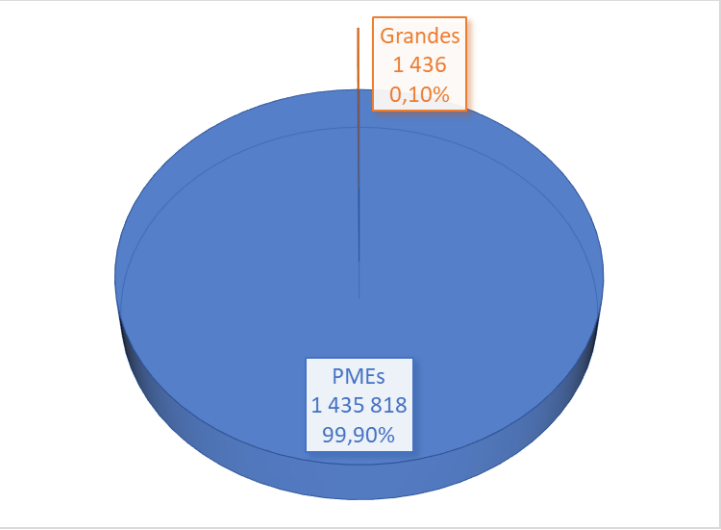



**Figura 2 – Distribuição de Grandes Empresas e PMEs em Portugal**

[1]https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_indicadores&indOcorrCod=0009800&contexto=bd&selTab=tab2&xlang=pt

Do total de PMEs, 1.380.398 (96,14%) são consideradas Micro, 47.406 (3,3%) consideradas Pequenas e 8.014 (0,56%) consideradas Médias, de acordo com a Figura 3.

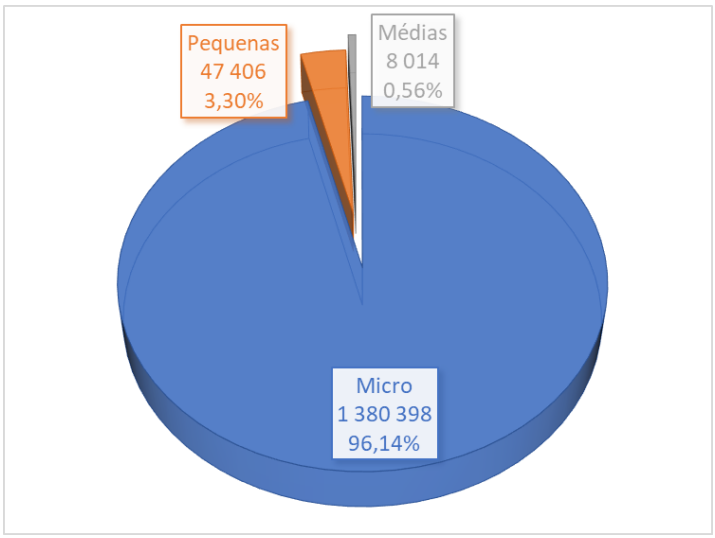



**Figura 3 – Distribuição por tipo de PME em Portugal**

Sendo o atual ambiente empresarial complexo, as PME assumem muitas formas e dimensões, podendo existir estreitas relações financeiras, operacionais ou de governação com outras empresas. Estas relações muitas vezes tornam difícil estabelecer uma fronteira precisa entre uma PME e uma empresa de maior dimensão.

O Guia da Comissão Europeia [12] é um instrumento prático destinado a ajudar as PME a identificarem-se enquanto tal, para poderem receber apoio da UE ou dos seus Estados-Membros. A definição de uma PME tem em conta os três critérios seguintes:

- efetivos;
- volume de negócios anual;
- balanço total anual.

Ao comparar os dados com os limiares estabelecidos para os três critérios, uma empresa pode determinar se é uma micro, pequena ou média empresa:

- Uma **Micro** empresa é definida como uma empresa que emprega menos de dez pessoas e cujo volume de negócios ou balanço total anual não excede 2 milhões de euros.
- Uma **Pequena** empresa é definida como uma empresa que emprega menos de 50 pessoas e cujo volume de negócios ou balanço total anual não excede 10 milhões de euros.
- Uma **Média** empresa é definida como uma empresa que emprega menos de 250 pessoas e que tem ou um volume de negócios anual que não excede 50 milhões de euros, ou um balanço anual não superior a 43 milhões de euros.

A Figura 4, representa os critérios de definição de uma PME, nos seus 3 critérios.

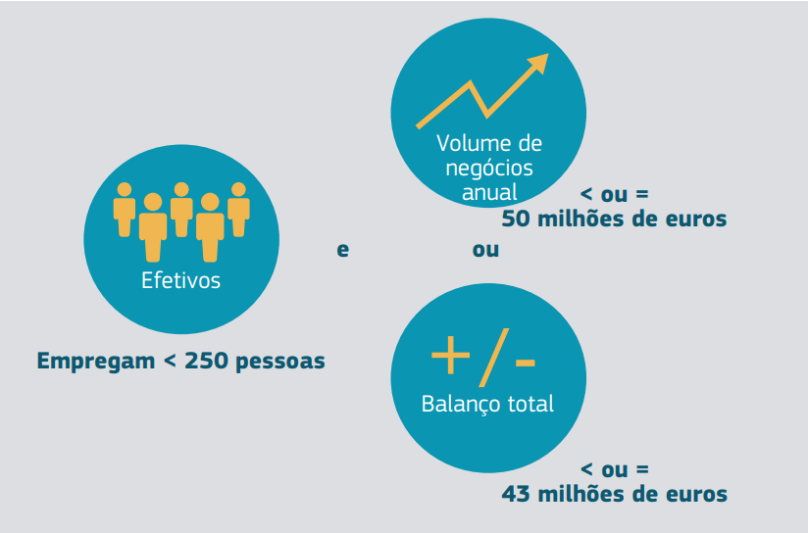



**Figura 4 – Critérios para a definição de PME na UE [12]**

Ainda segundo dados do INE[2], referentes ao ano de 2022, a Região Centro, tinha um, total de 286.988 PME, correspondendo a 19,98% do total nacional, sendo que a Região de Leiria tinha um total de 39.710 (2,78% do total nacional). A Tabela 1 apresenta um quadro da localização geográfica por dimensão de empresa, com uma distribuição pormenorizada da Região de Leiria e concelho de Leiria.

**Tabela 1 – Número de Empresas por Localização geográfica e Dimensão em Portugal**

| Localização geográfica (NUTS - 2013) | Número de Empresas por Localização geográfica e Dimensão | | | | | |
|---|---|---|---|---|---|---|
| | Período de referência dos dados - 2022 | | | | | |
| | Total Empresas | Total PME | Micro | Pequenas | Médias | Grandes |
| | N.º | N.º | N.º | N.º | N.º | N.º |
| **Portugal** | 1 437 254 | 1 435 818 | 1 380 398 | 47 406 | 8 014 | 1 436 |
| **Continente** | 1 374 879 | 1 373 497 | 1 320 435 | 45 343 | 7 719 | 1 382 |
| **Região de Leiria** | 39 733 | 39 710 | 37 697 | 1 730 | 283 | 23 |
| **Alvaiázere** | 888 | 888 | 853 | 30 | 5 | 0 |
| **Ansião** | 1 523 | 1 522 | 1 458 | 51 | 13 | 1 |
| **Batalha** | 2 190 | 2 190 | 2 050 | 123 | 17 | 0 |
| **Castanheira de Pêra** | 258 | 258 | 249 | 6 | 3 | 0 |
| **Figueiró dos Vinhos** | 642 | 642 | 628 | 14 | 0 | 0 |
| **Leiria** | 19 094 | 19 083 | 18 113 | 829 | 141 | 11 |
| **Marinha Grande** | 4 913 | 4 908 | 4 642 | 221 | 45 | 5 |
| **Pedrógão Grande** | 455 | 455 | 446 | 9 | 0 | 0 |
| **Pombal** | 6 748 | 6 746 | 6 370 | 332 | 44 | 2 |
| **Porto de Mós** | 3 022 | 3 018 | 2 888 | 115 | 15 | 4 |

[2] https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_indicadores&indOcorrCod=0009819&contexto=bd&selTab=tab2

As PMEs em Portugal empregavam 3.560.233 pessoas, (correspondendo a 79,33% dos empregos). Sendo que as PMEs do conselho de Leiria empregavam 116.058 pessoas (3,25% do total nacional). A Tabela 2, apresenta um quadro resumo dos dados do INE[3], com a localização geográfica por número de trabalhadores e dimensão da empresa, com uma distribuição pormenorizada da Região de Leiria e concelho de Leiria.

**Tabela 2 – Número de pessoas ao serviço das Empresas por Dimensão em Portugal**

| Localização geográfica (NUTS - 2013) | Pessoal ao serviço das Empresas por Dimensão e Localização geográfica | | | | |
|---|---|---|---|---|---|
| | Período de referência dos dados - 2022 | | | | |
| | Escalão de pessoal ao serviço | | | | |
| | Total | Menos de 10 pessoas | 10 - 49 pessoas | 50 - 249 pessoas | 250 e mais pessoas |
| | N.º | N.º | N.º | N.º | N.º |
| **Portugal** | 4 487 322 | 1 989 900 | 867 821 | 702 512 | 927 089 |
| **Continente** | 4 318 165 | 1 905 675 | 830 200 | 677 647 | 904 643 |
| **Centro** | 791 188 | 403 973 | 173 077 | … | … |
| **Região de Leiria** | 122 584 | 59 018 | 32 851 | 24 189 | 6 526 |

Através destes números pode-se perceber a importância que as PMEs representam para Portugal, assim como do concelho de Leiria.

## 2.2. Transformação Digital

Para Wade [13] (na publicação da *Global Center for Digital Business Transformation*), as ferramentas e tecnologias digitais estão a influenciar profundamente a maneira como os negócios são conduzidos hoje em dia. Elas já causaram disrupções em muitas indústrias e ameaçam fazer o mesmo em outras.

Nestes processos, existem sempre riscos e recompensas, porém, de maneira desigual. Sendo que algumas indústrias são mais afetadas do que outras, existem ações que as organizações podem tomar para aumentar as suas recompensas e reduzir os seus riscos.

A transformação digital dos negócios pode-se manifestar de várias formas, e uma transformação inteligente requer priorização. Para auxiliar no processo de decidir o que transformar, foi desenvolvido pelo autor uma ferramenta que a que chamou de "Plano de Digitalização". O plano de digitalização define 7 categorias distintas, cada uma das quais pode ser transformada digitalmente:

- **o modelo de negócio** - como uma empresa ganha dinheiro;
- **a estrutura** - como a empresa está organizada;
- **as pessoas** - que trabalham para a empresa;

[3] https://www.ine.pt/xportal/xmain?xpid=INE&xpgid=ine_indicadores&indOcorrCod=0009819&contexto=bd&selTab=tab2

- **os processos** - como uma empresa faz as coisas;
- **a capacidade de TI** - como a informação é gerida;
- **as ofertas** - que produtos e serviços uma empresa oferece;
- **o modelo de *Engagement*** - como a empresa interage com os seus *stakeholders*.

Algumas perguntas norteadoras para cada categoria são colocadas, e através das respostas pode ser criado um plano para responder às necessidades de transformação. Assim, uma organização pode criar um planeamento para a transformação digital do negócio. Dando enfase à vertente tecnológica, dentro das capacidades de TI, apresentam-se as seguintes questões:

- Quão eficaz é a infraestrutura de TI: É capaz de apoiar as suas ambições digitais?
- Quão eficaz é o TI voltado para o futuro: *website*, redes sociais?
- Quão eficaz é o seu relacionamento com o cliente (Sistema de Gestão)?
- A estratégia do TI é clara e alinhada com a estratégia corporativa?
- Os "ativos obscuros" estão ligados, existe acesso a todos os dados se necessários?
- Está a ser obtido valor dos dados?

Wade [13], concluí que que as oportunidades de uma transformação bem-sucedida são maiores se uma organização abordar mais do que um elemento ao mesmo tempo. Essa resposta é apropriada para as ameaças à disrupção digital, que frequentemente são encontradas se podem apresentar em várias formas.

## 2.3. Cadeias de abastecimento

Estrela [14], refere que as características das PMEs permitem-lhes fornecer produtos individualizados e funcionam como tecido auxiliar às grandes empresas, uma vez que uma esmagadora maioria das últimas recorre à subcontratação de empresas de menor dimensão para realizar serviços ou operações que, caso fossem feitas internamente, resultariam em custos maiores.

No mesmo trabalho sobre "A Gestão da Informação na Tomada de Decisão das PME da Região Centro" [14], refere que as PMEs, ao fazerem parte de uma cadeia de abastecimento de outras empresas de maior dimensão, no caso de alguns ciberataques, estes podem disseminar-se e comprometer a integridade dos seus sistemas de TI, afetando a sua capacidade produtiva (da empresa diretamente atingida), e por meio das relações da cadeia de abastecimento, também podem afetar os seus clientes e/ou fornecedores.

A PwC, na Pesquisa Global de Riscos 2022 [15], destaca que a cibersegurança desempenha um papel significativo na perda de confiança no ambiente empresarial atual. As empresas enfrentam uma série de desafios relacionados com a cibersegurança, incluindo ataques de *ransomware* cada vez mais frequentes e sofisticados. Esses ataques têm impactos diretos na confiança dos clientes, investidores e outras partes interessadas, colocando em risco a

reputação e a marca da empresa. O estudo enfatiza a necessidade de adaptação das capacidades de gestão de riscos e de resiliência das organizações para lidar com os desafios emergentes, como os relacionados à cibersegurança. A capacidade de resposta rápida e eficaz aos incidentes de cibersegurança é fundamental para proteger os ativos e a reputação da empresa.

Kamiya, Kang, Kim, Milidonis e Stulz [16], no seu trabalho, referem que quando os *stakeholders* de uma empresa observam um evento inesperado que afeta a empresa, eles podem decidir não fazer transações com a empresa em termos tão favoráveis quanto concordaram antes do evento. Por exemplo, se uma empresa divulga um defeito de produto que já foi totalmente resolvido, os clientes ainda podem estar dispostos a comprar os seus produtos a um preço mais baixo por considerarem o facto de que a empresa pode não ser tão confiável ou digna de confiança quanto pensavam. A perda que uma empresa sofre quando os *stakeholders* exigem melhores condições para fazer transações com ela após um evento inesperado, que torna a empresa mais arriscada para transacionar, é chamada de perda de reputação.

## 2.4. Gestão da Cibersegurança

Qualquer empresa que lida com dados sensíveis, como informações financeiras, dados pessoais de clientes, informações médicas ou propriedade intelectual, precisa de adotar medidas consistentes de cibersegurança para proteger esses dados contra acessos não autorizados.

As empresas que dependem fortemente da tecnologia para a sua operação, seja para processos internos, transações *online*, armazenamento em *cloud*, precisam de preparar a continuidade do negócio e evitar interrupções.

Empresas emergentes e em rápido crescimento muitas vezes são alvos atrativos para ciberataques, pois podem ter recursos limitados para investir em cibersegurança. No entanto, proteger os dados desde o início é crucial para evitar problemas futuros.

O Relatório Cibersegurança em Portugal - Economia [17], publicado em Maio de 2022, apresenta dados sobre as questões enfrentadas pelas empresas na dimensão económica da Cibersegurança pelas empresas Portuguesas. Este estudo baseia-se numa pesquisa extensiva e na análise de dados secundários de várias fontes. Os dados primários foram obtidos por meio de pesquisas conduzidas ou apoiadas pelo Observatório de Cibersegurança do Centro Nacional de Cibersegurança[4]. Ele examina o setor de cibersegurança em Portugal, analisando a oferta, e investiga a exposição, políticas e

[4] https://www.cncs.gov.pt/pt/observatorio/

práticas de cibersegurança em empresas portuguesas, especialmente nas pequenas e médias.

Os gastos anuais destinados à cibersegurança PMEs em Portugal apresentam uma grande disparidade. Cerca de 36,8% das empresas dedicam menos de 3.000 euros por ano a essas funções, enquanto aproximadamente 34,1% alocam uma quantia superior. Entre aquelas que investem mais de 3.000 euros, metade delas alocam valores entre 3.000 e 8.000 euros. Cerca de 7% destinam entre 8.000 e 15.000 euros, 6,6% entre 15.000 e 50.000 euros, e 3,4% mais de 50.000 euros. 20,7% das empresas não têm conhecimento, ou não revelam quanto gastam anualmente em cibersegurança, enquanto 8,6% delas não têm qualquer orçamento para este fim, como é possível verificar na Figura 5.

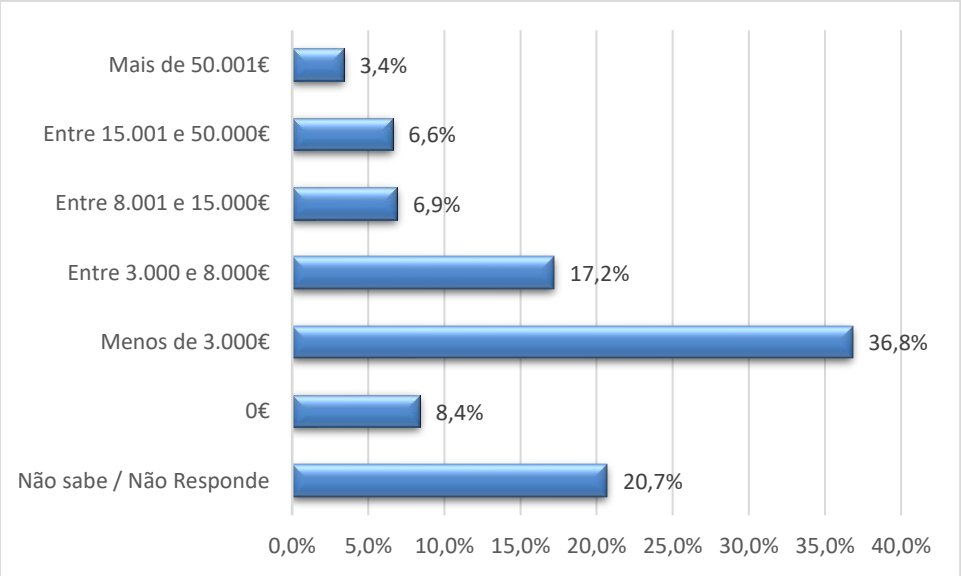



**Figura 5 – Orçamento anual de cibersegurança [17]**

Outro dado interessante apresentado pelo relatório prende-se com o responsável pela gestão da cibersegurança. Metade das empresas (50,4%) confiam a gestão da cibersegurança a uma empresa especializada ou a um profissional externo. Cerca de um terço das empresas (32,9%), a cibersegurança é tratada internamente, utilizando os recursos próprios da organização. Em 7,6% das empresas, não há ninguém designado para essas funções, enquanto 8,6% declaram não saber ou não têm informação sobre quem está encarregue desta função. Uma, em cada duzentas empresas, a gestão da cibersegurança fica a cargo de um membro da família ou de um amigo.

O relatório refere que conforme as organizações crescem em tamanho, nota-se uma diminuição nas respostas 'Ninguém' e 'Não sabe/Não responde'. A gestão informal da cibersegurança, realizada por familiares e amigos, é praticamente insignificante em pequenas empresas e completamente inexistente nas médias empresas. Nas empresas de maior dimensão, a gestão interna ganha relevância, em comparação com a externalização, como é possível verificar na Figura 6.

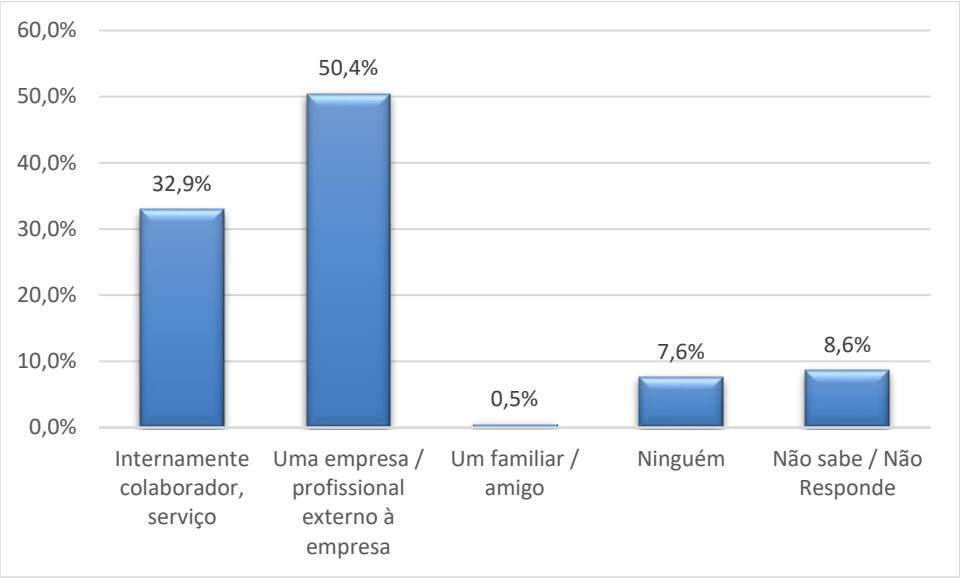



**Figura 6 – Responsabilidade pela gestão de cibersegurança [17]**

As principais práticas de segurança das TIC adotadas pelas empresas pesquisadas incluem a atualização regular de *software* (86,3%), autenticação de utilizadores por meio de palavras-passe seguras (77,8%) e controlo de acesso à rede corporativa (72,9%). Cerca de um terço das empresas (34,3%) mantém registos para análise pós-incidentes de segurança, enquanto aproximadamente um quinto (20,9%) emprega técnicas de cifragem dos dados, documentos ou *e-mails*. Os testes de segurança são apenas realizados por 22,0% e a avaliação de riscos adotadas por 18,9% das empresas. Com o aumento da sua dimensão, a percentagem de empresas que adotam cada uma das medidas de segurança das TIC consideradas é superior, como é possível verificar na Figura 7.

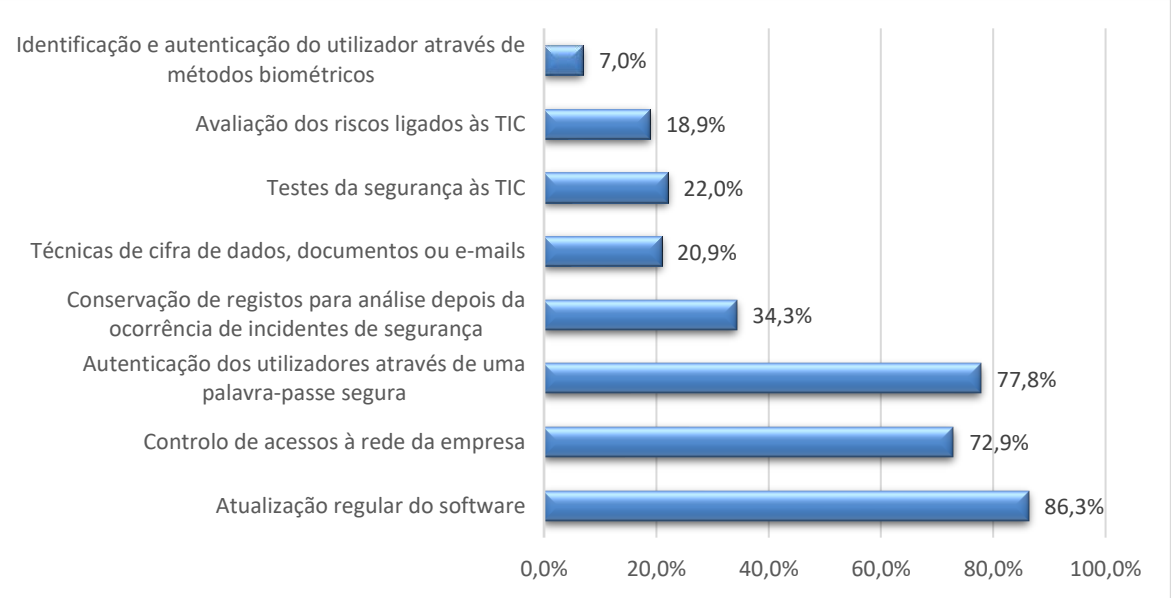



**Figura 7 – Principais medidas de segurança das TIC [17]**

Cerca de metade das empresas (47,1%) apontam o custo e a alocação de recursos como a principal barreira para implementar medidas de melhoria na cibersegurança. Outros desafios mencionados incluem a falta de cultura de cibersegurança entre os colaboradores (26,5%), escassez de pessoal qualificado (22,6%) e desconhecimento sobre as medidas a serem adotadas (22,0%). A aquisição de tecnologia adequada é uma barreira de menor relevância para as empresas (11,4%), como é possível verificar na Figura 8.

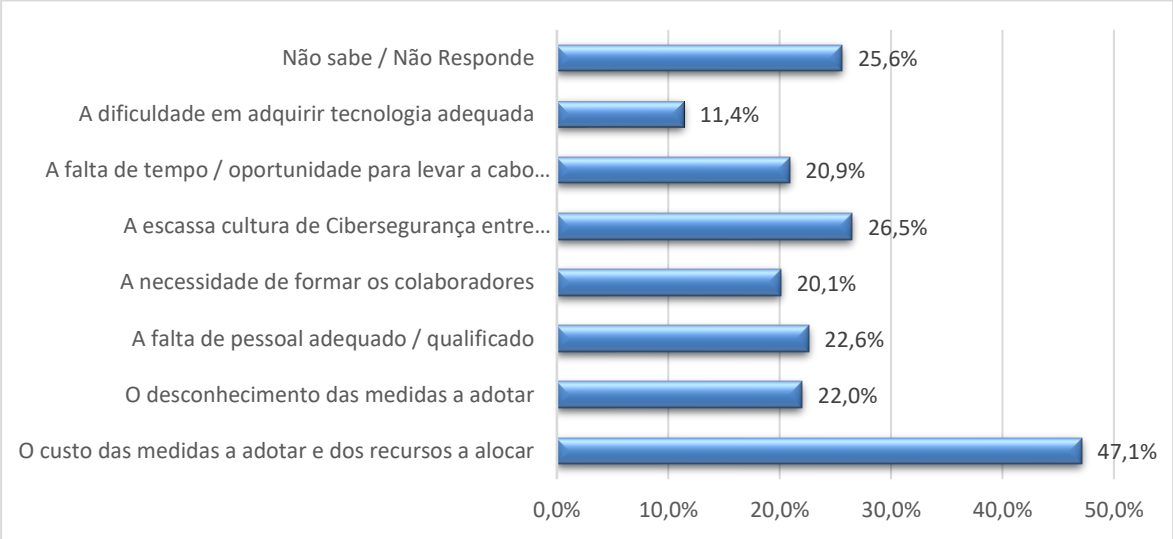



**Figura 8 – Principais barreiras para melhorar o nível de cibersegurança [17]**

## 2.5. Cibersegurança

Samonas e Coss [18], referem que o tríade *Confidentiality Integrity Availability (CIA)* tem sido uma pedra angular nas práticas de segurança da informação há décadas, inicialmente decorrente da necessidade militar de proteger informações classificadas. No entanto, à medida que a tecnologia de computadores evoluía e se tornava mais acessível, o foco mudava da proteção de *hardware* para a proteção contra divulgação não autorizada de informações, modificação não autorizada de dados e negação de uso não autorizada. Ao longo do tempo, modelos de segurança como Bell-La Padula [19] (confidencialidade), Biba [20] (integridade) e o modelo de deteção de intrusões de Denning [21] (disponibilidade) foram desenvolvidos para abordar essas preocupações. Lançaram as bases para o triângulo CIA, que estes têm sido amplamente utilizados na prática de segurança da informação e na literatura.

Através da revisão da literatura foi possível obter algumas definições de cibersegurança, que se considera fornecer as perspetivas da cibersegurança.

Kemmerer [2] define "*Cybersecurity consists largely of defensive methods used to detect and thwart would-be intruders*".

A ITU [22] define a Cibersegurança como uma coleção de ferramentas, políticas, conceitos de segurança, salvaguardas de segurança, diretrizes, abordagens de gestão de risco, ações, formação, melhores práticas, garantias e tecnologia, que podem ser usadas para proteger o ambiente de cibersegurança de uma organização e os ativos do utilizador.

Já para NICCS [23] define a Cibersegurança como atividade/processo, habilidade/capacidade ou estado, através do qual os sistemas de informação e comunicação e as informações neles contidas são protegidos e/ou defendidos contra danos, uso ou modificação não autorizada ou exploração.

Schatz, Bashroush e Wall [24] definem como a abordagem e ações associadas aos processos de gestão de riscos de segurança seguidos por organizações e Países para proteger a confidencialidade, integridade e disponibilidade de dados e ativos utilizados no ciberespaço.

NIST [25] define "*The ability to protect or defend the use of cyberspace from cyber-attacks*".

## 2.6. Estratégia da União Europeia para a Cibersegurança

Em 2016 a União Europeia (UE), aprovou a Diretiva NIS 2016/1148 [26], sobre a Segurança de Redes e Sistemas de Informação, esta legislação estabelece as medidas para aumentar a cibersegurança em toda a UE. O seu objetivo principal foi a melhoria da resiliência das infraestruturas críticas e dos serviços digitais, estabelecendo requisitos de segurança e gestão de incidentes, que os países membros devem implementar nas suas políticas nacionais de cibersegurança. Este documento marcou a primeira ação legislativa da UE para fortalecer a colaboração entre os Estados-membros no campo da cibersegurança.

A NIS 2016/1148 [26] estabelece requisitos de segurança para operadores de serviços considerados essenciais, em setores críticos como:

- energia;
- transportes;
- instituições financeiras;
- infraestruturas de mercado;
- saúde;
- abastecimento de água potável;
- infraestruturas digitais.

Aplicando-se também aos fornecedores de serviços digitais, como plataformas de comércio online, motores de pesquisa e serviços *cloud*.

Esta Diretiva, foi transposta para Lei n.º 46/2018 a 13 de agosto de 2018 [27], estabelecendo o regime jurídico da segurança do ciberespaço, definindo também o Centro Nacional de Cibersegurança (CNCS) como responsável pela supervisão da adequada implementação da Diretiva NIS.

O Decreto-Lei n.º 65/2021 de 30 de julho de 2021 [28], veio regulamentar o regime jurídico da segurança do ciberespaço e definir os requisitos para as entidades, nomeadamente:

- comunicação do ponto de contacto permanente e responsável de segurança;
- comunicação do inventário dos ativos essenciais para a prestação dos serviços;
- execução de análises dos riscos globais e parciais;
- elaboração e atualização de um plano de segurança;
- comunicação do relatório anual;
- implementação de meios que permitam detetar, classificar e notificar incidentes ao CNCS.

Já em 14 de dezembro de 2022, foi publicada pela UE a Diretiva NIS2 2022/2555 [29] que vem substituir a Diretiva NIS 2016/1148. Nesta nova Diretiva, é feita uma extensão do âmbito de aplicação, tendo sido acrescentados os seguintes setores à lista de setores críticos definidos nos Anexos I e II:

Anexo I:

- águas residuais;
- gestão de serviços TIC (entre empresas);
- administração pública;
- espaço.

Anexo II:

- serviços postais e de estafeta;
- gestão de resíduos;
- produção, fabrico e distribuição de produtos químicos;
- produção, transformação e distribuição de produtos alimentares;
- indústria transformadora;
- prestadores de serviços digitais;
- investigação.

Esta nova Diretiva (NIS2) terá de ser transposta para legislação nacional até 17 de outubro de 2024.

Essa transição destaca o compromisso da UE em fortalecer a resiliência e promover uma abordagem coordenada para lidar com ameaças digitais em toda a UE. Ao promover a cooperação, visa melhorar a troca de informações e melhores práticas, para além de fortalecer os mecanismos de supervisão.

A implementação exigirá recursos adequados, colaboração contínua entre os setores público e privado e adaptação às mudanças tecnológicas em curso. A transição da NIS para a NIS2 é mais um passo na proteção dos sistemas de informação críticos, reconhecendo a importância crescente da cibersegurança num mundo digital em constante evolução.

## 2.7. Normas de Cibersegurança

A identificação e utilização de *standards* de cibersegurança, é fundamental pois fornecem diretrizes e práticas para fortalecer a postura de segurança das organizações e pessoas.

### 2.7.1. NIST - *Cybersecurity Framework*

O *National Institute of Standards and Technology*, denominado de NIST [30], é uma agência do Departamento de Comércio dos Estados Unidos da América (EUA), em que a sua origem remonta ao final do século XIX, quando foi fundado como *Bureau of Standards* em 1901. A sua principal função era promover a padronização de pesos e medidas nos Estados Unidos, mas ao longo do tempo, as suas responsabilidades cresceram para incluir o desenvolvimento e a promoção de *standards* de tecnologia, segurança, criptografia, ciência de dados, entre outros.

A primeira versão (1.0) da *Cybersecurity Framework* (CSF) [31], foi lançada em 2014 como resposta às crescentes ameaças à cibersegurança enfrentadas por organizações públicas e privadas nos EUA. Em abril de 2018, foi feita atualização para versão 1.1 [4], esta versão não representou uma revisão completa, mas sim uma continuação melhorada da versão 1.0, integrando *feedbacks* e contribuições da comunidade de cibersegurança. Um dos aspetos mais relevantes foi a ampliação das subcategorias existentes, proporcionando uma visão mais detalhada sobre as práticas recomendadas para a implementação dos controlos de segurança.

O objetivo *Cybersecurity Framework* é fornecer orientação e instruções claras para ajudar as organizações a fortalecer a sua postura de cibersegurança, independentemente do setor ou tamanho. Pretende fornecer um conjunto de práticas recomendadas para a cibersegurança, permitindo uma compreensão comum entre as organizações, ajudando a melhorar a comunicação e colaboração. Devido à sua flexibilidade, permite que as organizações personalizem as suas abordagens de cibersegurança de acordo com suas necessidades específicas, riscos, tamanho e capacidades existentes.

Promovendo uma cultura da melhoria contínua, incentiva as organizações a rever e melhorar constantemente as suas práticas de segurança. Oferece uma estrutura abrangente que aborda não apenas as questões técnicas, mas também os aspetos relacionados com a *governance* e as pessoas, reconhecendo que a cibersegurança é uma responsabilidade partilhada entre as várias partes de uma organização.

*A NIST Cybersecurity Framework* é composta por cinco áreas principais, representadas na Figura 9, sendo estes a: **Identificação, Proteção, Deteção, Resposta** e **Recuperação**, conhecidas como "funções", que fornecem uma estrutura abrangente para ajudar as organizações a entender, gerir, planear e implementar estratégias eficazes, abordando os diversos pontos, por forma a melhorar sua postura.


**Figura 9 – Atributos chave da NIST *Cybersecurity Framework*** [5]

[5] https://www.nist.gov/document/cybersecurityframeworkv1-1presentationpptx

Na Tabela 3, são apresentadas as cinco função da *NIST Cybersecurity Framework* [4], e fornece uma visão geral concisa das principais áreas de foco desta estrutura.

**Tabela 3 – Descrição de atributos chave da NIST CSF**

| | |
|---|---|
| **Identificar** | Compreender e gerir os riscos de cibersegurança para o sistemas, pessoas, processos e tecnologias.<br>Incluí a identificação de ativos críticos, avaliação de vulnerabilidades, compreender as potências ameaças e entender o contexto funcional e regulamentar no qual a organização está sujeita. Ter uma compreensão clara dos processos de negócios e como eles podem ser afetados por possíveis falhas de segurança. |
| **Proteger** | Desenvolver e implementar medidas de segurança para proteger sistemas e dados contra ameaças à cibersegurança.<br>Após identificação, esta área concentra-se na implementação de medidas de segurança apropriadas para mitigar esses riscos. Isso incluí o estabelecimento de controlos de acesso, formação e consciencialização dos utilizadores, implementação de tecnologias de segurança, além de políticas e procedimentos de segurança eficazes. |
| **Detetar** | Estabelecer capacidades para identificar a ocorrência de incidentes de cibersegurança.<br>O objetivo desta área é estabelecer a capacidade de identificar incidentes o mais rápido possível. Isso envolve a implementação de sistemas e processos para detetar atividades suspeitas, ou não autorizadas, nos sistemas de informação da organização, assim como a sua monitorização.<br>Entender o impacto de eventos de cibersegurança é crucial, e comunicar informações às partes interessadas, fortalece relacionamentos.<br>Conhecer os fluxos de dados esperados na empresa aumenta a capacidade de detetar atividades inesperadas, sendo essencial para a cibersegurança. |
| **Responder** | Desenvolver planos de resposta a incidentes de cibersegurança para lidar com ameaças identificadas.<br>Testar e manter os planos de resposta atualizados é crucial para garantir que todos compreendem as suas responsabilidades. Quanto mais preparada a organização estiver, maior a possibilidade de uma resposta eficaz.<br>A coordenação com partes interessadas, internas e externas, incluindo prestadores de serviços, é fundamental para melhorar os planos de resposta. |
| **Recuperar** | Restaurar e retomar o normal funcionamento dos sistemas e processos após um incidente de cibersegurança, o mais rápido possível.<br>Incluí a análise do que aconteceu, a melhoria de medidas de segurança para evitar incidentes semelhantes no futuro, e a recuperação de dados e sistemas para garantir a continuidade dos negócios.<br>A comunicação com partes interessadas (internas e externas), é crucial durante a recuperação. Os planos, devem detalhar como, e quando, as informações devem ser partilhadas, garantindo que as partes recebem os dados relevantes sem divulgar informações inadequada. |

Os vários níveis de implementação da *framework* oferecem uma visão da postura de cibersegurança da organização, em relação ao risco e aos seus processos de gestão. Esses níveis, variam de **Parcial** (Nível 1) a **Adaptativo** (Nível 4) [4], onde indicam o nível de rigor e sofisticação na gestão de riscos da organização. Eles refletem o quanto a organização considera as necessidades do negócio, e integra a cibersegurança nas práticas gerais de gestão de riscos. O processo de seleção do nível leva em conta práticas atuais de gestão do risco, ambiente de ameaças, requisitos legais, objetivos de negócios, segurança da cadeia de valor e restrições organizacionais. É essencial que as organizações determinem o nível desejado, alinhado aos objetivos organizacionais, viável para implementação, e capaz de reduzir o risco de cibersegurança para níveis aceitáveis.

Para as pequenas empresas o NIST desenvolveu o *Cybersecurity Framework Steps for Small Manufacturers* [32], destinado a enfrentar, de forma rápida e económica, as ameaças à cibersegurança. Estas são etapas simples e de baixo custo, onde se baseiam nas orientações oficiais da *framework* de cibersegurança, que foram adaptadas para atender às necessidades destas empresas, para que possam identificar, avaliar e gerir os riscos de cibersegurança.

O NIST encontra-se a desenvolver a *Cybersecurity Framework* 2.0 [33], que corresponde a uma evolução da versão anterior e que apresenta melhorias estando mais adaptada para responder aos novos desafios. A nova versão está a ser desenvolvida para ser ainda mais flexível, permitindo que as organizações de várias dimensões, e setores, adaptem as práticas de cibersegurança de acordo com suas necessidades específicas. Reforça a importância da gestão de riscos em todos os níveis da organização, auxiliando na identificação, avaliação e mitigação de ameaças. Incorpora práticas como inteligência artificial, automação e *machine learning*, para ajudar as organizações a enfrentarem ameaças cada vez mais avançadas. Assim como pretende alinhar-se e integrar-se mais profundamente com outros *standards* e *frameworks* de segurança, facilitando a adoção conjunta e a interoperabilidade com outras práticas de cibersegurança.

### 2.7.2. ISO/IEC 27001

ISO/IEC 27001 [34] é o *standard* mais conhecido e denominado de *Information Security Management Systems* (ISMS), também conhecido como Sistema de Gestão da Segurança da Informação (SGSI). Este fornece diretrizes e práticas recomendadas para apoiar as organizações a gerir e proteger os ativos de informação.

A ISO/IEC 27001, teve a sua origem na norma BS 7799, desenvolvida pela *British Standards Institution* (BSI), quando existiu uma crescente preocupação com a segurança da informação, à medida que existiu uma dependência da tecnologia pelas organizações.

A ISO/IEC 27001:2022, foi publicada em outubro de 2022, que vem atualizar a versão de ISO/IEC 27001:2013, onde as alterações estão centradas nos controlos do Anexo A, que foram reagrupados, renomeados ou adicionados.

"A implementação da norma ISO/IEC 27001, permite às organizações uma eficaz gestão e proteção de toda a informação considerada crítica, através da correta seleção e implementação dos controlos de segurança, originando assim um elevado grau de confiança de todas as partes interessadas, principalmente dos clientes" [35].

Para a BSI [36], as empresas ao aplicarem a ISO/IEC 27001, podem ter benefícios, como:

- Proteção da empresa, reputação e agregação de valor;
- Proteção de registos pessoais e informações confidenciais;
- Redução do risco;
- Aumento da confiança na da organização.

A Figura 10, representa de forma esquemática estes benefícios.


**Figura 10 - Principais benefícios da ISO/IEC 27001 sentidos pelos clientes BSI [36]**

Segundo dados do Instituto Português de Acreditação (IPAC) [37], referentes a 31-12-2022, atualizados a 27-03-2023, em Portugal no ano de 2022, existiam 162 empresas certificadas, na ISO/IEC 27001. Na Tabela 4, é possível acompanhar a evolução desde 2019 do número de empresas certificadas. Estas quase que duplicaram nos últimos 4 anos (a que se referem os dados publicados). O que indicia uma evolução na importância que as empresas têm dado na certificação deste referencial de segurança da informação.

**Tabela 4 – Evolução das empresas certificadas ISO/IEC 27001** [6]

| Nº Certificados | Sist.Gestão | 2019 | 2020 | 2021 | 2022 |
|---|---|---|---|---|---|
| ISO/IEC 27001 | T.Informação | 87 | 99 | 134 | 162 |

Na Tabela 5, é apresentado um resumo do sector de atividade económica, onde é possível verificar que o sector das tecnologias de informação e informática está destacado nesta certificação com 86 empresas, representando 47,2% do total.

**Tabela 5 – Empresas certificadas no sector de atividade económica**[7]

| Código IAF | Certificadas no sector de atividade económica | Nº Empresas |
|---|---|---|
| **3** | Indústrias alimentares, bebidas e tabaco | 19 |
| **4** | Indústria têxtil | 1 |

[6] http://www.ipac.pt/docs/publicdocs/bdec/BDEC_2022_Publica_v3.xlsx
[7] existem empresas que pertencem a mais de um setor

| | | |
|---|---|---|
| **9** | Impressão, serviços relacionados com a impressão e reprodução de suportes gravados | 2 |
| **19** | Fabrico de equipamento elétrico e de ótica | 5 |
| **20** | Construção e reparação naval | 9 |
| **22** | Fabrico de material de transporte (exceto construção e reparação naval, fabrico de aeronaves e de veículos espaciais) | 1 |
| **24** | Reciclagem | 1 |
| **25** | Produção, transporte e distribuição de eletricidade | 2 |
| **27** | Produção e distribuição de água | 1 |
| **29** | Comércio por grosso e a retalho; reparação de veículos automóveis, motociclos e bens de uso pessoal e doméstico | 5 |
| **30** | Alojamento e restauração (restaurantes e similares) | 0 |
| **31** | Transportes, armazenagem e comunicações | 19 |
| **32** | Atividades financeiras e imobiliárias; aluguer de máquinas e equipamentos sem pessoal, e de bens pessoais e domésticos | 6 |
| **33** | Tecnologias de informação e informáticas | 86 |
| **34** | Investigação e desenvolvimento; arquitetura, engenharia e técnicas afins | 22 |
| **35** | Outros serviços | 34 |
| **36** | Administração pública, defesa e segurança social obrigatória | 3 |
| **37** | Educação | 1 |
| **39** | Outros serviços coletivos, sociais e pessoais | 4 |
| **Não Classif** | Não classificadas ou identificadas | 1 |

Já na Tabela 6, são apresentados os dados pertencentes à Região Centro com um total de 15 empresas, correspondendo a 9,2% do total de empresas certificadas. Sendo que Lisboa e Porto possuem 124 empresas certificadas, representado 79% do total.

**Tabela 6 – Empresas Certificadas ISO/IEC 27001, região Centro**

| Entidade | Normas | Código(s) EA | Local |
|---|---|---|---|
| ANKIX SYSTEMS, Lda | ISO/IEC 27001:2013 | 33 | Aveiro |
| BLUETREND TECHNOLOGIES, LDA | ISO/IEC 27001:2013 | 33 | Coimbra |
| Câmara Municipal de Águeda | ISO/IEC 27001:2013 | 36 | Aveiro |
| ENEIDA, GRID INTELLIGENCE, S.A. | ISO/IEC 27001:2013 | 19 | Coimbra |
| GLAREVISION, S.A. | ISO/IEC 27001:2013 | 33 | Leiria |
| HUMAN PROFILER, Lda | ISO/IEC 27001:2013 | 35 | Aveiro |
| inCentea - Tecnologia de Gestão, S.A.; | ISO/IEC 27001:2013 | 33 | Leiria |
| INOVAR +AZ - SISTEMAS DE INFORMAÇÃO, LDA | ISO/IEC 27001:2013 | 33 | Aveiro |
| MATCH PROFILER - Consultadoria e Desenvolvimento de Sistemas de Gestão, Lda | ISO/IEC 27001:2013 | 33 | Aveiro |
| PARADIGMA RESILIENTE - LDA | ISO/IEC 27001:2013 | 19 | Guarda |
| PLM PLURAL, S.A. | ISO/IEC 27001:2013 | 34 | Aveiro |
| SOCARTO - Sociedade de Levantamentos Topo Cartográficos, Lda | ISO/IEC 27001:2013 | 34 | Leiria |

| | | | |
|---|---|---|---|
| SYS-MATCH - Consultores de Sistemas de Informação, Lda | ISO/IEC 27001:2013 | 33 | Aveiro |
| Uartrónica - Electrónica, Lda. | ISO/IEC 27001:2013 | 19 | Aveiro |
| WAVECOM - SOLUÇÕES RADIO SA | ISO/IEC 27001:2013 | 31;34 | Aveiro |

Já na região de Leiria existem 3 empresas certificadas (1,8% do total nacional), pertencendo aos setores de atividade Tecnologias de informação e informática (2) e Investigação e desenvolvimento; arquitetura, engenharia e técnicas afins (1), como é possível verificar na Tabela 7.

**Tabela 7 – Empresas certificadas ISO/IEC 27001, região de Leiria**

| Entidade | Normas | Código(s) EA | Local |
|---|---|---|---|
| GLAREVISION, S.A. | ISO/IEC 27001:2013 | 33 | Leiria |
| inCentea - Tecnologia de Gestão, S.A.; | ISO/IEC 27001:2013 | 33 | Leiria |
| SOCARTO - Sociedade de Levantamentos Topo Cartográficos, Lda | ISO/IEC 27001:2013 | 34 | Leiria |

Os principais controlos da ISO/IEC 27001:2022 [5], são na sua base os mesmos que na versão anterior, contudo, trouxeram atualizações nos requisitos e orientações. Centrando-se numa abordagem mais moderna e alinhada com a evolução da tecnologia e dos desafios de segurança da informação, estando divididos em 4 controlos: **Organizacionais, Pessoas, Físicos** e **Tecnológicos**.

**Organizacionais**

- Definição, aprovação, publicação e comunicação das políticas de segurança da informação, garantindo que sejam conhecidas pelos envolvidos e revistas periodicamente.
- Definição e atribuição de funções relacionadas com a segurança da informação de acordo com as necessidades da organização.
- Evitar conflitos de responsabilidades em áreas conflituantes.
- Garantir que todos os colaboradores aplicam a segurança da informação de acordo com as políticas estabelecidas.
- Estabelecer e manter contato com autoridades e grupos especializados em segurança.
- Recolher e analisar informações sobre ameaças à segurança da informação para produzir conhecimento das ameaças.
- Gerir ativos de informação, políticas de uso aceitável, controlo de acesso, gestão de identidades, segurança nas relações com fornecedores e acordos de fornecimento.
- Definição e implementação de processos para gerir riscos de segurança em serviços de fornecedores, segurança na utilização de serviços em *cloud*, preparação e resposta a incidentes de segurança.

- Planos de continuidade de negócios, resposta a requisitos legais, proteção da propriedade intelectual, proteção de registos, privacidade e proteção de informações pessoais.
- Documentação de procedimentos.

**Pessoas**

- Gestão de permissões para acesso a recursos e informações sensíveis.
- Administração de identidades digitais dos funcionários, incluindo criação, manutenção e exclusão de contas.
- Divisão das responsabilidades entre diferentes pessoas para evitar conflitos de interesse e possíveis fraudes.
- Garantir que uma única pessoa não tem controlo sobre todas as fases de uma atividade crítica.
- Definir como os dados pessoais são recolhidos, usados, armazenados e partilhados.
- Formação dos utilizadores sobre práticas de segurança, políticas da empresa e ameaças à cibersegurança.
- Estabelecer procedimentos para lidar com violações de segurança ou incidentes relacionados às pessoas.
- Definir etapas para investigação, resposta e mitigação de riscos.

**Físicos**

- Definição e uso de perímetros de segurança para proteger áreas que contêm informações e ativos sensíveis.
- Implementação de segurança física para escritórios, salas e instalações, assim como a sua monitorização.
- Proteção contra ameaças físicas e ambientais, como desastres naturais e ameaças físicas intencionais ou não à infraestrutura.
- Medidas de segurança para trabalhar em áreas restritas.
- Regras para manter mesas limpas de papéis e dispositivos removíveis,
- Localização segura e proteção adequada dos equipamentos.
- Proteção de ativos que se encontram fora das instalações da organização.
- Gestão da vida útil de dispositivos de armazenamento, incluindo aquisição, uso, transporte e destruição, conforme requisitos de classificação e manipulação da organização.
- Proteção das instalações de processamento contra falhas de energia ou outras interrupções.
- Proteção dos cabos de transporte de energia ou dados contra intercetação, interferência ou danos.
- Manutenção adequada de equipamentos para garantir a disponibilidade, integridade e confidencialidade da informação.

- Remoção de dados sensíveis e *software* licenciado de equipamentos antes da sua reutilização ou destruição.

**Tecnológicos**

- Proteção das informações em dispositivos dos utilizadores.
- Restrição e gestão dos direitos de acesso privilegiado.
- Gestão adequada do acesso ao código fonte e ferramentas de desenvolvimento.
- Implementação de tecnologias e procedimentos seguros de autenticação.
- Monitorização e ajustes de recursos de acordo com as necessidades.
- Implementação de proteção contra *malware* apoiada por consciencialização do utilizador.
- Identificação, avaliação e mitigação de vulnerabilidades técnicas em sistemas.
- Estabelecimento, documentação e monitorização das configurações de *hardware*, *software* e redes.
- Eliminação segura de informações quando não forem necessárias.
- Anonimização de dados.
- Aplicação de medidas de prevenção de fugas de informação.
- Manutenção de cópias de segurança da informação.
- Implementação de soluções redundantes para responder aos requisitos de disponibilidade.
- Armazenamento e análise de registos de atividades relevantes.
- Monitorização de redes, sistemas e aplicações para deteção de comportamentos anómalos.
- Sincronização dos relógios de sistemas de processamento de informação.
- Restrição e controlo do uso de programas que possam sobrepor-se a controlos do sistema.
- Procedimentos seguros para gerir a instalação de *software* em sistemas.
- Proteção e gestão de dispositivos de rede para proteger informações.
- Separação de redes da organização.
- Gestão de acesso a *websites* externos para reduzir exposição a conteúdo malicioso.
- Regras para o uso efetivo de cifragem e gestão de chaves.
- Regras para o desenvolvimento seguro de *software* e sistemas.
- Definição e implementação de processos de teste de segurança no ciclo de vida do desenvolvimento.
- Segregação e proteção dos ambientes de desenvolvimento, teste e produção.
- Procedimentos de gestão de mudanças para sistemas de processamento.
- Seleção, proteção e gestão apropriada de informações de teste.

A aplicação do ciclo PDCA (*Plan-Do-Check-Act*) na ISO/IEC 27001:2022 [38], desempenha um papel decisivo na garantia da eficácia, e na constante melhoria dos processos de cibersegurança numa organização. Esta estabelece diretrizes e requisitos para a

implementação, manutenção e melhoria de um Sistema de Gestão de Segurança da Informação.

Na fase de ***Plan*** (Cláusulas 0 a 3), são identificados os riscos de segurança da informação enfrentados pela organização. Isso envolve a definição de objetivos de segurança, avaliação de vulnerabilidades, identificação de ameaças e criação de políticas e controlos de segurança.

Na fase do ***Do*** (Cláusulas 4 a 8), os planos definidos são implementados, incluindo a aplicação das políticas de segurança, formação dos utilizadores, aquisição tecnológica e a execução dos controlos estabelecidos para proteger a informação da organização.

A fase ***Check*** (Cláusula 9), concentra-se na avaliação da eficácia dos controlos e medidas de segurança implementados, são realizadas auditorias, revisões e avaliações para garantir que os controlos estão a funcionar conforme o esperado, e sejam capazes de mitigar os riscos identificados.

Por fim, na fase ***Act*** (Cláusula 10), com base nos resultados das avaliações, são implementadas ações corretivas e preventivas, pode envolver ajustes nos controlos, revisão de políticas ou procedimentos, para melhorar a eficácia da segurança da informação.

A importância do PDCA reside na sua capacidade de promover uma abordagem sistemática e cíclica para melhorar continuamente os processos de segurança da informação. Ele ajuda a identificar falhas, ações inadequadas ou áreas que requerem melhorias, permitindo que a organização reaja proactivamente a novas ameaças e mantenha a conformidade com os *standards* de segurança.

A Norma ISO/IEC 27001 não é disponibilizada gratuitamente, sendo um documento normativo oficial precisa ser adquirido ao IPQ[8]. No entanto, existem informações e recursos disponíveis publicamente que oferecem uma visão geral e orientações sobre a norma, sendo que o documento oficial não está acessível sem custos.

### 2.7.3. Quadro Nacional de Referência para a Cibersegurança

O Quadro Nacional de Referência para a Cibersegurança, denominado QNRSC [6] é um guia de cibersegurança que visa oferecer às organizações uma estrutura para lidar com as ameaças atuais sobre os ativos de informação. Alinhado com a Lei n.º 46/2018 [27] que trata da segurança no ciberespaço, transpondo a Diretiva SRI [26] (ou NIS) da União Europeia, relativa a medidas destinadas a garantir um elevado nível comum de segurança

[8] https://www.ipq.pt/loja/normas/

das redes e dos sistemas de informação em toda a União. A Figura 11, representa numa linha temporal a evolução da estratégia nacional de segurança do ciberespaço.


**Figura 11 – Enquadramento cronológico [6]**

Este procura estabelecer os requisitos mínimos de segurança da informação recomendados. Reconhecendo a diversidade de organizações em termos de tamanho e maturidade, o documento sugere uma abordagem crítica e flexível, encorajando cada organização a adaptar as medidas de segurança às suas necessidades específicas.

O guia está estruturado em cinco objetivos principais: **Identificar, Proteger, Detetar, Responder** e **Recuperar**. Cada objetivo é subdividido em categorias e subcategorias, com exemplos de implementação tecnológica, processual e evidências correspondentes. Estes exemplos não são uma lista rígida de ações, mas representam diretrizes de alto nível baseadas em referências internacionais e normas técnicas. Na Figura 12, encontram-se representados os objetivos de segurança do QNRCS.


**Figura 12 – Objetivos de segurança definidos no QNRCS [6]**

- **Identificar:** Consiste em entender o contexto da organização, os seus ativos essenciais para os processos críticos e os riscos relevantes associados. Essa compreensão guia a definição e prioritização de recursos e investimentos de acordo com os objetivos gerais e a estratégia de gestão de riscos da organização.
- **Proteger:** Envolve a implementação de medidas para proteger os processos e ativos da organização, independentemente de sua natureza tecnológica. Essas medidas são direcionadas para proteger a organização em três dimensões: Pessoas, Processos e Tecnologia.
- **Detetar:** Definição e aplicação de medidas para identificar prontamente incidentes, ou, reconhecer eventos que possam afetar adversamente a segurança das redes e sistemas de informação.

- **Responder**: Consiste na definição e execução de ações adequadas após a deteção de um incidente. As medidas propostas buscam mitigar o impacto do incidente, reduzindo seus potenciais efeitos adversos.
- **Recuperar:** Envolve a definição e aplicação de atividades para gerir os planos e medidas de recuperação dos processos e serviços afetados por um incidente de cibersegurança. Essas medidas visam garantir a resiliência da organização em suas dimensões: Pessoas, Processos e Tecnologia, permitindo à organização utilizar essas medidas para apoiar a recuperação oportuna de suas atividades após um incidente.

As diretrizes e medidas propostas pelo QNRCS, fundamentam-se em quarto referências, que tratam da segurança da informação e cibersegurança de maneira complementar. Todos eles têm reconhecimento global como alicerce para aplicação e análise de medidas de gestão de riscos, e boas práticas no contexto de governo, segurança da informação e/ou cibersegurança:

- NIST SP-800-53 Rev4 - na Secção 2.7.1 foi abordada a estrutura NIST CSF, que se centra numa abordagem baseada em risco, a SP 800-53, fornece controlos técnicos e detalhados. O CSF foi desenhado para ser mais flexível e adaptável às ameaças, enquanto o SP 800-53 fornece controlos de segurança específicos para cada sistema, assim como orientações sobre como selecionar, implementar e avaliar controlos de segurança;
- ISO/IEC 27001:2013 - temática abordado na Secção 2.7.2;
- *CIS Controls* 7.0 - abordado na Secção 2.7.4, na versão 8.0;
- COBIT 5 [39]- é uma framework de governo e gestão de TI desenvolvido pela ISACA (*Information Systems Audit and Control Association*). Ele oferece princípios, práticas, ferramentas e modelos que ajudam as organizações a gerir e controlar seus sistemas de informação de forma eficaz. Auxilia na *governance* de TI, fornece diretrizes para alinhar os objetivos de negócio com os recursos de tecnologia da informação, garantindo a entrega de valor, mitigação de riscos e uso adequado dos recursos.

O Quadro de Avaliação de Capacidades de Cibersegurança [40] é um complemento ao QNRCS, seguindo a estratégia do Centro Nacional de Cibersegurança (CNCS) para capacitar organizações. Disponibiliza referências e ferramentas para cada medida de cibersegurança, detalhando três níveis de capacidade para que as organizações atinjam os cinco objetivos do quadro, considerando o seu contexto e tamanho.

Este classifica as medidas de segurança em três níveis de implementação: **Inicial**, **Intermédio** e **Avançado**, com práticas e evidências específicas para cada nível.

- **Inicial**: Medidas básicas de segurança, geralmente em iniciativas informais e *ad-hoc* para alcançar o objetivo de segurança.

- **Intermédio**: Medidas de segurança que abordam a maioria das situações e necessidades para atingir os objetivos de segurança da informação. Implementação formal das medidas.
- **Avançado**: Medidas avançadas de segurança envolvendo monitorização contínua, avaliações regulares e revisões considerando mudanças, incidentes, testes e exercícios para melhorias proativas.

Tem como objetivo que a organização progrida cumulativamente pelos níveis, começando pelo "Inicial" até alcançar o "Avançado", aplicando essas medidas de forma independente para cada objetivo de segurança.

Os níveis de capacidade variam conforme as características de cada organização, como tamanho e serviços oferecidos. Onde uma empresa pequena pode não necessitar de políticas de segurança complexas ou procedimentos formais para contratação de pessoal. As medidas de segurança são organizadas conforme a estrutura de objetivos do QNRCS e sua sofisticação é distribuída de acordo com a classificação apresentada.

### *2.7.4. CIS Controls*

O *Center for Internet Security, Inc*, designado por CIS [41], teve o seu inicio em agosto de 2000, quando um grupo de líderes empresariais e governamentais se reuniu em Washington, D.C. para discutir a preocupante onda de ciberataques. Daquele, e outros encontros, surgiu a visão de criar uma organização independente, sem fins lucrativos, com missão dedicada a prevenir e mitigar novas ameaças à cibersegurança.

Através de um esforço global e colaborativo, tem desenvolvido *standards* reconhecidos mundialmente nomeadamente os *CIS Controls* e *CIS Benchmarks*, juntamente com ferramentas tecnológicas especializadas para ajudar os profissionais de segurança a implementar e gerir as proteções de segurança.

Os *CIS Controls* [42] [43] representam um conjunto de práticas recomendadas para defesa cibernética, oferecendo estratégias específicas e aplicáveis para deter os ataques mais comuns. São uma lista concisa e prioritária de medidas defensivas altamente eficazes, servindo como ponto inicial essencial para todas as empresas interessadas em melhorar sua cibersegurança.

O desenvolvimento dos *CIS Controls* iniciou-se em 2008 por meio de um consórcio internacional que agregava diversas entidades, como empresas, agências governamentais e profissionais de diferentes áreas do ecossistema da cibersegurança. Esses especialistas voluntários aplicam a sua experiência para conceber as ações mais eficientes na proteção cibersegurança.

A atualização e revisão ocorrem por meio de um processo colaborativo informal. Especialistas do governo, da indústria e académicos, com conhecimentos técnicos

diversificados, unem-se para identificar os controlos de segurança mais eficazes, com base em diferentes pontos de vista, como vulnerabilidades, ameaças, tecnologias defensivas e gestão empresarial.

Um dos principais benefícios é a priorização, onde estes auxiliam as organizações na rápida definição de estratégias defensivas iniciais, direcionando recursos para ações de alto valor imediato. Isso permite focalizar atenção e recursos em questões de risco únicas para o negócio ou missão, otimizando a cibersegurança de acordo com as necessidades específicas de cada organização.

O foco principal é melhorar a capacidade da organização de prevenir e deter ataques antes que se tornem incidentes. Estes controlos não se concentram em fornecer diretrizes detalhadas para deteção, mitigação ou resposta a incidentes, mas sim em reduzir o número de incidentes ao impedir violações e explorações bem-sucedidas contra a organização. Assim, ao comparar os controlos disponibilizados pelo CIS com outros *frameworks*, estes oferecem uma base sobre a qual é possível construir os *frameworks* de segurança mencionados anteriormente, e fornece uma abordagem pró-ativa para minimizar incidentes de segurança.

***CIS Controls* v8**

Historicamente, os *CIS Controls* [7] eram ordenados em sequência para concentrar as atividades de cibersegurança de uma empresa, com um subconjunto dos seis primeiros *CIS Controls* referidos como "ciberhigiene". No entanto, isso mostrou-se excessivamente simplista. Como resultado, a partir da Versão 7.1, foram criados os *Implementation Groups* (IGs) dos *CIS Controls* como sendo a nova orientação recomendada para priorizar a implementação.

Os IGs dos *CIS Controls* são categorias autoavaliadas para empresas. Cada IG identifica um subconjunto dos *CIS Controls,* que a comunidade avaliou amplamente como aplicáveis para uma empresa com perfil de risco, e recursos semelhantes para se esforçar em implementar. Esses IGs representam uma visão horizontal dos *CIS Controls* adaptada para diferentes tipos de empresas.

Cada IG baseia-se no anterior: o IG2 incluí o IG1, e o IG3 incluí todas as *Safeguards* dos CIS do IG1 e IG2. Na Tabela 8, são apresentados os Grupos de Implementação do *CIS Controls* [30].

**Tabela 8 – Grupos de Implementação**

| | |
|---|---|
|  | **IG1** – possuí 56 *Safeguards*<br>Uma empresa do **IG1** é possuí uma dimensão pequena ou média, com conhecimento limitado em TI e cibersegurança para dedicar à proteção de ativos. A preocupação principal destas empresas é manter a operação do negócio, já que têm pouca tolerância a períodos de paragens. A sensibilidade dos dados que estão a ser protegidos é baixa e está principalmente relacionada com informação sobre os colaboradores e financeiras.<br><br>As salvaguardas selecionadas para o **IG1** devem ser implementáveis com conhecimento limitado em cibersegurança e visam conter ataques gerais e não direcionados. As salvaguardas são projetadas para funcionar em conjunto com *hardware* e *software* comerciais prontos para uso. |
|  | **IG2** (incluí IG1) – possuí 74 *Safeguards* adicionais<br>Uma empresa do **IG2** possuí pessoas responsáveis pela gestão e proteção da infraestrutura de IT. Essas empresas apoiam vários departamentos com diferentes perfis de risco, com base na função do trabalho e na missão. Unidades de pequenas empresas podem ter obrigações de conformidade regulatória. Empresas do **IG2** frequentemente armazenam e processam informações sensíveis de clientes ou da própria empresa e conseguem suportar interrupções curtas do serviço. Uma preocupação importante é a perda de confiança do público se ocorrer uma violação.<br><br>As salvaguardas selecionadas para o **IG2** ajudam as equipas de segurança a lidar com o aumento da complexidade operacional. Algumas salvaguardas dependerão de tecnologia de nível empresarial e conhecimentos especializados para instalação e configuração adequadas. |
|  | **IG3** (incluí **IG1** e **IG2**) - possuí 23 *Safeguards* adicionais<br>Uma empresa do **IG3** possuí especialistas em segurança, especializados em diferentes aspetos da cibersegurança como, gestão de riscos, teste de penetração, segurança de aplicações. Os ativos e dados do **IG3** contêm informações sensíveis ou funções sujeitas a supervisão regulatória e de conformidade. Uma empresa do **IG3** deve lidar com a disponibilidade de serviços e a confidencialidade e integridade de dados sensíveis. Ataques bem-sucedidos podem causar danos significativos ao bem-estar público.<br><br>As salvaguardas selecionadas para o **IG3** devem mitigar ataques direcionados de um adversário sofisticado e reduzir o impacto de ataques *zero-day*. |

Os *CIS Controls* consistem em 18 medidas abrangentes que ajudam a fortalecer a postura de cibersegurança. Estes priorizam as atividades, em detrimento das funções, e da propriedade do dispositivo. Desta forma, podem-se implementar os controlos de uma forma que funcione para cada situação. Na Tabela 9, são apresentados os 18 controlos críticos de segurança do *CIS Controls* [44].

**Tabela 9 – Lista dos 18 controlos críticos de segurança do *CIS Controls***

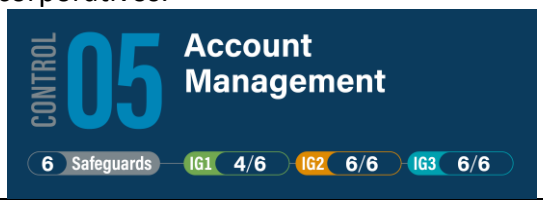
| |
|---|
| ***CIS Control* 1: Inventário e Controlo de Ativos da Empresa**<br><br>Gerir ativamente (inventariar, rastrear e corrigir) todos os ativos corporativos (dispositivos de utilizador final, incluindo dispositivos portáteis e móveis; dispositivos de rede; dispositivos não computacionais (IoT); e servidores) ligados à infraestrutura fisicamente, virtualmente, remotamente e assim como aqueles que se encontram em ambiente *cloud*, para conhecer com precisão a totalidade dos ativos que precisam ser monitorizados e protegidos dentro da empresa. Permite a identificação de ativos não autorizados e não geridos para remoção ou correção.<br>  |
| ***CIS Control* 2: Inventário e Controlo de Ativos de Software**<br><br>Gerir ativamente (inventariar, rastrear e corrigir) todo o *software* (sistemas operativos e aplicações) na rede para garantir que apenas *software* autorizado seja instalado e possa ser executado e permite identificar e impedir a instalação ou execução de *software* não autorizado e não gerido.<br>  |
| ***CIS Control* 3: Proteção de Dados**<br><br>Desenvolver processos e controlos técnicos para identificar, classificar, manusear de forma segura, reter e descartar dados.<br>  |

***CIS Control* 4: Configuração segura de ativos e *software* corporativos**

Estabelecer e manter a configuração segura dos ativos corporativos (dispositivos de utilizador final, incluindo dispositivos portáteis e móveis; dispositivos de rede; dispositivos não computacionais/IoT; e servidores) e do *software* (sistemas operativos e aplicações).


***CIS Control* 5: Gestão de Contas**

Utilizar processos e ferramentas para atribuir e gerir autorizações e credenciais para contas de utilizadores, incluindo contas de administrador, bem como contas de serviço, para ativos e *software* corporativos.




***CIS Control* 6: Gestão de Controlo de Acesso**

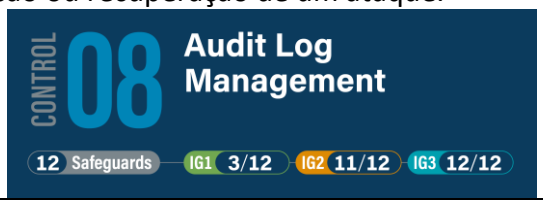
Utilizar processos e ferramentas para criar, atribuir, gerar e revogar credenciais e privilégios de acesso para contas de utilizador, administrador e serviço em ativos e *software* corporativos.


***CIS Control* 7: Gestão contínua de vulnerabilidades**

Elaborar um plano para avaliar continuamente e rastrear vulnerabilidades em todos os ativos corporativos dentro da infraestrutura da empresa, visando remediar e minimizar a janela de oportunidade para possíveis invasores. Monitorizar fontes públicas e privadas da indústria à procura de novas informações sobre ameaças e vulnerabilidades.

***CIS Control* 8: Gestão de *logs* de Auditoria**

Recolher, alertar, analisar e manter registos de Auditoria de eventos que possam ajudar na deteção, compreensão ou recuperação de um ataque.




***CIS Control* 9: Proteções de *e-mail* e *browser de Internet***

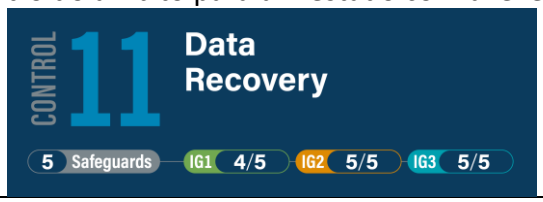
Melhorar as proteções e deteções de ameaças por meio de *e-mails* e na *web*, pois são oportunidades para os atacantes manipularem o comportamento humano por meio de interações diretas.


***CIS Control* 10: Proteção contra *malware***

Impedir ou controlar a instalação, disseminação e execução de aplicações, códigos ou *scripts* maliciosos em ativos corporativos.


***CIS Control* 11: Recuperação de Dados**

Estabelecer e manter práticas de recuperação de dados suficientes para restaurar os ativos corporativos dentro do âmbito para um estado confiável e pré-incidente.




***CIS Control* 12: Gestão de infraestrutura de rede**

Estabelecer, implementar e gerir ativamente (rastreio, relato, correção) dispositivos de rede, a fim de evitar que atacantes explorem serviços de rede e pontos de acesso vulneráveis.

***CIS Control* 13: Monitorização e Proteção de Redes**

Operar processos e ferramentas para estabelecer e manter monitorização de rede abrangente e defesa contra ameaças à segurança em toda a infraestrutura de rede da empresa.


***CIS Control* 14: Consciencialização de segurança e treinamento de competências**

Estabelecer e manter um programa de consciencialização de segurança para influenciar o comportamento dos utilizadores para que sejam conscientes da segurança e devidamente qualificados para reduzir os riscos de cibersegurança para a empresa.


***CIS Control* 15: Gestão de fornecedores de serviços**

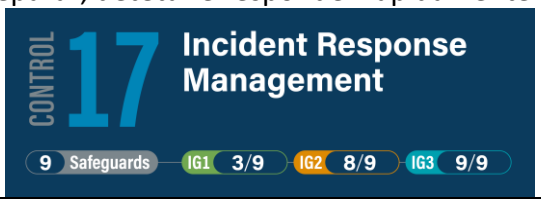
Desenvolver um processo para avaliar os fornecedores de serviço que detêm dados confidenciais ou são responsáveis por plataformas ou processos de TI críticos da empresa, para garantir que esses fornecedores estão a proteger essas plataformas e dados de forma adequada.


***CIS Control* 16: Segurança de Aplicações**

Gerir o ciclo de vida de segurança do *software* desenvolvido, alojado ou adquirido internamente para prevenir, detetar e corrigir pontos fracos de segurança antes que eles possam afetar a empresa.

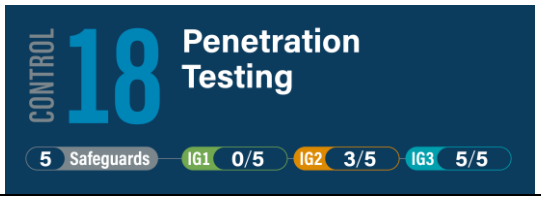
***CIS Control* 17: Gestão de Resposta a Incidentes**

Estabelecer um programa para desenvolver e manter a capacidade de resposta a incidentes (por exemplo, políticas, planos, procedimentos, funções definidas, treino e comunicações) para preparar, detetar e responder rapidamente a um ataque.




***CIS Control* 18: Teste de Penetração**

Testar a eficácia e a resiliência dos ativos empresariais identificando e explorando pontos fracos nos controlos (pessoas, processos e tecnologia) e simulando os objetivos e ações de um atacante.




O guia de implementação para pequenas e médias empresas do *CIS Controls* IG1 [45], foi criado para capacitar as PMEs, auxiliando-os na proteção de seus negócios através da utilização de um conjunto limitado, mas prioritário de ações. Este serve como um roteiro para ajudar as PMEs a adotarem rapidamente o Grupo de Implementação 1 (IG1). Após implementar as medidas sugeridas neste guia, é essencial que as PMEs identifiquem quais salvaguardas do IG1 ainda não foram concluídas, e assegurem que todas elas sejam implementadas na sua infraestrutura de IT. Este guia destina-se a ajudar as pequenas empresas a defenderem-se contra algumas das ameaças mais comuns, incluindo:

- Roubo de informações;
- Roubo de credenciais;
- Ataques de *phishing;*
- *Ransomware*;
- Desastres naturais;
- Desfiguração e tempo de inatividade.

Os documentos disponibilizados pelo *CIS Controls* estão disponíveis para serem utilizados por qualquer pessoa para melhorar a sua própria cibersegurança [43]. Contudo se forem utilizados para fins comerciais, deve ser adquirida uma subscrição do *CIS SecureSuite*, que fornecerá acesso a recursos adicionais.

***CIS SecureSuite* para Uso Académico** [46]

Esta opção oferece alguns benefícios adicionais adequados ao ambiente académico, onde as instituições académicas públicas dos EUA têm direito a uma adesão gratuita ao *CIS SecureSuite*. Entre os benefícios desta subscrição destaca-se:

- Acesso ilimitado às melhores práticas construídas por consenso para garantir a segurança dos seus sistemas e dados;
- Comparar a configuração dos seus sistemas-alvo com as recomendações nos *CIS Benchmarks*;
- Acompanhar a implementação dos *CIS Controls* com a nossa ferramenta de autoavaliação;
- Personalizar políticas de configuração para atender às necessidades únicas da sua organização;
- Distribuir ferramentas aos estudantes para ajudar a proteger seus sistemas de *laptop* e *desktop*.

Já as instituições académicas privadas dos EUA e internacionais têm direito a um desconto de 30%.

Esta *framework* servirá como base para a continuidade do trabalho, orientando a implementação das melhorias de cibersegurança nas PMEs. Para esse fim, serão utilizados e analisados os documentos disponibilizados em *websites* de acesso público. Contudo para o contexto deste trabalho, seria interessante ter acesso á informação fornecida no contexto de uma instituição de ensino pública dos EUA, onde os benefícios enunciados estão em linha com os objetivos deste trabalho.

## 2.8. Avaliação de Maturidade

Para o *National Cyber Security Centre* - UK [47], um modelo de maturidade é uma ferramenta para avaliar a eficácia de uma organização em alcançar um objetivo especifico. Os modelos permitem identificar onde as práticas são fracas, ou onde estão realmente enraizadas.

No contexto da cibersegurança, os modelos ajudam a distinguir organizações onde a segurança é intrínseca, daquelas onde é apenas uma adição superficial. Eles são úteis porque as grandes melhorias podem levar tempo, sendo que os modelos fornecem uma forma de medir o progresso na incorporação da segurança nas operações quotidianas e estratégicas.

Os modelos descrevem uma série de capacidades que se espera ver numa organização com uma abordagem eficaz em cibersegurança. Cada capacidade descreve atividades e processos esperados em diferentes níveis de maturidade. Uma organização pode comparar as suas práticas com esses níveis para avaliar sua própria maturidade. No entanto,

comparar a maturidade de uma organização com outras pode ser problemático, pois cada organização é única e fatores contextuais podem influenciar a maturidade de maneiras não facilmente mensuráveis.

### *2.8.1. Cybersecurity Capability Maturity Model*

O *Cybersecurity Capability Maturity Model* (C2M2) [8], pode ajudar organizações de vários setores, tipos e dimensão, a avaliar e a implementar melhorias nos seus objetivos de cibersegurança e fortalecer a sua resiliência operacional. Desde o lançamento da versão 1.0, em 2012, tanto a tecnologia como os agentes de ameaças, tornaram-se mais sofisticados, criando novos vetores de ataque e introdução de novos riscos.

O C2M2 versão 2.1, melhora o alinhamento com *standards* de cibersegurança reconhecidos internacionalmente e melhores práticas, incluindo publicação do NIST 800-53 e o NIST *Cybersecurity Framework* versão 1.1. [4].

O C2M2 foi elaborado para orientar o desenvolvimento de um programa de cibersegurança ou para ser utilizado com uma metodologia de autoavaliação, permitindo que uma organização meça e melhore o seu programa de cibersegurança. Existem dois instrumentos de autoavaliação disponíveis gratuitamente para qualquer organização, que incluem uma ferramenta baseada em PDF[9] e outra em HTML[10]. O conteúdo do modelo é apresentado em um nível elevado de abstração para que possa ser aplicado por organizações de vários tipos, estruturas, tamanhos e setores industriais. O uso amplo do modelo por um setor pode apoiar a comparação das capacidades de cibersegurança do setor

O modelo incluí 356 práticas que são agrupadas em 10 domínios, onde cada domínio é um agrupamento de práticas de cibersegurança. As práticas dentro de um domínio são agrupadas por objetivos - realizações alvo que apoiam o domínio, dentro de cada objetivo, as práticas são ordenadas por *Maturity Indicator Levels* (MILs).

As práticas representam as atividades que uma organização pode realizar para estabelecer e aperfeiçoar a capacidade no domínio. As práticas dentro de cada domínio são organizadas em objetivos, que representam realizações que apoiam o domínio.

Cada objetivo num domínio consiste num conjunto de práticas, que são organizadas de acordo com o nível de indicador de maturidade (MIL).

A Figura 13, representa a estrutura dos elementos de cada domínio que depois apresentam as práticas e indicadores de maturidade desse mesmo domínio.

[9] https://c2m2.doe.gov/evaluationToolkit
[10] https://c2m2.doe.gov/c2m2-assessment

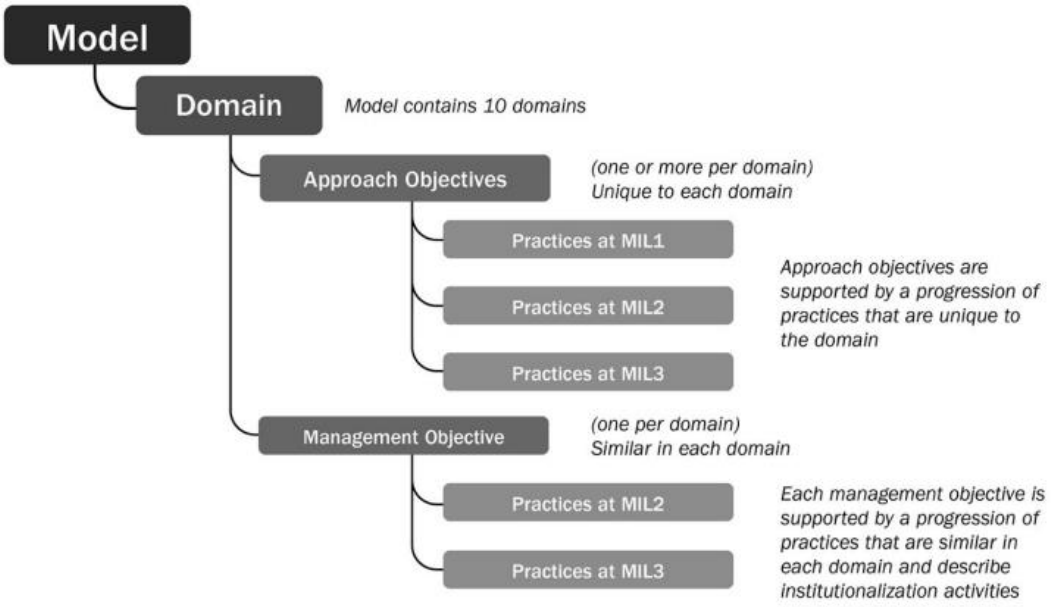



**Figura 13 - Resumo dos elementos de cada domínio [8]**

Para cada domínio, o modelo oferece um propósito, que é um resumo de alto nível da intenção do domínio, seguido por notas introdutórias que fornecem mais contexto e introduzem as práticas.

**Níveis de Indicadores de Maturidade**

O modelo define quatro níveis de indicadores de maturidade (MILs), MIL0 a MIL3, que se aplicam independentemente a cada domínio no modelo, definem uma dupla progressão de maturidade: uma progressão de abordagem e uma progressão de gestão.

- **MIL0**: As práticas não são executadas.
- **MIL1**: São executadas práticas iniciais, mas podem ser *ad hoc*.
- **MIL2**:
    - Características de Gestão:
        - As práticas são documentadas;
        - Os recursos adequados são alocados para apoiar o processo.
    - Característica de Abordagem:
        - Práticas são mais completas ou avançadas do que no MIL1.
- **MIL3**:
    - Características de Gestão:
        - As atividades são direcionadas por políticas (ou outras diretrizes organizacionais);
        - A responsabilidade, responsabilização e autoridade para executar as práticas estão atribuídas;
        - Pessoal que executa as práticas possui capacidades e conhecimentos adequados;

        - A eficácia das atividades é avaliada e monitorizada.
    - Característica de Abordagem:
        - As práticas são mais completas ou avançadas do que no MIL2.

Uma organização realiza uma autoavaliação em relação ao modelo, usa essa autoavaliação para identificar lacunas de capacidade, prioriza essas lacunas e desenvolve planos para abordá-las e, finalmente, implementa os planos para resolver as lacunas. À medida que os planos são implementados, os objetivos de negócio mudam e o ambiente de risco evolui, o processo é repetido, tal como representado na Figura 14.

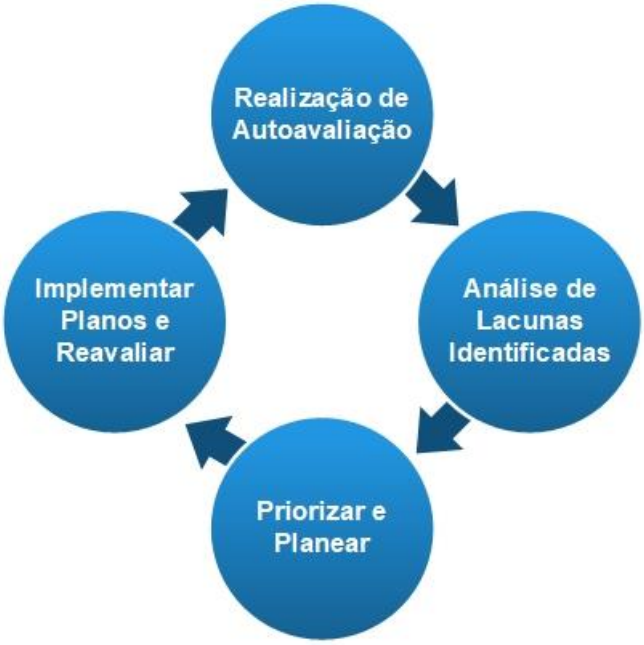



**Figura 14 - Abordagem potencial para utilizar o modelo**

- **Etapa 1:** Realização de Autoavaliação

Oferece a capacidade de medir a implementação das atividades de cibersegurança dentro de uma organização. Um dos objetivos de design do modelo é possibilitar que as organizações concluam uma autoavaliação para uma única função num dia, sem estudo extensivo ou preparação. No preenchimento da autoavaliação deve incluir pessoal operacional, partes interessadas, gestão e outros que possam fornecer informações úteis sobre o desempenho da organização nas práticas de cibersegurança.

Após a conclusão da autoavaliação, é gerado um relatório de pontuação que fornece um resumo do desempenho em relação ao modelo, bem como o status de implementação das práticas.

- **Etapa 2:** Analise de Lacunas Identificadas

O relatório de pontuação da autoavaliação identifica as lacunas no desempenho das práticas do modelo. O primeiro passo de análise para a organização é determinar se essas

lacunas são significativas e importantes para a organização resolver. A organização deve determinar o nível de desempenho das práticas e a conquista do MIL para cada domínio que melhor permita alcançar seus objetivos de negócio e estratégia de cibersegurança.

Para organizações que usam o modelo pela primeira vez, um perfil alvo geralmente é identificado após a autoavaliação inicial. Organizações com mais experiência no modelo geralmente já identificaram um perfil alvo antes de passar por uma autoavaliação.

- **Etapa 3:** Priorizar e Planear

Após a conclusão da análise das lacunas, a organização deve priorizar as ações necessárias para implementar completamente as práticas que permitem alcançar a capacidade desejada em domínios específicos. A priorização deve ser feita usando critérios, como o impacto das lacunas nos objetivos organizacionais, a importância do objetivo de negócio apoiado pelo domínio, o custo de implementar as práticas necessárias e a disponibilidade de recursos para implementá-las.

Deve ser desenvolvido um plano para abordar as lacunas selecionadas, podendo abranger um período de semanas, meses ou anos, dependendo da extensão das melhorias necessárias para fechar as lacunas selecionadas e alcançar a capacidade desejada. Devem ser realizadas revisões pela liderança para avaliar o estado, remover obstáculos e identificar correções necessárias conforme a implementação avança.

- **Etapa 4**: Implementar Planos e Reavaliar Periodicamente

Os planos desenvolvidos na etapa anterior devem ser implementados para lidar com as lacunas identificadas. As autoavaliações devem ser realizadas periodicamente para garantir que o progresso desejado seja alcançado. Também devem ser realizadas reavaliações quando existem mudanças significativas no ambiente de negócio, tecnologia, mercado ou ameaças, para garantir que o perfil atual corresponda ao estado desejado da organização.

A natureza adaptável do modelo, permitindo ajustes conforme os objetivos do negócio, fortalece a sua aplicabilidade como um instrumento dinâmico e alinhado com as necessidades do cenário de segurança da informação

### *2.8.2. Capability Maturity Model Integration*

A *Information Systems Audit and Control Association* (ISACA) [9], é uma organização sem fins lucrativos dedicada ao avanço da confiança digital, reconhecida no campo de Sistemas de Informação/Tecnologia da Informação há mais de cinco décadas. O seu principal compromisso reside na capacitação de profissionais para ampliar as suas competências em áreas como: Auditoria, cibersegurança e tecnologias emergentes. Ao ser membro, é disponibilizado o acesso a recursos educacionais e há a possibilidade de obter certificações reconhecidas internacionalmente.

O *Capability Maturity Model Integration* (CMMI) [48] foi criado para o Departamento de Defesa dos EUA para avaliar a qualidade e a capacidade de seus fornecedores de *software*. O modelo expandiu-se além da engenharia de *software* para ajudar qualquer organização em qualquer setor a construir, melhorar e medir as suas capacidades e desempenho. A avaliação ajuda a identificar pontos fortes e oportunidades de melhoria dos processos de uma organização e compara se os processos estão alinhados com as melhores práticas do CMMI. Os modelos CMMI podem ajudar qualquer setor a criar, melhorar e medir recursos e desempenho.

No contexto da segurança da informação, o CMMI ajuda a alinhar os controlos com as necessidades do negócio, identificar e corrigir lacunas e fragilidades, e demonstrar conformidade e valor para as partes interessadas. A CMMI *CyberMaturity* harmoniza e ajuda a identificar lacunas na implementação de *frameworks* líderes como:

- *National Institute of Standards and Technology Cybersecurity* Framework (NIST CSF, 800-171);
- ISO/IEC (27001, 27002);
- *Threat Kill Cycle*;
- *Federal Financial Institutions Examination Council* (FFIEC);
- CMMC.

Com a utilização do modelo CMMI [49], as organizações obtêm melhores resultados quando direcionam os esforços de melhoria dos seus processos para um número limitado de áreas simultaneamente. Os objetivos de melhoria, devem sempre derivar das necessidades do negócio, desta forma as organizações colhem benefícios quando o foco da melhoria está nos resultados e desempenho empresarial, tornando-se assim mais duradouros.

Existem 4 níveis de capacidade, que se referem-se aos êxitos no desempenho e melhoramento dos processos em áreas de prática específicas da organização. As práticas são agrupadas de Nível 0 a Nível 3, delineando um progresso evolutivo. Cada nível baseia-se no anterior, introduzindo novas funcionalidades ou critérios mais rigorosos, resultando em uma capacidade melhorada.

- Nível de capacidade 0: Incompleto;
- Nível de capacidade 1: Inicial;
- Nível de capacidade 2: Gerido;
- Nível de capacidade 3: Definido.

Os 6 níveis de maturidade delineiam uma trajetória progressiva para as iniciativas de melhoramento de desempenho e processos da organização. Em cada nível, o conjunto predefinido de áreas de prática também serve como uma rota para melhorar o desempenho.

- Nível de Maturidade 0: Incompleto;
- Nível de Maturidade 1: Inicial;
- Nível de Maturidade 2: Gerido;
- Nível de Maturidade 3: Definido;
- Nível de Maturidade 4: Gerido Quantitativamente;
- Nível de Maturidade 5: Otimizado.

Os riscos de cibersegurança mais relevantes para uma organização não são os mesmos para outra. Com a utilização da plataforma CMMI *CyberMaturity* permite perceber onde deve estar foco para mitigar as ameaças à cibersegurança. O questionário de avaliação de riscos facilita a identificação de ameaças à cibersegurança de forma simples e direta. Permite a definição de parâmetros como, a probabilidade, e o impacto que cada evento de risco terá na organização no caso de ocorrência de eventos de risco específicos relacionados a várias vulnerabilidades potenciais.

No final, a plataforma apresenta um relatório de lacunas com o resultado da autoavaliação para mostrar quantas práticas não estão de acordo com o modelo, para cada área de capacidade, começando com as áreas de maior risco, conforme determinado pelo seu perfil de risco.

O acesso aos recursos da plataforma CMMI *CyberMaturity* é condicionado e apresenta custos elevados, onde neste contexto, não é passível de ser realizada uma avaliação prática da informação disponibilizada na documentação

### 2.8.3. Selo de Maturidade Digital em Cibersegurança

O Selo de Maturidade Digital (SMD) [50] faz parte do Plano de Ação para a Transição Digital, visando impulsionar a transformação digital na economia. Empresas que seguem normas e diretrizes alinhadas com as melhores práticas e requisitos europeus podem obter certificações de maturidade em quatro áreas: Sustentabilidade, Cibersegurança, Privacidade e Proteção de Dados Pessoais, e Acessibilidade. O SMD amplia a gama de certificações existentes, oferecendo mais possibilidades para que as PME se certifiquem e progridam na digitalização.

O SMD em Cibersegurança [51] representa o compromisso das organizações em seguir um guia durante o processo de transição digital, especialmente em um mundo cada vez mais dependente das tecnologias de informação e comunicação (TIC). Para alcançar essa certificação, as organizações devem aderir aos requisitos definidos para esta área, classificados em níveis de maturidade: Bronze, Prata ou Ouro. O processo de certificação é conduzido por entidades certificadoras devidamente credenciadas pelo Instituto Português de Acreditação (IPAC).

O SMD em Cibersegurança [52] procura reduzir os diversos riscos que as organizações enfrentam em termos de cibersegurança, oferecendo assim maior prevenção e proteção

para as informações. Para conquistar essa certificação, as organizações precisam aderir aos requisitos estabelecidos na norma DNP TS 4577-1:2021 [10], implementando-os em todos os setores e processos que envolvem o uso de Tecnologias da Informação e Comunicação (TIC). Esses requisitos foram escolhidos a partir de referências nacionais, como o Quadro Nacional de Referência para a Cibersegurança (QNRCS), o Roteiro para as Capacidades Mínimas de Cibersegurança e o Quadro de Avaliação de Capacidades de Cibersegurança.

A certificação em Cibersegurança é aberta a todas as organizações, independentemente seu ramo de atuação, tipo ou tamanho, com ênfase especial nas PMEs que desejam evidenciar sua conformidade na área da Cibersegurança.

Essa certificação está dividida em três níveis, representados na Tabela 10, nos quais os requisitos se tornam progressivamente mais complexos e a metodologia de verificação durante a Auditoria se torna mais detalhada. Assim, à medida que se avança nos níveis de certificação, a exigência e o rigor dos critérios aumentam.

**Tabela 10 – Níveis do Selo Digital de Cibersegurança [52]**

| | |
|---|---|
|  | **Bronze** - Práticas fáceis de implementar que reforçam a segurança da organização contra os riscos de cibersegurança mais frequentes e prejudiciais. São especialmente úteis para empresas de menor dimensão, com menos experiência ou recursos limitados de pessoas e tecnologia para lidar com esses riscos, ou mesmo para organizações que têm uma menor necessidade de cibersegurança. |
|  | **Prata** - Práticas de nível intermédio que requerem o cumprimento de conformidade tanto nos requisitos deste nível quanto do nível anterior (bronze). Destinadas a organizações que possuem competências de cibersegurança acima do básico, têm uma média dimensão ou enfrentam maiores necessidades de cibersegurança devido à sua dependência mais significativa desta área para o sucesso das suas operações. |
|  | **Ouro** - Destinado a organizações mais qualificadas em cibersegurança, com recursos técnicos e humanos robustos, que têm uma necessidade crucial de proteger as redes e dados. É obrigatório demonstrar conformidade não apenas com os requisitos deste nível, mas também dos níveis anteriores (bronze e prata). Essa certificação também se aplica a empresas para as quais a cibersegurança é vital nas suas operações críticas ou onde um incidente nessa área pode ameaçar a própria existência da organização. |

A DNP TS 4577-1:2021 - Maturidade digital – Selo Digital - Parte 1: Cibersegurança - Requisitos não é disponibilizada gratuitamente, sendo um documento normativo oficial precisa ser adquirido ao IPQ [11].

[11] https://www.ipq.pt/loja/normas/

O SMD em Cibersegurança, mede a maturidade digital e refere-se à capacidade de uma organização utilizar eficazmente a tecnologia digital para atingir seus objetivos estratégicos e operacionais. A abordagem divide-se em três áreas principais: Organizacional, Técnica e Humana.

**Organizacional:** Esta área envolve a criação e implementação de políticas, procedimentos e diretrizes que regem a cibersegurança dentro da organização. Isso incluí políticas de acesso à informação, protocolos de resposta a incidentes, políticas de uso aceitável de recursos digitais, entre outros. Aqui, a organização avalia e gere os riscos relacionados com a cibersegurança, que a identificação de ameaças, avaliação de vulnerabilidades e implementação de medidas para mitigar riscos.

**Técnica:** Envolve a implementação de tecnologias específicas para proteger os ativos digitais da organização, como *firewalls*, sistemas de deteção e prevenção de intrusões, antivírus. Pretende garantir que apenas os utilizadores autorizados tenham acesso aos recursos digitais da organização. Isso incluí sistemas de autenticação forte, gestão de identidades e políticas de acesso. Proteger dados sensíveis através de cifragem é uma medida técnica importante para garantir a confidencialidade e integridade da informação.

**Humana:** A componente humana é frequentemente considerada o elo mais fraco na cibersegurança. Treinar os utilizadores para reconhecer ameaças, adotar boas práticas de segurança e estar cientes dos riscos é crucial. Promover uma cultura organizacional que valorize a cibersegurança é essencial.

A Tabela 11, apresenta um resumo das medidas por cada nível da certificação [42].

**Tabela 11 – Requisitos das medidas de cibersegurança dos SMD em Cibersegurança**

| **Bronze** | |
|---|---|
| **Organizacional** | O.ID – Identificação de funções ou atividades críticas e dependência das TIC.<br>O.IAC – Inventariação dos ativos (*hardware e software*) e documentação da arquitetura de comunicação de dados, assim como a atualização regular.<br>O.PUA – Política(s) de utilização aceitável dos recursos TIC, orientação para a boa utilização dos recursos TIC.<br>O.RSI – Identificação de responsável pela segurança da Informação, com um conhecimento aprofundado negócio e técnico. |

| | |
|---|---|
| **Técnica** | T.CS – Cópias de segurança através de uma plataforma realizadas de forma automática e regular.<br>T.AS – Atualizações de segurança automáticas dos sistemas operativos e aplicações.<br>T.PPT – Proteção de postos de trabalho contra vírus e código malicioso.<br>T.PPI – Proteção perimetral (firewall), segmentação de rede, desativação de passwords por defeito. Segurança física dos principais componentes.<br>T.CWC – Conformidade *Webcheck* - Ligação HTTPS; Certificado SSL e SPF.<br>T.AM – Autenticação multifator, nas aplicações críticas e quando disponível. |
| **Humana** | H.PF – Plano de Formação em segurança da informação e cibersegurança. Validar a sai correta implementação.<br>H.FIC – Fontes de informação e canais de comunicação, obtenção de informação fidedigna para acompanhar novas ameaças. |
| **Prata** | |
| **Organizacional** | O.PP – Política de palavras-passe.<br>O.PAP – Política de acessos e permissões, menor privilégio.<br>O.GMO – Gestão da mudança organizacional, na entrada, saída e troca de funções de colaboradores.<br>O.PRI – Plano de reação a incidentes de Cibersegurança. |
| **Técnica** | T.CWC – Conformidade *Webcheck* – HSTS, Cabeçalhos de Segurança e DKIM.<br>T.GP – Solução de gestão de palavra-passe associadas á gestão da infraestrutura.<br>T.PAD – Privilégios de acesso diferenciados, menor privilégio.<br>T.SC – Securização (*hardening*) de configurações (TPM e proteção BIOS), sistema operativo e aplicações.<br>T.CA – Controlo Aplicacional, de *software* não autorizado.<br>T.RAR – Recolha de armazenamento de registos, dos sistemas operativos e aplicações, no mínimo de 1 ano e capacidade de armazenamento local de 1 mês. |
| **Humana** | H-PF – Plano de formação para os perfis técnicos. |
| **Ouro** | |
| **Organizacional** | O.AGR – Análise e gestão do risco (nível de risco) – identificar vulnerabilidade; calcular probabilidade e avaliar criticidade de cada ativo.<br>O.SOC – Centro de Operações de Segurança – prevenir; detetar; avaliar e responder a ameaças e incidentes de cibersegurança.<br>O.PCN – Plano de continuidade de negócio – contendo informações para a organização continuar em caso de incidente. |

| | |
|---|---|
| **Técnica** | T.CS – Cópias de segurança – níveis adicionais de proteção alinhado com o Plano de Continuidade de Negócio.<br>T.PPT – Proteção de postos de trabalho – Gestão centralizada da proteção de vírus e código malicioso.<br>T.CWC – Conformidade *Webcheck* – DNSSEC, TLS, DMARC, STARTTLS.<br>T.RSC – Redundância de sistemas críticos.<br>T.CEC – Cifragem dos discos equipamentos corporativos.<br>T.TSA – Testes de segurança e de aceitação de serviços – realizados por equipas ofensivas – avaliar o comportamento perante situações de ataque.<br>T.TRI – Testes de resposta a incidentes de segurança – duas vezes por ano. |
| **Humana** | H.EC – Realização de exercícios de avaliação de Cibersegurança – aos utilizadores, por exemplo através de uma simulação de *phishing.* |

Para o cumprimento dos controlos é necessário a recolha de evidências e a documentação dos processos implementados, que ajudam a demonstrar não apenas o cumprimento do controlo específico da norma, mas também a abordagem abrangente e contínua da organização em relação à segurança, mostrando como os controlos são implementados, monitorizados e mantidos ao longo do tempo.

O SMD em Cibersegurança, representa um reconhecimento formal do nível de preparação e cibersegurança da organização, apresentando requisitos concretos para o seu cumprimento em alinhamento com a estratégia do CNCS. A certificação não apenas reflete um estado atual de segurança, mas também demonstra uma postura proativa na identificação e mitigação de ameaças à cibersegurança, o que é crucial num mundo digital cada vez mais complexo e vulnerável.

Assim como em qualquer certificação, as empresas certificadas têm uma vantagem competitiva ao demonstrar aos clientes, parceiros e investidores o compromisso com a segurança dos dados e sistemas. Permitindo evidenciar a sua capacidade de resistir e se recuperar de ciberataques, minimizando danos operacionais e financeiros.

Com a crescente preocupação com a proteção de dados pessoais e sensíveis, o selo de maturidade em cibersegurança é uma forma de mostrar que as organizações estão empenhadas em proteger essas informações.

A obtenção do SMD em Cibersegurança exige a implementação de boas práticas e políticas de segurança, contribuindo para elevar o nível de consciência sobre a importância da cibersegurança em Portugal.

Neste trabalho, e face ao contexto atual em que existem inúmeras recomendações e *frameworks* de segurança que podem ser adotadas por uma PME, optou-se por utilizar as medidas de segurança descritas no Selo de Maturidade Digital em Cibersegurança como o

principal guia de avaliação. Estas oferecem uma abordagem prática e direta que possibilita às PMEs em Portugal elevar o nível de segurança dos dados e sistemas. Com esta escolha é pretendido uma adoção de uma abordagem eficaz e prática para garantir a segurança das organizações e ficarem preparadas para se submeter a um processo de validação por uma entidade certificadora.

# 3. Revisão de Literatura

A cibersegurança tornou-se uma preocupação crescente para organizações de todos os tamanhos, mas as PMEs enfrentam desafios únicos. Nesse contexto Galvin [53], refere-se a um estudo realizado junto de 1.377 CEOs de PMEs, que indicam que 62% das empresas pesquisadas não possuem uma estratégia de cibersegurança atualizada ou ativa. Onde a falta de uma proteção adequada torna essas empresas alvos fáceis para os criminosos, que podem explorar vulnerabilidades com relativa facilidade. Refere ainda, que para as empresas que se encontram dentro desta estatística, está na altura de fazer uma mudança e seguir as quatro etapas definidas para começar a construir uma estratégia:

- Avaliar o estado atual da cibersegurança da empresa, identificando deficiências e pontos fracos;
- Designar uma pessoa responsável pela cibersegurança e envolver os líderes de diferentes áreas da organização;
- Avaliar e priorizar os ativos da empresa, reconhecendo os mais críticos e valiosos;
- Decidir entre uma gestão interna ou externalizar certos aspetos da cibersegurança, considerando a possibilidade de usar serviços de terceiros ou contratar consultores especializados.

Alahmari e Ducan [54], apresentam um trabalho de revisão de 15 artigos, onde através de vários métodos de análise, descrevem a importância da gestão de riscos de cibersegurança para PMEs, onde destacam que embora essas empresas recorram a novas tecnologias, muitas das vezes subestimam as ameaças de cibersegurança. Essa subestimação pode aumentar as vulnerabilidades e os riscos das PMEs, tornando-se desafios reais para elas e outras entidades relacionadas. Os autores procuram entender o papel da gestão das PMEs na abordagem dos riscos de cibersegurança nos últimos anos. A subestimação dos riscos pode levar a consequências desastrosas, afetando tanto os ativos tangíveis quanto os intangíveis, podendo até levar à falência do negócio.

Este fornece uma visão geral da gestão de riscos de cibersegurança nas PMEs dos estudos existentes e as possíveis indicações para trabalhos futuros, onde são apresentadas 5 perspetivas:

- **Ameaças de Cibersegurança:** As PMEs enfrentam ameaças como violações e negação de acesso a dados, muitas vezes subestimando os riscos devido ao seu tamanho.
- **Comportamentos de Cibersegurança:** O comportamento dos funcionários é crucial, pois a ignorância das políticas de informação e diretrizes organizacionais pode levar a ameaças de cibersegurança.
- **Práticas de Cibersegurança:** As práticas atuais de cibersegurança são muitas vezes inadequadas, com pouca participação na comunidade de pesquisa de

cibersegurança e práticas de externalização como a *cloud* sendo vistas como soluções, mas não substitutos para boas práticas.

- **Consciencialização de Cibersegurança:** A falta de consciencialização sobre cibersegurança pode aumentar os riscos, destacando a necessidade de programas de consciencialização eficazes e uma compreensão mais profunda das vulnerabilidades específicas.
- **Tomada de Decisões de Cibersegurança**: Os acionistas e gestores desempenham um papel crucial na tomada de decisões em relação à segurança da informação, sendo fundamental envolver especialistas no processo de tomada de decisões para melhorar a consciencialização e as práticas de segurança.

Autores como Pérez et al. [55], Jain et al. [56], Sukumar et al. [57] e Ouma [58], apresentam outros trabalhos sobre a Gestão de Risco e as ameaças, focados na importância crescente da gestão de riscos e nas ciberameaças enfrentadas pelas empresas. Os autores, discutem a vulnerabilidade das empresas, especialmente as PMEs, perante as ameaças em constante evolução. Propõem diferentes *frameworks* e soluções para avaliar e mitigar os riscos, incluindo o uso de tecnologias de virtualização e automação para identificar e mitigar ameaças.

Comum aos trabalhos na área da cibersegurança, há a necessidade da existência de uma estratégia para cada organização para lidar com as ameaças. Assim, Shojaifar e Järvinen [59], propõem uma *framework* de classificação para abordar a competência e consciencialização em cibersegurança das PMEs, reconhecendo que essas empresas são heterogêneas nas suas necessidades e capacidades de cibersegurança. A *framework* identifica cinco tipos de PMEs com base em suas características e necessidades específicas de segurança:

- **PME abandonada em cibersegurança** - Não possuem política ou orientação de cibersegurança, nem competência em segurança. Não alocam recursos para cibersegurança, não têm perceção clara de ameaças e não veem a necessidade de medidas de segurança. Precisam de motivação externa, acesso a conhecimentos básicos de segurança e ligação com especialistas confiáveis.
- **PME sem capacidade em cibersegurança** - Possuem uma política parcial de cibersegurança, são conscientes de algumas ameaças, mas não têm uma visão holística. Faltam capacidades em cibersegurança e ligação a especialistas para desenvolver competências. Estão dispostas a cumprir políticas de segurança e podem melhorar suas capacidades com acesso a formação e especialistas em segurança.
- **PME conectada a especialistas em cibersegurança** - Possuem política parcial de cibersegurança e dependem de terceiros para gerir as medidas de segurança. Conscientes da importância da cibersegurança, têm acesso a conhecimento e capacidades, mas os utilização carecem de capacidade adequada.

- **PME capaz em cibersegurança** - Possuem cultura de cibersegurança e política de segurança alinhada, com competências de TI e cibersegurança. Precisam de acesso a tecnologias atualizadas e notícias de cibersegurança para manter-se informadas sobre incidentes e ameaças.
- **PME provedora de serviços em cibersegurança** - Oferecem soluções de segurança para outras empresas, possuindo cultura e política de segurança. Mantêm uma atitude proativa, revendo regularmente as suas políticas e formando os utilizadores.

Ozkan e Spruti [60], apresentam-nos fundamentos da padronização da cibersegurança para PMEs europeias, visando superar os desafios de iniciar a padronização da cibersegurança. Definem os principais conceitos no domínio da cibersegurança e propõem um processo de cinco etapas para estabelecer e melhorar a cibersegurança usando *standards* e estruturas. As medidas de segurança presentes nesses *standards* e estruturas são comparadas e unificadas em 17 categorias de controlo para fornecer às PMEs um ponto de referência rápido. São apresentadas quatro categorias diferentes de PMEs (*Digital Enabler, Digitally Based, Digitally Dependent, Start-ups*), fornece orientações personalizadas para a implementação dos controlos, integrando os principais conceitos, processos e controlos de segurança derivados de *standards* e estruturas reconhecidos internacionalmente.

Os processos das cinco etapas derivam da cláusula de Planeamento da norma ISO/IEC 27001 [5], descrevem-se as etapas do processo:

- **Compreender o Perfil da Empresa -** avaliar o perfil da empresa para entender os seus fatores internos e externos que podem afetar a cibersegurança.
- **Realizar uma Avaliação de Risco de Segurança –** identificar as ameaças, vulnerabilidades e riscos associados e avaliar a sua probabilidade e impacto.
- **Identificar Controlos de Segurança Aplicáveis -** selecionar os controlos de segurança adequados para mitigar os riscos identificados, com base na categoria da PME no ecossistema digital.
- **Aplicar os Controlos de Segurança** - definir um plano de implementação para os controlos selecionados e implementá-los na empresa.
- **Monitorizar e Melhorar** - avaliar continuamente a eficácia dos controlos implementados, revendo periodicamente os riscos e controlos, fazendo melhorias conforme necessário.

Benz e Chatterjee [61], propõem uma ferramenta de avaliação da cibersegurança, denominada de *Cybersecurity Evaluation Tool* para PMEs que baseada numa avaliação *on-line* de 35 perguntas a ser respondida pelos responsáveis do TI para autoavaliar a sua maturidade dentro das cinco categorias da estrutura NIST [32]: identificar, proteger, detetar, responder e recuperar. Foi desenvolvido com base no *NIST Cybersecurity Framework* Versão 1.1 (CSF) [4], onde foram selecionadas 35 dos 96 *standards* mais relevantes para empresas típicas de PMEs, visando simplificar a avaliação de riscos.

O processo de desenvolvimento envolveu a realização de uma pesquisa online com 50 responsáveis de TI de PMEs para avaliar a maturidade da empresa em relação a cada um dos 35 *standards*. Um mecanismo de avaliação foi então usado para calcular a pontuação média de maturidade para cada padrão e identificar lacunas significativas.

A ferramenta proposta no trabalho destes autores, apresenta um relatório e agrupa as questões em categorias do NIST CSF, apresentando a pontuação média do respondente, a pontuação média da indústria e a pontuação de melhores práticas. São fornecidas recomendações práticas com estimativas de custo e esforço.

Franco et al. [62], Azinheira et al. [63] e Pawar et al. [64], focam-se também na utilização de *frameworks* e soluções específicas para os desafios de cibersegurança enfrentados pelas PMEs. Eles destacam a necessidade de abordagens adaptadas às capacidades e necessidades das pequenas empresas, incluindo o desenvolvimento de soluções práticas e acessíveis que levem em consideração a falta de recursos e conhecimentos técnicos das PMEs, na área da Cibersegurança.

Sasidharan [65], apresenta uma abordagem para implementar a otimização do sistema Windows usando os *CIS Controls* [7], o foco está na aplicação dos controlos para fortalecer os sistemas Windows, utilizando ferramentas de segurança, um kit de remediação e *frameworks* padrão. A implementação bem-sucedida desses controlos proporciona conforto às equipas de IT, segurança na avaliação e manutenção da *baseline* de segurança da infraestrutura de IT. O estudo aborda os desafios enfrentados pelas organizações na implementação de políticas de fortalecimento de infraestruturas de produção complexas, destacando a importância de testes adequados e aprovação dos principais interessados.

O uso do *CIS Controls* oferece uma abordagem escalável e centralizada para gerir e monitorizar a segurança dos sistemas Windows, permitindo fácil ajuste e aplicação de políticas. Neste trabalho, são apresentados detalhes sobre os componentes do *CIS Controls*, incluindo os *Build Kits CIS Benchmarks* [66], e ferramentas de avaliação. A implementação bem-sucedida dos *CIS Controls* não apenas fortalece a segurança da infraestrutura de TI, mas também simplifica os processos de auditoria e conformidade. Este caso de estudo fornece informações para organizações que pretendem melhorar a segurança de seus sistemas Windows, destacando os benefícios e as etapas práticas para implementar os *CIS Controls* de forma eficaz e abrangente.

Chidukwani et al. [67], analisam a cibersegurança das PMEs, destacando a sua importância económica e a vulnerabilidade dessas empresas a ciberataques devido à implementação inadequada de medidas de segurança. Conclui que a pesquisa nesse campo é predominantemente qualitativa e focada principalmente nas funções de Identificar e Proteger do *NIST* CSF V1.1 [4], com pouca atenção para as outras funções. Há uma concentração significativa em estratégias e políticas de segurança, mas pouca atenção é dada à implementação prática, deteção, resposta e recuperação. Além disso, é necessário

direcionar mais esforços para a resiliência cibernética, garantindo uma abordagem equilibrada entre prevenção, resposta e recuperação de ciberataques, especialmente considerando o alto índice de ataques às PMEs.

Avaliação e Maturidade da Cibersegurança é também aborda por autores como Razaket al. [68], Hasani et al. [69], AL-Dosari e Fetais [70], Wake et al. [71], Groš [72], Marica et al. [73], Vasudevan [74] e Pawar e Palivela [75], onde exploram os desafios enfrentados pelas *startups* de tecnológicas e PMEs na avaliação de sua maturidade em cibersegurança. Eles utilizam *frameworks* existentes e propõem soluções para avaliar a maturidade em cibersegurança e quantificar o retorno sobre os investimentos em cibersegurança.

Os trabalhos apresentados para esta análise abordam temas relacionados com a maturidade das organizações, com ênfase na compreensão do estado atual das empresas na área da cibersegurança. Alguns destes estudos recorrem a inquéritos para avaliar as capacidades existentes nas empresas e determinar o seu nível de maturidade em cibersegurança. Noutros, são desenvolvidos modelos com o foco em proteger as PMEs contra as ameaças, onde estas, enfrentem desafios como os recursos limitados e falta de competências técnicos, sendo igualmente vulneráveis a ciberataques. Concluindo-se que é crucial desenvolver abordagens adaptadas às necessidades específicas das PMEs para avaliar e melhorar sua maturidade.

Estes trabalhos destacam ainda a importância de desenvolver modelos robustos e testá-los em casos reais para entender melhor como as organizações podem melhorar a sua postura de cibersegurança. Enfatizam a necessidade de abordagens inovadoras e ferramentas adequadas para avaliar e melhorar a cibersegurança das PMEs, reconhecendo a sua importância na economia e as suas vulnerabilidades.

# 4. Metodologia

Com o estudo prévio apresentado nos capítulos iniciais, identifica-se a necessidade de as empresas aplicarem uma estratégia de cibersegurança. Em Portugal dentro do universo das empresas destacam-se as PMEs, pois são em maior número, possuem mais trabalhadores e fazem parte de cadeias de abastecimento que podem colocar em causa outras empresas maiores.

Este capítulo detalha a metodologia utilizada no desenvolvimento de uma estratégia de cibersegurança que pode ser aplicada às PMEs. Na Figura 15, são apresentadas as 4 fases da metodologia utilizada neste trabalho. Pretende-se assim apresentar de forma abrangente as fases e decisões que constituem este trabalho, desde a conceção inicial até a implementação prática. Descreve-se assim o processo pelo qual o questionário foi desenvolvido, incluindo a definição dos critérios de avaliação, a seleção das perguntas e controlos relevantes, até à elaboração de medidas de mitigação dos principais riscos identificadas (áreas de melhoria).

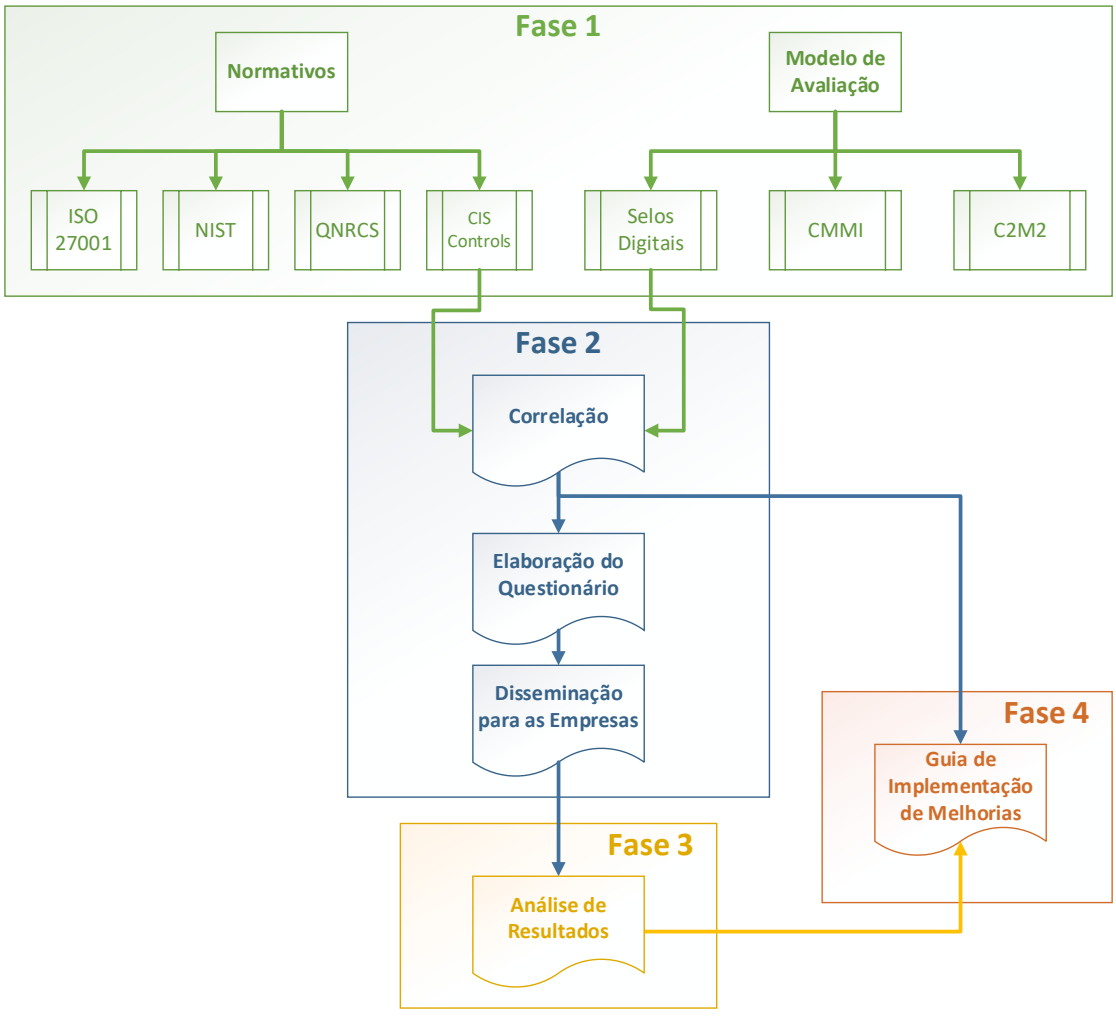



**Figura 15 – Diagrama da metodologia implementada**

## 4.1. Estudo de Normativos e Modelos de Avaliação

Na Secção 2.7, é descrita a realização do estudo efetuado sobre algumas *frameworks* de cibersegurança, como: o *NIST Cybersecurity Framework* [4], ISO/IEC 27001 [5], o Quadro Nacional de Referência para Segurança Cibersegurança [6] e o *CIS Controls* [7]. Através da realização deste estudo, foi possível obter uma melhor compreensão e efetuar um levantamento mais abrangente das melhores práticas e diretrizes disponíveis para proteger os sistemas de informação e dados das organizações contra ameaças. Esta análise serviu como base para a seleção do normativo a ser considerado ao longo do estudo, e para a definição de orientações a serem seguidas. Tendo sendo sido escolhido o *CIS Controls*, que nos apresenta um conjunto de melhores práticas de cibersegurança desenvolvidas pelo *Center for Internet Security* (CIS), onde são definidos controlos de segurança prioritários que fornecem uma abordagem prática e exequível para melhorar a postura de cibersegurança das empresas.

Já na Secção 2.8, foram examinados alguns modelos de avaliação de maturidade, como C2MC [8], CMMI [49] e o SMD em Cibersegurança [10]. A estratégia foi entender que requisitos podem ser utilizados para uma avaliação da postura de cibersegurança das organizações. Ao utilizar um modelo de avaliação *standard*, permite ter um plano para identificar lacunas e áreas de melhoria nas práticas das organizações participantes e orientar quais as recomendações de melhoria. Após esta análise foi escolhido o SMD em Cibersegurança, nos níveis bronze e prata, pois este oferece um conjunto de critérios e requisitos que as empresas devem seguir com a vantagem que ficam mais preparadas para obter a obtenção de uma certificação de uma Norma Portuguesa. Fornece assim uma referência clara para avaliar e melhorar a cibersegurança.

## 4.2. Correlação SMD em Cibersegurança e *CIS Controls*

Nesta fase, a estratégia passou pela identificação de correspondências entre as medidas de cibersegurança dos níveis Bronze e Prata, especificados no SMD em Cibersegurança, e as funções de segurança definidos pelo *CIS Controls*, que poderiam apoiar a sua validação. Esta correlação foi realizada com base em três elementos heurísticos definidos por Azinheira et al. [63]: Ação, Âmbito e Alvo.

- **Ação** (AC): Os critérios incluem uma similaridade das ações em termos do objetivo de segurança, áreas de foco, requisitos técnicos e práticas recomendadas;
- **Alvo** (AL): Existe um contexto de aplicação semelhante entre o requisito do SMD e a função de segurança do *CIS Controls*, embora não tenha exatamente a mesma ação;
- **Âmbito** (AM): O SMD, possuí um requisito que não vem descrito nos controlos de segurança, mas existe um documento auxiliar que dá resposta ao âmbito.

Cada medida ou requisito definido pelo SMD em Cibersegurança pode estar associado a uma, ou várias funções de segurança do *CIS Controls*, onde ao implementar essas medidas, as organizações visam garantir que todas as funções de segurança relevantes sejam abordadas de maneira eficaz, fortalecendo assim sua postura de cibersegurança como um todo.

Existe uma função de segurança do *CIS Controls* que dá resposta a dois requisitos do SMD, um no nível bronze e outro no nível prata pois esta medida em concreto vai sendo incrementada nos 2 níveis, e no *CIS Controls* é apresentada apenas como uma.

O resultado deste mapeamento é apresentado na Secção 5.4, onde são expostas as correlações e a matriz do mapeamento final.

### 4.2.1. Elaboração do Questionário

Ainda dentro desta fase foi abordada a elaboração do questionário, para o qual foi necessário a utilização de uma plataforma para a disseminação do questionário junto das empresas, onde foi efetuada uma análise de possíveis plataformas de inquérito, tendo como base 4 critérios:

- Utilização gratuita (ou com um baixo custo) para o número de inquéritos a realizar;
- Ser de fácil utilização durante a elaboração do questionário e durante o processo de resposta, evitando a existência de botões de navegação entre questões;
- Disponibilizar o questionário com um aspeto profissional e apelativo;
- Possuir um *backoffice* que permitisse a extração dos dados de forma direta, para folha de cálculo.

Sendo já do conhecimento, o Microsoft Forms[12] e Google Forms[13] foram excluídos por terem um aspeto mais informal. Foi assim identificada a plataforma QuestionPro[14], que se mostrou cumprir os requisitos pretendidos, tendo-se procedido à realização de alguns testes para verificar a sua usabilidade. Esta apresenta uma interface profissional e intuitiva de utilização, possuí uma funcionalidade de perguntas condicionais, permitindo uma personalização. Contudo, durante a construção do questionário optou-se por não utilizar esta funcionalidade. A plataforma tem um plano gratuito que permite até 100 perguntas e de 199 respostas por inquérito.

Durante a sua utilização, surgiu uma limitação, onde sempre que se utilizavam palavras relacionadas com: “palavras-passe”; “palavras-passe”; “*passwords*”, o conteúdo era bloqueado. Após o contato com o suporte técnico, e explicado o âmbito do trabalho, essa limitação foi removida. Realça-se então a preocupação desta plataforma em ter medidas

[12] https://www.microsoft.com/pt-pt/microsoft-365/online-surveys-polls-quizzes
[13] https://www.google.com/forms/about/
[14] https://www.questionpro.com/

de segurança para evitar que seja utilizada para fins menos lícitos, por exemplo enviando um inquérito recorrendo com intuito de engenharia social, em que poderiam ser solicitadas *passwords*.

### 4.2.2. Disseminação para as Empresas

A escolha do perfil das empresas para responder a este questionário desempenha um papel fundamental na eficácia e relevância das respostas obtidas. A Figura 16, apresenta o fluxograma com os critérios utilizados para a escolha das PMEs.

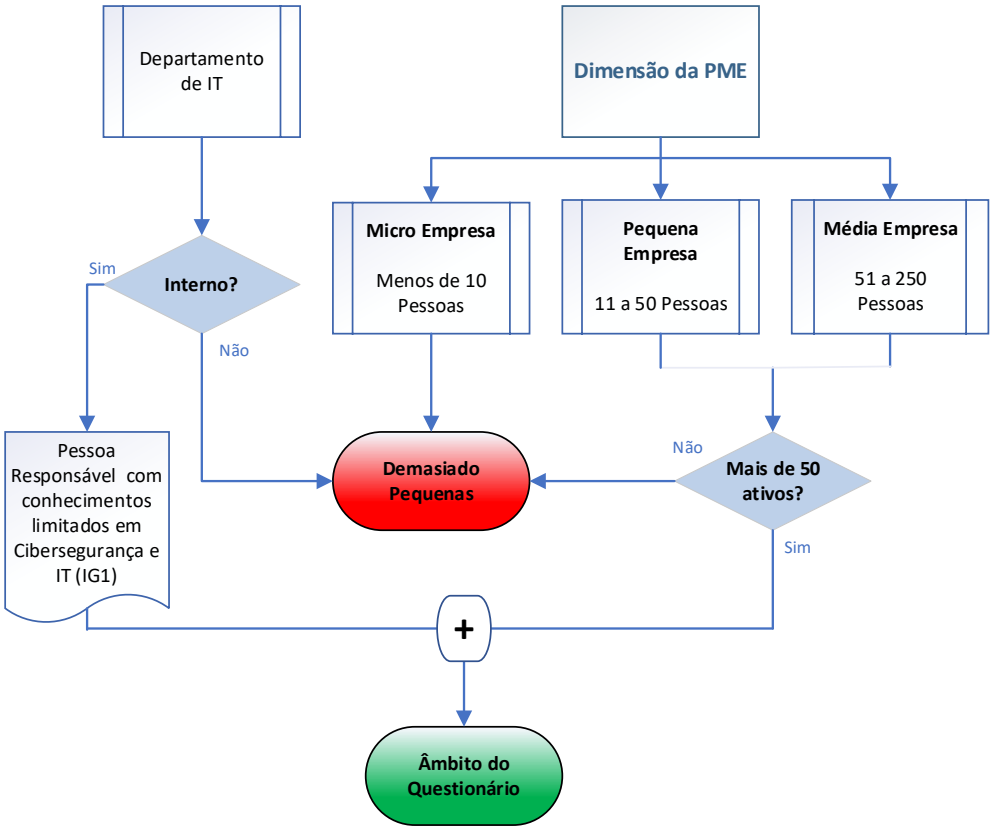



**Figura 16 – Critérios utilizados na escolha da PME**

Na vertente da **Dimensão**, as Microempresas podem não ter uma infraestrutura de TI ou o número de ativos significativo para uma avaliação abrangente de cibersegurança. Por outro lado, pequenas e médias empresas com mais de 50 ativos são mais propensas a ter uma presença digital substancial, incluindo redes, servidores, aplicações e dados sensíveis. No entender do autor, estão mais adequadas para avaliações detalhadas de cibersegurança, garantindo que o questionário é relevante para suas operações e desafios.

Sendo um questionário técnico é importante, que o mesmo seja preenchido por alguém do **Departamento de Informática**, se possível o Responsável, devendo este pertencer à própria organização, pois esta está intimamente envolvida nas operações de TI da empresa, e tem um entendimento profundo dos sistemas, aplicações e processos. A perspetiva

deste, é essencial para avaliar a postura de cibersegurança da empresa de uma forma mais precisa e abrangente.

Sendo o perfil IG1 do *CIS Controls* direcionado para empresas que possuem **Conhecimentos em Cibersegurança** internamente reduzidos, significa que a pessoa pode ter uma compreensão mais básica dos princípios de cibersegurança, e precisa de orientação ou ajuda externa adicional para implementar medidas mais avançadas. Esse perfil é adequado porque reflete a realidade de muitas PMEs, onde recursos especializados em cibersegurança são escassos, mas existe uma conscientização sobre a importância da cibersegurança.

A Figura 17, representa quatro critérios adicionais que também poderiam ter sido tidos em conta para a escolha do perfil da empresa. Tendo acabado por ser excluídos, por dois motivos principais, nomeadamente, porque continham informações confidenciais e ia limitar o número de empresas a responder.

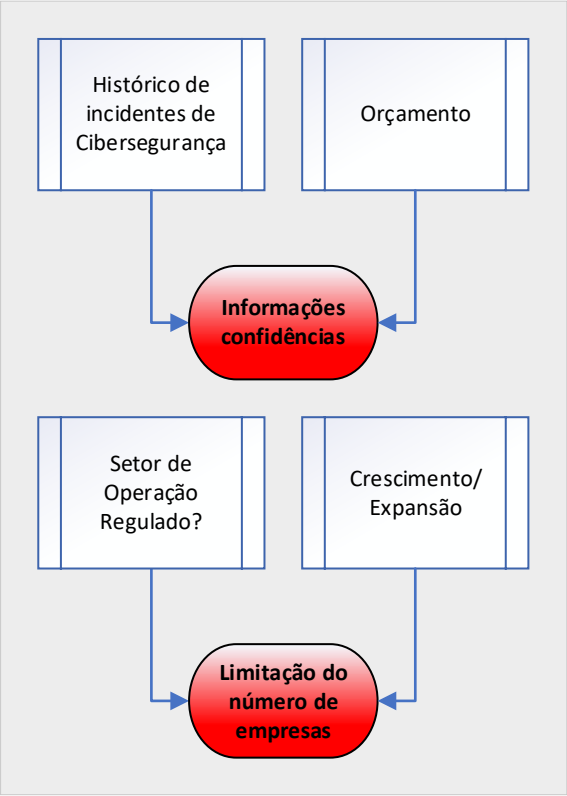



**Figura 17 – Critérios excluídos na escolha da PME**

- **Setor** - O setor em que a empresa opera pode influenciar significativamente as suas necessidades e desafios de cibersegurança. Os setores regulamentados, como serviços financeiros ou saúde, têm de responder a requisitos específicos de conformidade que afetam as suas estratégias de cibersegurança.
- **Histórico de Incidentes de Segurança** - Empresas que têm um histórico conhecido de incidentes de cibersegurança podem ser alvos prioritários para avaliações de segurança mais detalhadas.

- **Orçamento de Cibersegurança** - O orçamento disponível para iniciativas de cibersegurança pode influenciar diretamente a eficácia das medidas de segurança implementadas. Empresas com orçamentos maiores podem ter investido em tecnologias e recursos mais avançados, enquanto aquelas com orçamentos menores podem ter adotado abordagens mais básicas.
- **Crescimento e Expansão –** As Empresas em fase de crescimento ou expansão podem enfrentar desafios diferentes de cibersegurança devido à rápida evolução das suas infraestruturas e operações.

Contudo, tendo em conta o tempo disponível e a inclusão de muitos critérios, poderia aumentar significativamente a complexidade do processo de seleção. Isto ia tornar a identificação e avaliação das empresas adequadas mais demorada e complicada, dificultando a eficiência do processo. Ao limitar o número de critérios, é possível manter o foco na relevância direta do questionário de cibersegurança para as empresas selecionadas. Assim como, alguns critérios adicionais, como histórico de incidentes de segurança ou orçamento de cibersegurança, não se encontram disponíveis, sendo mesmo confidenciais. Por fim iria dificultar a aplicação consistente desses critérios.

Pretende-se que as respostas permitam a definição de tendências, possibilitando o desenvolvimento de estratégias e medidas de segurança para enfrentar os desafios emergentes e em constante evolução.

Uma vez definido o perfil das empresas, as empresas foram escolhidas de acordo com os critérios definidos, garantindo que se enquadrassem no perfil desejado para a avaliação de cibersegurança. Foram então selecionadas 22 empresas da esfera profissional do autor, convidando-as a participar e a fornecer a sua autoavaliação, através do preenchimento do questionário.

Em termos operacionais, foi enviado um *e-mail* personalizado ao responsável de cada empresa explicando o propósito do questionário, a importância da cibersegurança nas empresas e indicando o procedimento que deveriam seguir para dar resposta ao mesmo. Como nota final, foram informados sobre a confidencialidade das informações fornecidas, ressalvando que estas não seriam utilizadas para fins comerciais. Como medida de segurança, o questionário foi protegido com uma senha, assegurando que somente as empresas selecionadas e autorizadas pudessem aceder para responder.

O período de preenchimento do questionário pelas empresas decorreu durante 3 semanas, onde após terminado deste, procedeu-se à extração das respostas da plataforma. As informações foram de imediato anonimizadas, tendo essa medida sido adotada para proteger os dados contra acesso não autorizado ou divulgação não intencional. Através da anonimização, as informações de identificação foram removidas e substituídas por um identificador sequencial, garantindo a privacidade dos respondentes e a confidencialidade das informações fornecidas.

## 4.3. Análise de Resultados

Após a recolha dos dados resultantes das respostas ao questionário, iniciou-se a análise para identificar as áreas mais deficitárias. A estratégia de análise incluí a comparação das respostas do questionário, divididas pelas 3 áreas de incidência dos SMD em Cibersegurança: Organizacional, Técnica e Humana. Assim como a divisão por funções de segurança: Identificar; Proteger, Detetar, Responder e Recuperar, definidos no *CIS Controls*.

Tendo como base este estudo, na Secção 6 é feita uma Análise dos Resultados onde são identificas as áreas em que as organizações apresentam maior vulnerabilidade, ou necessidade de melhoria nas suas práticas de segurança. Dessa forma apresenta-se também um trabalho no sentido de ajudar a mitigar, ou dar resposta às áreas que se encontram mais deficitárias.

## 4.4. Guia de Implementação de Melhorias

Reconhecendo as limitações de recursos comuns nas PMEs, um dos objetivos deste trabalho é a elaboração de um guia, focado em soluções práticas, acessíveis, de elevado impacto, e fundamentais para proteger os dados e sistemas contra ameaças, e que possam ser aplicadas à generalidade das PMEs.

Para isso, a utilização de uma estrutura existente como a que é fornecida pelo *CIS Controls, Implementation Guide for SME* [45] é fundamental devido ao seu reconhecimento global. Onde os controlos são atualizados regularmente para refletir as últimas ameaças e melhores práticas, garantindo que as organizações que os adotam estejam sempre alinhadas com o estado da arte em cibersegurança. O *Implementation Guide for SME*, foca-se na quase totalidade dos controlos do IG1 do *CIS Controls*, definido como *essential cyber hygiene*, oferecendo um valor de segurança eficaz com tecnologia e processos que geralmente já estão disponíveis. Uma vez que no processo de correlação foram identificadas outras necessidades que não se encontram cobertas pelo documento, este guia foi complementado, com outras ações que se encontravam fora deste guia.

Durante a análise dos resultados do questionário, foi identificada uma lacuna significativa relacionada com o fator humano. A formação e a conscientização dos colaboradores são cruciais para o fortalecimento da postura de cibersegurança de qualquer organização. No guia são apresentadas medidas para melhorar a educação em cibersegurança e aumentar a sensibilização para as ameaças, promovendo uma cultura de segurança robusta dentro das PMEs.

Por fim ao seguir estas práticas, pretende-se também que as empresas estejam preparadas para responder às exigências do SMD em Cibersegurança do nível Bronze e Prata. O guia encontra-se no Anexo C.

# 5. Desenvolvimento

Neste capítulo aborda-se a integração dos critérios de avaliação do SMD em Cibersegurança com as práticas de segurança recomendadas pelos *CIS Controls*, fornece uma visão geral deste mapeamento. Esta integração visa enriquecer a análise da maturidade de cibersegurança das PMEs, fornecendo assim uma perspetiva alinhada com *standards* reconhecidos internacionalmente.

Na Figura 18, encontram-se definidas as 6 etapas consideradas durante este processo.


**Figura 18 – Fases da elaboração do questionário**

O SMD em Cibersegurança surge como uma ferramenta para avaliar e melhorar a postura de cibersegurança. Para as PMEs os níveis Bronze e Prata encontram-se mais acessíveis para a sua implementação, sendo o nível Ouro mais exigente, apresentando a necessidade de maior investimento para dar resposta a alguns dos seus requisitos. Assim será possível obter um roteiro claro para a melhoria contínua, onde é fornecido um conjunto consolidado de práticas de segurança reconhecidas globalmente.

Nesta análise, pretende-se assim examinar cada dos requisitos das medidas de cibersegurança do SMD em Cibersegurança, nos níveis Bronze e Prata, e estabelecer uma correlação com uma ou várias medidas de segurança delineados no *CIS Controls* do IG1 e, se necessário do IG2. Como referido na Secção 4.2, esta correlação foi realizada com base em três elementos heurísticos definidos por Ação, Âmbito e Alvo.

## 5.1. Mapeamento Nível Bronze

Como observado anteriormente na Secção 2.8.3, o nível Bronze destaca-se por práticas de simples implementação que fortalecem a segurança da organização contra os riscos mais comuns e prejudiciais de cibersegurança. Estas estratégias são especialmente vantajosas para empresas de menor dimensão e com menos conhecimentos, ou com recursos limitados, tanto em termos de pessoas, como de tecnologia para enfrentar os desafios. Além disso, são igualmente úteis para organizações que não possuem um requisito tão elevado por medidas de cibersegurança.

Apresenta-se de seguida o mapeamento efetuado do nível Bronze com o *CIS Controls*, considerando cada uma das três áreas de incidência da organização: organizacional, técnica e humana:

### 5.1.1. Área Organizacional

O SMD, define o **O.ID-1 - Identificação de funções ou atividades críticas,** onde a organização deve identificar as funções ou atividades críticas, e as dependências existentes das TIC. Para garantir uma identificação completa e atualizada de funções, ou atividades críticas e sua dependência das TIC, podemos relacionar o **Alvo (AL)** dessa medida do Selo Digital com o *CIS Controls* da seguinte forma:

**Medida de Segurança:** 3.2 Estabelecer e manter um inventário de dados IG1

**Tipo de Ativo:** Dados

**Função de Segurança:** Identificar

Este controlo do *CIS Controls* aborda diretamente a necessidade de criar e manter um inventário de dados, especialmente os sensíveis. Esta medida é crucial para entender quais os dados que são críticos para as operações da organização, e como eles estão relacionados às atividades dependentes das TIC. Ao manter um inventário atualizado, a organização pode garantir uma identificação precisa das funções, ou atividades críticas, e sua relação com os ativos de TIC. Isso permite uma melhor compreensão dos riscos, e ajuda na tomada de decisões informadas sobre a segurança da informação, e a continuidade dos negócios.

Assim, o *CIS Controls* não se alinha diretamente com o requisito específico do Selo Digital, mas ele aborda uma parte importante do processo necessário para cumprir essa exigência, fornece uma base sólida para a gestão das funções ou atividades críticas.

A evidência do Selo Digital, envolve um documento contendo a identificação de funções ou atividades críticas, dos ativos e da relação e/ou dependência entre eles.

O SMD, define o **O.IAC-1 - Inventariação dos ativos e documentos da arquitetura de comunicações de dados,** onde a organização deve inventariar todos os seus ativos, documentar a sua arquitetura de comunicações de dados, e atualizar esta informação sempre que necessário. Esta medida do Selo Digital propõe uma abordagem abrangente para garantir a segurança da informação, com foco na inventariação completa dos ativos e na manutenção regular dessa informação. Existem **Ações (AC),** a relacionar este requisito em 3 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 1.1 - Estabelecer e manter um inventário detalhado dos ativos corporativos IG1

**Tipo de Ativo:** Dispositivo

**Função de Segurança:** Identificar

**Descrição:** Esta medida visa manter um inventário completo de todos os ativos corporativos que podem armazenar ou processar dados. Isso inclui dispositivos de utilizador final, dispositivos de rede, dispositivos IoT e servidores. O inventário deve conter informações como endereço de rede, endereço de *hardware*, nome da máquina, proprietário do ativo, departamento e *status* de aprovação para ligação à rede.

**Medida de Segurança:** 2.1 - Estabelecer e manter um inventário do software IG1

**Tipo de Ativo:** Aplicações

**Função de Segurança:** Identificar

Esta medida requer um inventário detalhado de todo o *software* licenciado instalado nos ativos corporativos. O inventário de *software* deve incluir informações como título, editor, data de instalação, URL, versão, entre outros.

**Medida de Segurança:** 12.4 - Estabelecer e manter diagrama(s) de arquitetura IG2

**Tipo de Ativo:** Rede

**Função de Segurança:** Identificar

Esta medida visa manter diagramas de arquitetura e documentação de sistema de rede atualizados. Sendo essencial para entender a estrutura da rede e garantir que as mudanças significativas na empresa sejam refletidas na documentação.

Ao implementar as medidas do *CIS Controls*, a organização estará alinhada com práticas recomendadas de segurança da informação, conforme delineado pelos SMD. A disponibilização do inventário de ativos e do diagrama de rede será uma evidência tangível desse.

O SMD, define o **O.PUA-1 - Política de utilização aceitável dos recursos TIC,** a organização deve definir e disponibilizar junto de todos os seus utilizadores a política de utilização aceitável dos recursos TIC.

O **Âmbito (AM)** desta medida do Selo Digital está relacionado com a definição e implementação de uma Política de Utilização Aceitável (PUA) dos recursos da organização. Embora não esteja diretamente descrito nos controlos de segurança, existe um documento auxiliar que atende a esse requisito, que é o *template* disponibilizado pelo *CIS Controls Acceptable Use Policy* [76].

O *template* oferece uma estrutura abrangente para a criação de uma Política de Utilização Aceitável eficaz. Ele contém diretrizes sobre o que deve ser abordado na política, incluindo as linhas de orientação para a boa utilização dos recursos de TIC, garantindo assim que a utilização seja feita de forma segura, por todos os colaboradores com acesso aos mesmos. A organização pode assim elaborar uma PUA alinhada com as melhores práticas de segurança da informação. O modelo orienta a inclusão de seções importantes, como definição de responsabilidades, direitos e obrigações dos utilizadores, consequências pelo uso inadequado dos recursos, entre outros aspetos relevantes.

O SMD, define o **O.RSI-1 - Identificação de responsável pela função de Segurança da Informação,** onde a organização deve ter um ponto de contato do ponto de vista técnico/operacional que deve ser capaz de responder a eventuais solicitações externas, sendo esperada disponibilidade para contatos de emergência fora do horário de expediente. A medida do Selo Digital enfatiza a importância de identificar um responsável pela função de Segurança da Informação, que deve atuar como ponto de contato técnico/operacional da organização, e estar preparado para responder a solicitações externas, como aquelas feitas pelo CERT.PT. Existem **Ações (AC)**, a relacionar esse requisito em 2 medidas se segurança fornecidos pelo *CIS Controls*:

**Medida de Segurança:** 17.1 - Designar Pessoal para Gerir o Tratamento de Incidentes IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Responder

Esta medida requer a designação de uma pessoa responsável, e pelo menos uma substituta, para gerir o processo de tratamento de incidentes da empresa. Esta equipa está encarregue de coordenar e documentar os esforços de resposta e recuperação a incidentes. Se for utilizado um fornecedor externo, pelo menos uma pessoa interna da empresa deve supervisionar o trabalho.

**Medida de Segurança:** 17.2 - Estabelecer e Manter Informações de Contato para Comunicar Incidentes de Segurança IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Responder

Esta medida envolve estabelecer e manter informações de contato das partes que precisam ser informadas sobre os incidentes de segurança. Isso inclui funcionários internos, fornecedores externos, agências governamentais, parceiros, entre outros. É importante verificar anualmente esta lista de contatos para garantir que as informações se encontram atualizadas.

Ao disponibilizar a identificação do responsável pela função de segurança da informação como evidência, a organização demonstra conformidade com as medidas do Selo Digital.

### 5.1.2. Área Técnica

O SMD, define o **T.CS-1 - Cópias de Segurança -** A organização deve implementar uma política de cópias de segurança e garantir que as cópias de segurança podem ser utilizadas, caso seja necessário. Deve ainda garantir que as cópias de segurança são testadas e validadas regularmente, através da execução de planos de testes de restabelecimento. A medida do Selo Digital visa assegurar que os dados da organização sejam salvaguardados automaticamente, e regularmente por meio de uma plataforma de cópias de segurança, como unidades de armazenamento portátil e/ou na nuvem. Existem Ações, a relacionar esse requisito em 4 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 11.1 - Estabelecer e Manter um Processo de Recuperação de Dados IG1

**Tipo de Ativo:** Dados

**Função de Segurança:** Recuperar

Esta medida visa estabelecer e manter um processo de recuperação de dados que aborde o âmbito das atividades de recuperação, a prioritização e a segurança dos dados de *backup*. A documentação desse processo deve ser analisada e atualizada anualmente ou quando ocorrerem mudanças significativas na empresa.

**Medida de Segurança:** 11.2 - Executar Backups Automatizados IG1

**Tipo de Ativo:** Dados

**Função de Segurança:** Recuperar

Esta medida envolve a execução de *backups* automatizados dos ativos corporativos dentro do âmbito. Os *backups* devem ser realizados semanalmente ou com maior frequência, dependendo da sensibilidade dos dados.

**Medida de Segurança:** 11.3 - Proteger os Dados de Recuperação IG1

**Tipo de Ativo:** Dados

**Função de Segurança:** Proteger

Nesta medida, os dados de recuperação devem ser protegidos com controlos equivalentes aos dados originais. Isso pode incluir o uso de criptografia ou a segregação dos dados, dependendo dos requisitos de segurança.

**Medida de Segurança:** 11.4 - Estabelecer e Manter uma Instância Isolada de Dados de Recuperação IG1

**Tipo de Ativo:** Dados

**Função de Segurança:** Recuperar

Esta medida envolve estabelecer e manter uma instância isolada de dados de recuperação. Isso pode incluir o controlo da versão de destinos de *backup* por meio de sistemas ou serviços *offline*, na *cloud* ou *offsite*.

Ao exibir a plataforma existente, e demonstrar o processo de cópia de segurança como evidência, a organização demonstra conformidade com as medidas do Selo Digital e também está alinhada com as práticas recomendadas de segurança da informação delineadas pelos *CIS Controls*.

O SMD, define o **T.AS-1 - Atualizações de segurança -** a organização deve garantir a aplicação automática de atualizações de segurança dos sistemas operativos e componentes de *software* a todos os seus postos de trabalho. A medida do Selo Digital procura configurar e garantir a atualização automática dos sistemas de *software*, como sistemas operativos, produtividade, leitores de PDF, navegadores, entre outros. Existem **Ações (AC),** a relacionar esse requisito em 2 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 7.3 - Executar a Gestão Automatizada de Patches do Sistema Operativo IG1

**Tipo de Ativo:** Aplicações

**Função de Segurança:** Proteger

Esta medida envolve realizar atualizações do sistema operativo dos ativos corporativos por meio da gestão automatizada de *patches* mensalmente, ou com maior frequência. Isso garante que os sistemas operativos estejam atualizados com as correções de segurança mais recentes, reduzindo assim as vulnerabilidades.

**Medida de Segurança:** 7.4 - Executar a Gestão Automatizada de Patches de Aplicações IG1

**Tipo de Ativo:** Aplicações

**Função de Segurança:** Proteger

Esta medida envolve realizar atualizações de aplicações dos ativos corporativos por meio da gestão automatizada de *patches* mensalmente, ou com mais frequência. Manter as aplicações atualizadas é crucial para mitigar vulnerabilidades conhecidas e proteger contra possíveis ataques.

Ao demonstrar, através de acesso aleatório aos terminais, que a atualização automática dos sistemas operativos e componentes está implementada, a organização fornece evidências de conformidade com as medidas do Selo Digital.

O SMD, define o **T.PPT-1 - Proteção de postos de trabalho,** a organização deve garantir que se encontra instalado um antivírus nos seus postos de trabalho e dispositivos móveis. A medida do Selo Digital procura garantir a existência de proteção contra ameaças, como vírus e código malicioso, em todos os postos de trabalho e dispositivos móveis da organização. Existem **Ações (AC),** a relacionar esse requisito em 2 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 10.1 - Instalar e Manter um Software Anti-malware IG1

**Tipo de Ativo:** Dispositivo

**Função de Segurança:** Proteger

Esta medida envolve instalar e manter um *software* anti-*malware* em todos os ativos corporativos. Isso ajuda a proteger os dispositivos contra ameaças como vírus, *malware* e outros códigos maliciosos.

**Medida de Segurança:** 10.2 - Configurar Atualizações Automáticas de Assinatura Anti-malware IG1

**Tipo de Ativo:** Dispositivo

**Função de Segurança:** Proteger

Nesta medida, é importante configurar atualizações automáticas para os ficheiros de assinatura anti-*malware* em todos os ativos corporativos. Isso garante que o *software* anti-*malware* está sempre atualizado com as últimas definições de ameaças, permitindo uma proteção eficaz contra novos ataques.

Ao facultar acesso, de forma aleatória, a postos de trabalho e dispositivos móveis para validar que estão protegidos contra ameaças, a organização está a fornecer as evidências de conformidade com as medidas do Selo Digital.

O SMD, define o **T.PPI-1 - Proteção perimetral e da infraestrutura,** a organização deve garantir, tanto a proteção perimetral de infraestrutura como também a proteção física dos principais componentes da infraestrutura. A medida do Selo Digital visa garantir a proteção do perímetro da infraestrutura, tanto no nível lógico como no físico, incluindo a

implementação de uma *firewall* nos dispositivos, boas práticas de configuração e proteção através de *passwords* em todos os equipamentos expostos à *internet* e segurança física dos principais componentes da infraestrutura. Existem **Ações (AC),** a relacionar esse requisito em 5 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 4.4 - Implementar e Gerir uma Firewall nos Servidores IG1

**Tipo de Ativo:** Dispositivo

**Função de Segurança:** Proteger

Esta medida envolve implementar e gerir uma *firewall* nos servidores, utilizando a *firewall* do sistema operativo ou um agente de *firewall* de terceiros, sempre que houver suporte. Isso ajuda a controlar o tráfego de entrada e saída nos servidores, aumentando a segurança da infraestrutura.

**Medida de Segurança:** 4.5 - Implementar e Gerir a Firewall nos Dispositivos de Utilizador Final IG1

**Tipo de Ativo:** Dispositivo

**Função de Segurança:** Proteger

Esta medida envolve implementar e gerir uma *firewall* baseada no posto ou uma ferramenta de filtragem de portas nos dispositivos dos utilizadores finais. Deve existir uma regra de negação padrão que bloqueia todo o tráfego, exceto os serviços e portas explicitamente permitidos.

**Medida de Segurança:** 4.6 - Gerir com Segurança os Ativos e Software Corporativos IG1

**Tipo de Ativo:** Rede

**Função de Segurança:** Proteger

Esta medida abrange a gestão segura dos ativos e *software* corporativos, utilizando práticas como gestão de configuração, através de infraestrutura controlada por versão e acesso a interfaces administrativas por meio de protocolos de rede seguros, como SSH e HTTPS.

**Medida de Segurança:** 4.7 - Gerir Contas Padrão nos Ativos e Software Corporativos IG1

**Tipo de Ativo:** Utilizadores

**Função de Segurança:** Proteger

Esta medida envolve gerir contas padrão nos ativos e *software* corporativos, como *root*, *administrator* e outras contas de pré-configuradas. A implementação pode incluir a desativação das contas ou torná-las inutilizáveis. Isso é fundamental para evitar que credenciais padrão sejam exploradas por pessoal mal intencionadas.

**Medida de Segurança:** 12.2 - Estabelecer e Manter uma Arquitetura de Rede Segura IG2

**Tipo de Ativo:** Rede

**Função de Segurança:** Proteger

Esta medida visa estabelecer e manter uma arquitetura de rede segura, abordando segmentação, privilégio mínimo e disponibilidade. Isso ajuda a garantir que a rede seja organizada de maneira a limitar o impacto de possíveis ataques.

Ao exibir a implementação das medidas de segurança lógicas e físicas ao nível dos equipamentos e espaços afetos à infraestrutura, a organização demonstra conformidade com as medidas do Selo Digital e está alinhada com as práticas recomendadas de segurança da informação delineadas pelos *CIS Controls*.

O SMD, define o **T.CWC-1 - Conformidade *Webcheck*,** a organização tem de garantir que estão a ser aplicadas as melhores práticas ao nível de segurança de correio eletrónico e páginas de internet. A medida do Selo Digital busca implementar as melhores práticas associadas à segurança do correio eletrónico e acesso a páginas de internet. Existe uma **Ação (AC),** relacionada a este requisito nas medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 9.5 - Implementar o DMARC IG2

**Tipo de Ativo:** Rede

**Função de Segurança:** Proteger

Esta medida visa diminuir a possibilidade de *e-mails* forjados ou modificados de domínios válidos, implementando a política *Sender Policy Framework* (SPF) e utilização de certificado digital para os *websites* HTTPS.

Ao demonstrar evidências como a ligação HTTP/S, o certificado digital SPF e a implementação do *Domain-based Message Authentication Reporting and Conformance* (DMARC), a organização estará mostrando conformidade com as medidas do Selo Digital.

O SMD, define o **T.AM-1 - Autenticação Multifator,** a organização deve ter ativa a autenticação multifator nas suas aplicações críticas, sempre que esta opção se encontrar disponível. A medida do Selo Digital propõe ativar a autenticação multifator (MFA) em todas as aplicações críticas para a organização, sempre que esta opção estiver disponível, Existem **Ações (AC),** a relacionar esse requisito em 3 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 6.3 - Exigir MFA para Aplicações Expostas Externamente IG1

**Tipo de Ativo:** Utilizadores

**Função de Segurança:** Proteger

Esta medida requer que todas as aplicações corporativas ou de terceiros expostas externamente apliquem o MFA, sempre que houver suporte para isso. O MFA deve ser imposto por meio de um serviço de diretório ou fornecedor de *Single Sign-On* (SSO). Isso ajuda a fortalecer a autenticação e reduzir o risco de acesso não autorizado a sistemas críticos.

**Medida de Segurança:** 6.4 - Exigir MFA para Acesso Remoto à Rede IG1

**Tipo de Ativo:** Utilizadores

**Função de Segurança:** Proteger

Esta medida envolve exigir MFA para acesso remoto à rede. O MFA adiciona uma camada adicional de segurança ao processo de autenticação, especialmente importante para acesso remoto, onde os riscos de comprometimento são potencialmente maiores.

**Medida de Segurança:** 6.5 - Exigir MFA para Acesso de Administração IG1

**Tipo de Ativo:** Utilizadores

**Função de Segurança:** Proteger

Nesta medida, é necessário exigir MFA para todas as contas de acesso de administração, sempre que houver suporte para isso, em todos os ativos corporativos. Isso incluí ativos geridos no *site* local ou por meio de um fornecedor externo. O MFA adiciona uma camada adicional de proteção contra acesso não autorizado a recursos críticos da organização.

Ao identificar aplicações críticas que utilizam autenticação multifator, a organização estará demonstrando conformidade com as medidas do Selo Digital.

### 5.1.3. Área Humana

O SMD, define o **H.PF-1- Plano de Formação** e o **H.PF-2 - Plano de Formação -** A organização deve estabelecer um plano de ações de formação em segurança da informação e cibersegurança, bem como definir os processos e procedimentos necessários para garantir a sua correta implementação.

A medida do Selo Digital visa definir e executar um plano de formação sobre as políticas aprovadas e implementadas pela organização. Existe uma **Ação (AC),** a relacionar este requisito com as medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 14.1 - Estabelecer e Manter um Programa de Conscientização de Segurança IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Proteger

Esta medida envolve estabelecer e manter um programa de conscientização de segurança. O objetivo desse programa é formar a força de trabalho da empresa sobre como interagir com ativos e dados corporativos de maneira segura. Isso inclui a realização de formação na contratação e, no mínimo, anualmente, além de analisar e atualizar o conteúdo anualmente ou quando ocorrerem mudanças significativas na empresa que possam afetar essa proteção.

Já na segunda medida do Selo Digital propõe-se a execução de um plano de formação aplicável a todos os colaboradores da organização, com o objetivo de fornecer conhecimentos fundamentais de ciberhigiene e sobre as principais ameaças, como *phishing*, além de instruir sobre os canais de reporte dessas ameaças. Existe outra **Ação (AC),** a relacionar este requisito com as medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 14.2 - Treinar Membros da Força de Trabalho para Reconhecer Ataques de Engenharia Social IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Proteger

Esta medida envolve treinar os membros da força de trabalho para reconhecer ataques de engenharia social, como *phishing* e uso não autorizado. Isso inclui fornecer conhecimentos sobre como identificar e responder adequadamente a tentativas de *phishing*, que é uma das principais ameaças enfrentadas pelas organizações.

Ao realizar entrevistas aleatórias com membros da organização, a empresa pode obter evidências da eficácia do programa de conscientização de segurança. Essa prática ajuda a garantir que os funcionários estejam cientes das políticas de segurança e saibam como aplicá-las no seu dia-a-dia de trabalho.

O SMD, define o **H.FIC-1 - Fontes de informação e canais de comunicação -** a organização deve garantir que existe consulta regular de fontes de informação e acesso a canais de comunicação fidedignos. Para estabelecer um plano de comunicação eficaz e garantir a consulta regular de fontes de informação sobre ameaças à segurança da informação, podemos relacionar o **Alvo (AL)** desta medida do Selo Digital com o *CIS Controls* da seguinte forma:

**Medida de Segurança:** 17.3 Estabelecer e manter um processo corporativo para comunicar incidentes IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Responder

Embora esta medida do *CIS Controls* se concentre principalmente na comunicação de incidentes de segurança, ela também aborda a necessidade de ter um processo corporativo

bem definido, para relatar eventos de segurança. Isso inclui a definição de um cronograma de relatórios, a identificação do pessoal responsável pelo relato, o estabelecimento de um mecanismo para relatar e a determinação das informações mínimas a serem incluídas nos relatórios.

Ao adaptar este controlo para o contexto da medida do Selo Digital, podemos considerar que o plano de comunicação também deve incluir a forma como a organização consulta regularmente fontes de informação sobre ameaças, tais como os alertas de segurança emitidos por exemplo pelo CNCS, e como essas informações são disseminadas internamente. Isso garante que a organização esteja atualizada sobre eventos que possam representar ameaças à segurança da informação, e possa responder de maneira eficaz a esses eventos quando necessário.

A evidência demonstra que a organização não apenas estabeleceu um plano de comunicação eficaz, mas também que está comprometida em manter-se atualizada sobre as ameaças de segurança da informação, e em comunicar proactivamente essas informações dentro da organização. Isso contribui para uma postura de segurança proativa e ajuda a garantir uma resposta rápida e eficaz a qualquer incidente de segurança que possa surgir.

## 5.2. Mapeamento Nível Prata

A utilização do nível Prata (referido na Secção 2.8.3) já implica a adoção de práticas de nível intermedio, exigindo a conformidade, tanto com os requisitos deste nível, quanto do nível anterior (Bronze). Estas práticas são direcionadas a organizações que demonstram competências de cibersegurança além do básico, e possuem uma dimensão média ou enfrentam necessidades mais amplas de cibersegurança devido à sua maior dependência das tecnologias para garantir a operação do negócio.

### 5.2.1. Área Organizacional

O SMD, define o **O.PP-1 - Politica de palavra-passe,** a medida do Selo Digital procura definir uma política de palavra-passe que contenha requisitos mínimos de dimensão e complexidade, prazos para alteração regular e mecanismos técnicos para garantir sua execução. Existe uma **Ação (AC),** a relacionar este requisito com as medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 5.2 - Usar Palavras-Passe Exclusivas IG1

**Tipo de Ativo:** Utilizadores

**Função de Segurança:** Proteger

**Descrição:** Esta medida recomenda o uso de palavras-passe exclusivas para todos os ativos corporativos. As melhores práticas de implementação incluem, no mínimo, uma senha de

8 caracteres para contas que usam MFA, e uma senha de 14 caracteres para contas que não usam MFA. Deve ser garantido que cada conta tenha a sua própria senha, aumentando a segurança dos sistemas e reduzindo o risco de comprometimento de várias contas com uma única senha.

Ao apresentar uma política de palavras-passe que atenda aos requisitos de dimensão, complexidade, e prazos para alteração regular, a organização demonstra conformidade com as medidas do Selo Digital.

O SMD, define o **O.PAP-1 - Política de acessos e permissões** - a medida do Selo Digital procura segmentar os acessos de acordo com a necessidade de saber (*need-to-know*) e o princípio do menor privilégio (*least privilege*), além de documentar os níveis de acesso aos principais sistemas e aplicações. Existem **Ações (AC),** a relacionar esse requisito em 2 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 5.1 - Estabelecer e Manter um Inventário de Contas IG1

**Tipo de Ativo:** Utilizadores

**Função de Segurança:** Identificar

Esta medida envolve estabelecer e manter um inventário de todas as contas geridas na empresa, incluindo contas de utilizador e administrador. O inventário deve conter informações como nome da pessoa, nome de utilizador, datas de início/término e departamento. Isso ajuda a garantir que apenas as contas autorizadas tenham acesso aos sistemas e aplicações, conforme necessário, alinhando-se com os princípios de *least privilege* e *need-to-know*.

**Medida de Segurança:** 3.3 - Configurar Listas de Controlo de Acesso a Dados IG1

**Tipo de Ativo:** Dados

**Função de Segurança:** Proteger

Esta medida consiste em configurar listas de controlo de acesso a dados com base na necessidade de conhecimento do utilizador. As listas de controlo de acesso devem ser aplicadas a sistemas de ficheiros, bases de dados e aplicações locais e remotas, garantindo que apenas os utilizadores autorizados tenham acesso aos dados necessários para realizar as suas funções.

Ao apresentar evidências do processo de gestão de acessos e da matriz de segregação de funções por acessos e respetivas atribuições, a organização demonstra conformidade com as medidas do Selo Digital.

O SMD, define o **O.GMO-1 - Gestão da mudança organizacional,** a organização deve efetuar as devidas atualizações ao nível de procedimentos TIC, aquando da entrada, alteração e saída de colaboradores.

A medida do Selo Digital busca definir uma política que assegura a mudança organizacional ao nível das TIC, com ênfase nas ações a serem executadas após a saída de um colaborador ou mudança de funções associadas a ele. **Ações (AC),** a relacionar esse requisito em 2 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 6.1 - Estabelecer um Processo de Concessão de Acesso IG1

**Tipo de Ativo:** Utilizadores

**Função de Segurança:** Proteger

Este controlo envolve estabelecer e seguir um processo, preferencialmente automatizado, para conceder acesso aos ativos corporativos quando há uma nova contratação, concessão de direitos ou mudança de função de um utilizador. Isso garante que novos colaboradores ou colaboradores com funções alteradas tenham acesso apropriado aos recursos de TI, de acordo com suas responsabilidades e necessidades.

**Medida de Segurança:** 6.2 - Estabelecer um Processo de Revogação de Acesso IG1

**Tipo de Ativo:** Utilizadores

**Função de Segurança:** Proteger

Este controlo consiste em estabelecer e seguir um processo, preferencialmente automatizado, para revogar o acesso aos ativos corporativos, desativando contas imediatamente após o encerramento, revogação de direitos ou mudança de função de um utilizador. Desativar contas, em vez de excluí-las, pode ser necessário para preservar os registos de auditoria e garantir que nenhum acesso não autorizado seja mantido após a mudança organizacional.

Ao apresentar evidências de documentos contendo políticas de mudança organizacional, especialmente as ações relacionadas à saída ou mudança de funções de um colaborador, a organização demonstra conformidade com as medidas do Selo Digital.

O SMD, define o **O.PRI-1 - Plano de reação a incidentes de Cibersegurança -** criar um plano de reação a incidentes de cibersegurança que inclua, no mínimo as funções e responsabilidades; quem e quando contatar; como reagir a eventos críticos, para garantia que a organização se encontra preparada para responder a situações de incidentes de cibersegurança. A medida do Selo Digital procura definir um plano de reação a incidentes de cibersegurança, que inclua funções e responsabilidades, procedimentos de contato e como reagir a eventos críticos, como ataques de negação de serviço e *ransomware*. Existe uma **Ação (AC),** a relacionar este requisito com as medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 17.4 - Estabelecer e Manter um Processo de Resposta a Incidentes IG2

**Tipo de Ativo:** N/A

**Função de Segurança:** Responder

Este controlo envolve estabelecer e manter um processo de resposta a incidentes que aborde funções e responsabilidades, requisitos de conformidade e um plano de comunicação. Isso inclui a definição de procedimentos claros sobre como lidar com incidentes de cibersegurança, quem deve ser contatado em caso de incidente, como responder a eventos críticos, como ataques de negação de serviço e *ransomware*, e como comunicar e coordenar a resposta dentro e fora da organização.

Ao apresentar o plano de reação a incidentes de cibersegurança como evidência, a organização demonstra conformidade com as medidas do Selo Digital.

### 5.2.2. Área Técnica

O SMD, define o **T.CWC-2 - Conformidade Webcheck -** a organização tem de garantir que estão a ser aplicadas as melhores práticas a nível de segurança de correio eletrónico e páginas de internet.

A medida do Selo Digital visa implementar as melhores práticas relacionadas à segurança do correio eletrónico e acesso a páginas da internet. Para demonstrar conformidade com esse requisito, o nível intermediário exige a implementação de *HTTP Strict Transport Security* (HSTS), cabeçalhos de segurança e *DomainKeys Identified Mail* (DKIM) como evidências.

À semelhança do **T.CWC-1** esta **Ação (AC)** é um incremento das medidas da segurança do correio eletrónico e *internet* e também se encontra alinhada com o *CIS Controls* 9.5 - Implementar o DMARC, que recomenda para além da implementação do DMARC e DKIM, que são as práticas mencionadas no nível intermédio de evidências (anteriormente já se tinha implementado o SPF no **T.CWC-1**).

Relacionando o HSTS com a medida de segurança do Selo Digital, podemos considerar a importância de implementar o HSTS como parte integrante das práticas de segurança do correio eletrónico e *internet*. Ao garantir que as comunicações sejam realizadas apenas através de HTTPS, o HSTS ajuda a proteger contra ataques de *spoofing* e ataques *man-in-the-middle*, garantindo a integridade e confidencialidade das informações transmitidas.

O HSTS pode ser visto como uma camada adicional de proteção para fortalecer a segurança das comunicações online, incluir o HSTS como parte das práticas de segurança do correio eletrónico e *internet* é uma medida proativa para mitigar possíveis vulnerabilidades e proteger a organização contra ameaças cibernéticas.

Ao apresentar as evidências de implementação de HSTS, cabeçalhos de segurança e DKIM, a organização está demonstrando conformidade com as melhores práticas de segurança do correio eletrónico e acesso a páginas da internet, ao mesmo tempo em que está seguindo as recomendações do *CIS Controls*.

O SMD, define o **T.GP-1 - Gestão da palavra-passe -** a organização deve definir mecanismos de autenticação e estes devem ser mantidos de acordo com as características dos sistemas e dos perfis de acesso. Deve garantir que as palavras-passe se encontram armazenadas através de uma solução para a gestor de palavras-passe. O **Âmbito (AM)** desta medida do Selo Digital está relacionado com a segurança da informação e a gestão adequada das palavras-passe associadas à gestão da infraestrutura. Embora não esteja explicitamente descrito nos controlos de segurança, existe um documento auxiliar que complementa com a designação de o *CIS Password Policy Guide* [77].

A medida do Selo Digital destaca a importância de armazenar as palavras-passe associadas à gestão da infraestrutura de forma segura, preferencialmente através de uma solução de gestor de palavras-passe *offline*. Existe um alinhamento com as diretrizes do *CIS Controls*, que enfatizam a importância de proteger as credenciais de acesso. O documento do CIS *Password Policy Guide* pode servir como referência para ajudar na escolha criteriosa da solução do gestor de palavras-passe.

Para cumprir com a evidência exigida, é necessário demonstrar como a política de palavra-passe, alinhado com o **O.PP-1 - Politica de palavra-passe** está a ser aplicada na prática e como ela está alinhada com a solução do gestor de palavras-passe implementado. Isso pode envolver mostrar exemplos de palavras-passe geradas pela solução, garantindo que atendam aos requisitos da política estabelecida.

O SMD, define o **T.PAD-1 - Privilégios de acesso diferenciados -** A organização deve garantir que os acessos e permissões são concedidos de acordo com os princípios do menor privilégio e da segregação de funções. A medida do Selo Digital procura garantir que qualquer tipo de acesso atribuído, bem como as permissões de administração dos sistemas, aplicações e infraestrutura, sejam concedidos numa base de *need-to-know* e *least privilege*, e de acordo com a política definida. Existe uma **Ação (AC),** a relacionar este requisito com as medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 5.4 - Restringir Privilégios de Administrador a Contas de Administrador Dedicadas IG1

**Tipo de Ativo:** Utilizadores

**Função de Segurança:** Proteger

Este controlo envolve restringir os privilégios de administrador a contas de administrador dedicadas nos ativos corporativos. A realização de atividades gerais de computação, como

navegação na *Internet* e *e-mail*, deve ocorrer a partir da conta primária não privilegiada do utilizador. Isso ajuda a reduzir o risco de acesso não autorizado e limita o impacto de possíveis ataques, garantindo que apenas as pessoas autorizadas tenham acesso aos privilégios de administração, conforme necessário.

Ao apresentar registos da identificação de acessos a sistemas e aplicações por perfil funcional e assegurar a conformidade dos mesmos com a política definida, a organização demonstra conformidade com as medidas do Selo Digital.

O SMD, define o **T.SC-1 - Securização (*hardening*) de configurações -** a organização deve garantir que se encontram a ser praticadas as melhores práticas de segurança ao nível do posto de trabalho, das configurações do sistema operativo e principais aplicações utilizadas.

A medida do Selo Digital visa aplicar as melhores práticas de segurança e privacidade no nível do posto de trabalho, das configurações do sistema operativo e das principais aplicações utilizadas. Existem **Ações (AC),** a relacionar esse requisito em 5 medidas de segurança do *CIS Controls*.

**Medida de Segurança:** 3.6 - Cifrar Dados em Dispositivos de Utilizador Final IG1

**Tipo de Ativo:** Dispositivos

**Função de Segurança:** Proteger

Esta medida envolve cifrar os dados de dispositivos do utilizador final que contenham dados sensíveis. Exemplos de implementações incluem o uso de Windows BitLocker[15], Apple FileVault[16] ou Linux dm-crypt[17], entre outros. Isso ajuda a proteger os dados em caso de perda ou roubo do dispositivo.

**Medida de Segurança:** 4.1 - Estabelecer e Manter um Processo de Configuração Segura para Aplicações IG1

**Tipo de Ativo:** Aplicações

**Função de Segurança:** Proteger

Este controlo consiste em estabelecer e manter um processo de configuração segura para ativos corporativos, incluindo equipamentos do utilizador final, dispositivos móveis, dispositivos não computacionais/IoT e servidores, bem como *software* como sistemas

[15] https://learn.microsoft.com/en-us/windows/security/operating-system-security/data-protection/bitlocker/
[16] https://support.apple.com/pt-pt/guide/mac-help/flvlt001/mac
[17] https://www.linux.com/training-tutorials/how-encrypt-linux-file-system-dm-crypt/

operativos e aplicações. Isso garante que as configurações de segurança adequadas sejam aplicadas para proteger os ativos contra ameaças.

**Medida de Segurança:** 4.2 - Estabelecer e Manter um Processo de Configuração Segura para a Infraestrutura de Rede IG1

**Tipo de Ativo:** Rede

**Função de Segurança:** Proteger

Esse controlo envolve estabelecer e manter um processo de configuração segura para dispositivos de rede. Isso inclui *routers*, *switches*, *firewalls* e outros dispositivos que compõem a infraestrutura de rede da organização. Garantir que esses dispositivos estejam configurados de forma segura é crucial para proteger a rede contra acessos não autorizados e ataques.

**Medida de Segurança:** 4.3 - Configurar o Bloqueio Automático de Sessão nos Ativos Corporativos IG1

**Tipo de Ativo:** Utilizadores

**Função de Segurança:** Proteger

Este controlo envolve configurar o bloqueio automático de sessão nos ativos corporativos após um período definido de inatividade. Isso ajuda a proteger os dispositivos contra acessos não autorizados quando não estão em uso.

**Medida de Segurança:** 5.1 - Garantir o Uso Apenas de Navegadores e Clientes de E-mail Suportados Plenamente IG1

**Tipo de Ativo:** Aplicações

**Função de Segurança:** Proteger

Esta medida garante que apenas navegadores e clientes de *e-mail* suportados plenamente tenham permissão para ser executados na empresa, usando apenas a versão mais recente fornecida pelo fabricante. Isso ajuda a reduzir o risco de exploração de vulnerabilidades em *software* desatualizado.

Ao implementar esses controlos, a organização aplica as melhores práticas de segurança e privacidade nos seus postos de trabalho, sistemas operativos e aplicações, contribuindo para a resposta às evidências para o cumprimento do SMD em Cibersegurança.

O SMD, define o **T.CA-1 - Controlo aplicacional -** A organização deve garantir que não é permitida a instalação de aplicações não autorizadas por parte dos utilizadores. A medida do Selo Digital procura aplicar mecanismos que previnam a instalação de aplicações não

autorizadas por parte dos utilizadores. Existem **Ações (AC),** a relacionar esse requisito em 2 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 2.2 - Assegurar que o Software Autorizado seja Atualmente Suportado IG1

**Tipo de Ativo:** Aplicações

**Função de Segurança:** Identificar

Este controlo envolve assegurar que apenas o *software* atualmente suportado seja assinalado como autorizado no inventário de *software* para os ativos corporativos. Se o *software* não é suportado, mas é necessário para o cumprimento da missão da empresa, deve ser documentada uma exceção detalhando os controlos de mitigação e a aceitação do risco residual. Para qualquer *software* não suportado sem uma documentação de exceção, deve ser assinalado como não autorizado. Analisar o inventário de *software* para verificar o suporte do *software* pelo menos uma vez por mês ou com maior frequência.

**Medida de Segurança:** 2.3 - Endereçar o Software Não Autorizado IG1

**Tipo de Ativo:** Aplicações

**Função de Segurança:** Responder

Este controlo assegura que o *software* não autorizado seja retirado de uso em ativos corporativos ou possua uma exceção documentada. Deve-se analisar mensalmente ou com mais frequência para identificar e resolver quaisquer instâncias de *software* não autorizado.

Ao conceder acesso a equipamentos de forma aleatória para testar a instalação de um *software* não autorizado, a organização demonstra conformidade com as medidas do Selo Digital.

O SMD, define o **T.RAR-1 - Recolha e armazenamento de registos -** A organização deve garantir a salvaguarda dos registos dos sistemas operativos e das aplicações de suporte à atividade. A medida do Selo Digital visa garantir a disponibilidade e integridade dos registos produzidos pelos sistemas operativos e pelas aplicações de suporte à atividade, os quais são essenciais para análise e investigação de incidentes de cibersegurança. Existem **Ações (AC),** a relacionar esse requisito em 3 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 8.1 - Estabelecer e Manter um Processo de Gestão de Log de Auditoria IG1

**Tipo de Ativo:** Rede

**Função de Segurança:** Proteger

Este controlo envolve estabelecer e manter um processo de gestão de *log* de auditoria que defina os requisitos de *log* da empresa, incluindo a recolha, revisão e retenção de *logs* de auditoria para ativos corporativos. É essencial para garantir que os registos estejam disponíveis quando necessário para análise e investigação de incidentes.

**Medida de Segurança:** 8.2 - Recolher Logs de Auditoria IG1

**Tipo de Ativo:** Rede

**Função de Segurança:** Detetar

Este controlo aborda a necessidade de recolher *logs* de auditoria, garantindo que o *log* esteja ativado em todos os ativos. Isso assegura que eventos importantes sejam registados para permitir a deteção e resposta a incidentes de segurança.

**Medida de Segurança:** 8.3 - Garantir o Armazenamento Adequado do Registo de Auditoria IG1

**Tipo de Ativo:** Rede

**Função de Segurança:** Proteger

Este controlo visa garantir que o destino dos *logs* contenha o armazenamento adequado para cumprir o processo de gestão de *log* de auditoria da empresa. É fundamental para assegurar que os registos estejam protegidos contra alterações não autorizadas e que possam ser recuperados quando necessário para análise ou investigação.

Ao demonstrar a visualização do repositório central de registos ou a salvaguarda dos registos dos sistemas identificados como críticos, a organização evidencia a conformidade com as medidas do Selo Digital.

### 5.2.3. Área Humana

O SMD, define o **H.PF-3 - Plano de formação -** a organização deve estabelecer um plano de ações de formação em segurança da informação e cibersegurança, bem como definir os processos e procedimentos necessários par garantir a sua correta implementação. A medida do Selo Digital focada na formação avançada de colaboradores com perfis técnicos busca capacitar esses profissionais com conhecimentos mais especializados em cibersegurança. Existem **Ações (AC),** a relacionar esse requisito em 6 medidas de segurança do *CIS Controls*:

**Medida de Segurança:** 14.3 - Treinar Membros da Força de Trabalho nas Melhores Práticas de Autenticação IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Proteger

Este controlo envolve a preparação dos membros da força de trabalho nas melhores práticas de autenticação, como MFA (Autenticação Multifator) e gestão de credenciais. Isso visa fortalecer a segurança das contas e proteger contra acessos não autorizados.

**Medida de Segurança:** 14.4 - Treinar a Força de Trabalho nas Melhores Práticas de Tratamento de Dados IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Proteger

Este controlo aborda a preparação dos colaboradores sobre como identificar, armazenar, transferir, arquivar e destruir dados sensíveis adequadamente, garantindo o manuseio seguro dos dados e prevenindo exposições não autorizadas.

**Medida de Segurança:** 14.5 - Treinar Membros da Força de Trabalho sobre as Causas da Exposição Não Intencional de Dados IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Proteger

Este controlo envolve a preparação dos membros da força de trabalho para estarem cientes das causas da exposição não intencional de dados. Isso inclui orientar os colaboradores sobre situações como entrega incorreta de dados sensíveis, perda de dispositivos portáteis ou publicação de dados para públicos não autorizados. O objetivo é promover uma maior conscientização sobre as práticas que podem levar à exposição de dados e prevenir incidentes de segurança.

**Medida de Segurança:** 14.6 - Treinar Membros da Força de Trabalho sobre o Reconhecimento e Comunicação de Incidentes de Segurança IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Proteger

Esse controlo visa capacitar os colaboradores a reconhecerem potenciais incidentes de segurança e a comunicá-los adequadamente, facilitando uma resposta rápida e eficaz a ameaças cibernéticas.

**Medida de Segurança:** 14.7 - Treinar a Força de Trabalho sobre os Perigos de se Conectar e Transmitir Dados Corporativos em Redes Inseguras IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Proteger

Este controlo envolve a preparação dos colaboradores sobre os riscos associados à conexão e transmissão de dados em redes inseguras, fornece orientações para garantir a segurança das conexões, especialmente para funcionários remotos.

**Medida de Segurança:** 14.8 - Treinar a Força de Trabalho sobre os Perigos de se Ligar e Transmitir Dados Corporativos em Redes Inseguras IG1

**Tipo de Ativo:** N/A

**Função de Segurança:** Proteger

Este controlo envolve preparar os membros da força de trabalho sobre os perigos associados a conectar e transmitir dados em redes inseguras para atividades corporativas. Deve ser dada especial atenção se a empresa tiver utilizadores remotos, incluindo orientações para garantir que todos os utilizadores configurem adequadamente a sua infraestrutura de rede doméstica. O objetivo é conscientizar os utilizadores sobre os riscos de segurança associados à utilização de redes não confiáveis para proteger os dados corporativos contra exposição não autorizada.

A evidência a ser apresentada para esta medida inclui entrevistas aleatórias a membros da organização com perfis técnicos, visando avaliar a eficácia do plano de formação e partilhando a documentação que registar a assiduidade e avaliação dos participantes.

## 5.3. Mapeamento Nível Ouro

O Nível Ouro não foi mapeado pois existem medidas de cibersegurança que, devido à sua natureza e complexidade, podem não ser consideradas viáveis para serem implementadas e avaliadas em todo o tipo de PMEs. Destacam-se alguns desses controlos definidos no Nível Ouro e justifica-se o porquê de não terem sido consideradas relevantes para empresas de menor dimensão, que constituem o foco deste questionário:

- **O.AGR - Análise e Gestão de Risco:** a análise e gestão de risco são fundamentais para qualquer organização, mas para as PMEs e devido à complexidade e aos recursos necessários para conduzir uma análise abrangente podem ser excessivos. Para além da análise inicial, como em qualquer outra medida à necessário mantê-la atualizada e de uma forma geral as PMEs possuem recursos limitados, tornando difícil dedicar os recursos necessários para realizar uma análise de risco completa.
- **O.SOC - Centro de Operações de Segurança (SOC):** A implementação de um SOC requer investimentos significativos em tecnologia, pessoas e infraestrutura. Para PMEs, que geralmente têm orçamentos mais restritos, a criação e manutenção de um SOC pode ser financeiramente inviável e desnecessário para suas operações, ou então podem possuir um "falso SOC", que não tem a abrangência nem o tempo de resposta necessário para identificar e conter uma ameaça.

- **O.PCN - Plano de Continuidade de Negócios:** Todas as empresas devem ter um plano de continuidade de negócios, mas devido à sua extensão e à complexidade do plano vai apenas ser relevante consoante o tamanho e a natureza da organização. Para PMEs, um plano mais simplificado (com um bom sistema de cópias de segurança) e focado nas principais áreas, pode ser mais adequado do que um plano abrangente que aborda todos os aspetos da continuidade de negócios.
- **T.RSC - Redundância de Sistemas Críticos:** A implementação de redundância de sistemas críticos pode ser excessivamente dispendiosa e complexa para PMEs, que muitas vezes operam com sistemas de TI mais simples.
- **T.TSA - Testes de Segurança e de Aceitação de Serviços:** Embora seja importante testar a segurança dos sistemas e serviços, os testes formais podem ser excessivamente complexos e dispendiosos para PMEs, que muitas vezes não possuem os recursos técnicos ou financeiros para conduzir esses testes de maneira eficaz.
- **T.TRI - Testes de Resposta a Incidentes de Segurança:** Embora seja crucial ter procedimentos de resposta a incidentes, a complexidade dos testes formais de resposta a incidentes pode ser desproporcional para PMEs, que muitas vezes operam com equipas menores e recursos limitados.
- **H-EC - Realização de Exercícios de Avaliação de Cibersegurança:** Os exercícios de avaliação de cibersegurança são importantes para testar a prontidão e capacidade de resposta da organização, mas a sua implementação e coordenação podem ser desafiadoras para PMEs, que muitas vezes têm menos recursos e experiência em cibersegurança.

Todas estas medidas de cibersegurança são essenciais para organizações de maior dimensão, mas para empresas com recursos limitados, como as PMEs, a implementação e avaliação de tais controlos podem não ser práticas ou adequadas devido à sua dimensão e capacidade operacional limitada. É importante adaptar a avaliação da cibersegurança às necessidades e realidades específicas das PMEs, garantindo que os controlos e práticas recomendadas sejam viáveis e eficazes para proteger seus ativos e operações contra ameaças.

## 5.4. Mapeamento Final

Tendo sido o mapeamento um processo crítico que envolveu a análise das exigências do SMD em Cibersegurança e a correspondência desses requisitos com os controlos e *safeguards* detalhadas no *CIS Controls*. Na Figura 19 apresenta-se o resultado final dessa integração. Neste mapeamento do lado do SMD em Cibersegurança apresenta-se a referência da medida, a sua área de incidência e o tipo de correlação efetuada entre ambos, já do lado do *CIS Controls* apresenta-se o número da *safeguard* utilizada, a função de segurança e o IG a que pertence.

**Bronze**

| Referência Selo | Área | Tipo de Correlação | Safeguard CIS | Função de Segurança | Grupo |
|---|---|---|---|---|---|
| O.ID-1 | Organizacional | AL | 3.2 | Identificar | IG1 |
| O.IAC-1 | Organizacional | AC | 1.1 | Identificar | IG1 |
| | | AC | 2.1 | Identificar | IG1 |
| | | AC | 12.4 | Identificar | IG2 |
| O.PUA-1 | Organizacional | AM | Politica | PUA | |
| O.RSI-1 | Organizacional | AC | 17.1 | Responder | IG1 |
| | | AC | 17.2 | Responder | IG1 |
| T.CS-1 | Técnica | AC | 11.1 | Recuperar | IG1 |
| | | AC | 11.2 | Recuperar | IG1 |
| | | AC | 11.3 | Proteger | IG1 |
| | | AC | 11.4 | Recuperar | IG1 |
| T.AS-1 | Técnica | AC | 7.3 | Proteger | IG1 |
| | | AC | 7.4 | Proteger | IG1 |
| T.PPT-1 | Técnica | AC | 10.1 | Proteger | IG1 |
| | | AC | 10.2 | Proteger | IG1 |
| T.PPI-1 | Técnica | AC | 4.4 | Proteger | IG1 |
| | | AC | 4.5 | Proteger | IG1 |
| | | AC | 4.6 | Proteger | IG1 |
| | | AC | 4.7 | Proteger | IG1 |
| | | AC | 12.2 | Proteger | IG2 |
| T.CWC-1 | Técnica | AC | 9.5* | Proteger | IG2 |
| T.AM-1 | Técnica | AC | 6.3 | Proteger | IG1 |
| | | AC | 6.4 | Proteger | IG1 |
| | | AC | 6.5 | Proteger | IG1 |
| H.PF-1 | Humana | AC | 14.1 | Proteger | IG1 |
| H.PF-2 | Humana | AC | 14.2 | Proteger | IG1 |
| H.FIC-1 | Humana | AL | 17.3 | Responder | IG1 |

* utilizado numa medida do nível Prata

**Prata**

| Referência Selo | Área | Tipo de Correlação | Safeguard CIS | Função de Segurança | Grupo |
|---|---|---|---|---|---|
| O.PP-1 | Organizacional | AC | 5.2 | Proteger | IG1 |
| O.PAP-1 | Organizacional | AC | 5.1 | Identificar | IG1 |
| | | AC | 3.3 | Proteger | IG1 |
| O.GMO-1 | Organizacional | AC | 6.1 | Proteger | IG1 |
| | | AC | 6.2 | Proteger | IG1 |
| O.PRI-1 | Organizacional | AC | 17.4 | Responder | IG2 |
| T.CWC-2 | Técnica | AC | 9.5* | Proteger | IG2 |
| T.GP-1 | Técnica | AM | Politica | Passwords | |
| T.PAD-1 | Técnica | AC | 5.4 | Proteger | IG1 |
| T.SC-1 | Técnica | AC | 3.6 | Proteger | IG1 |
| | | AC | 4.1 | Proteger | IG1 |
| | | AC | 4.2 | Proteger | IG1 |
| | | AC | 4.3 | Proteger | IG1 |
| | | AC | 9.1 | Proteger | IG1 |
| T.CA-1 | Técnica | AC | 2.2 | Identificar | IG1 |
| | | AC | 2.3 | Responder | IG1 |
| T.RAR-1 | Técnica | AC | 8.1 | Proteger | IG1 |
| | | AC | 8.2 | Detetar | IG1 |
| | | AC | 8.3 | Proteger | IG1 |
| H.PF-3 | Humana | AC | 14.3 | Proteger | IG1 |
| | | AC | 14.4 | Proteger | IG1 |
| | | AC | 14.5 | Proteger | IG1 |
| | | AC | 14.6 | Proteger | IG1 |
| | | AC | 14.7 | Proteger | IG1 |
| | | AC | 14.8 | Proteger | IG1 |

* utilizado numa medida do nível Bronze

**Figura 19 – Mapeamento final das medidas do SMD com o *CIS Controls***

Neste mapeamento foram utilizadas um total de 45 *safeguards* IG1, reconhecendo a sua importância fundamental na proteção dos ativos e dados das PMEs. Além disso, foram incorporadas 4 *safeguards* do IG2, visando abordar aspetos mais avançados e específicos de cibersegurança. Complementando essas *safeguards*, foram incluídas também 2 políticas, proporcionando uma estrutura sólida e direcionada para orientar as práticas de cibersegurança dentro das PMEs avaliadas.

## 5.5. Questionário

Nesta secção, é detalha a estrutura do questionário, explicando a organização das perguntas e as opções de resposta. É abordado também as duas opções de análise através da abordagem pela divisão por funções de segurança, conforme definido pelo *CIS Controls*, e a divisão por áreas, de acordo com o SMD em Cibersegurança. Esta segmentação permite uma análise agregada dos resultados, possibilitando uma compreensão das áreas e funções que apresentam melhores e piores desempenhos. Com base nestes dados, será possível definir estratégias de melhoria direcionadas e para as áreas que mais necessitam.

### 5.5.1. Estrutura

Após a conclusão do mapeamento final entre SMD em Cibersegurança e o *CIS Controls*, foi possível produzir um questionário detalhado. Este foi estruturado para abranger as áreas

relevantes identificadas durante o mapeamento. As perguntas foram construídas de forma a avaliar o nível de implementação das *safeguards* do *CIS Controls* dentro das empresas, assegurando uma avaliação o mais detalhada possível.

O questionário foi organizado em torno das cinco funções de segurança delineadas pelo *CIS Controls*: Identificar, Proteger, Detetar, Responder e Recuperar. Para garantir que os participantes compreendiam o contexto de cada área abordada, o questionário fornece uma breve explicação sobre cada uma das funções de segurança.

Na versão final do questionário existiram 3 *safeguards* do *CIS Controls*, que foram agregadas apenas numa questão, classificada com o tipo Detetar, uma vez que estão relacionadas com os *logs,* nomeadamente:

- *safeguard* 8.1 - Estabelecer e manter um processo de gestão de *log* de auditoria
- *safeguard* 8.2 - Recolher *logs* de auditoria
- *safeguard* 8.3 - Garantir o armazenamento adequado do registo de auditoria

Já a *safeguard* 14.3 - Treinar membros da força de trabalho nas melhores práticas de autenticação, também foi excluída do mesmo, devido à sua semelhança com outras questões da área Humana.
Já as medidas do SMD em Cibersegurança **T.CWC-1** e **T.CWC-2,** foram agregadas apenas numa questão, uma vez que remetiam para o mesmo *safeguard* 9.5 - Implementar o DMARC.

### 5.5.2. Opções de Resposta

A tomada de decisão que definiu apenas utilizar apenas três níveis de resposta ao questionário pretendeu-se com fornecer simplicidade e clareza, e uma redução da complexidade das respostas por forma a facilitar a sua compreensão e utilização por parte das organizações. Ao limitar o número de níveis, torna-se mais fácil para as empresas entenderem o seu posicionamento em termos da avaliação da sua maturidade e identificar lacunas em relação às práticas recomendadas. A utilização dos três níveis pode também parecer simplista, mas ela reflete uma abordagem pragmática para evitar interpretações ambíguas ou nuances sutis nos resultados da avaliação. Isso ajuda a evitar confusões e discrepâncias na interpretação dos dados, garantindo uma análise mais precisa e consistente.

**Tabela 12 – Níveis de avaliação**

| Nível | Avaliação | % para a classificação |
|---|---|---|
| 1 | Não responde | 0% |
| 2 | Responde parcialmente | 50% |
| 3 | Responde totalmente | 100% |

De acordo com a Tabela 12, permite uma avaliação clara do nível de conformidade da empresa com os controlos, fornecendo uma representação visual das respostas e atribuindo um valor percentual que quantifica o grau de implementação das medidas de segurança.

- Responde totalmente (**Verde**): Esta opção indica que a empresa implementa totalmente o controlo conforme especificado, onde as medidas recomendadas foram adotadas e estão em pleno funcionamento. A percentagem atribuída a essa opção é de 100%, indicando que todas as medidas foram implementadas conforme o esperado.
- Responde parcialmente (**Amarelo**): Esta opção indica que a empresa implementou parcialmente o controlo, mas não totalmente conforme especificado. Algumas medidas foram adotadas, mas outras podem estar em falta ou não foram implementadas conforme as recomendações. A percentagem atribuída a essa opção é de 50%, indicando que apenas metade das medidas foram implementadas.
- Não responde (**Vermelho**): Esta opção indica que a empresa não implementou ou não colocou em prática nenhuma das medidas recomendadas. A percentagem atribuída a essa opção é de 0%, indicando que nenhuma das medidas foi implementada.

### 5.5.3. Divisão do Questionário por Funções de Segurança

O questionário está dividido e ordenado pelas 5 funções de segurança do *CIS Controls*: Identificar; Proteger; Detetar; Responder e Recuperar. Verifica-se que o mesmo não possuí uma divisão uniforme em cada umas das funções como é possível ver na Tabela 13 e na Figura 20, o mesmo foi o resultado do mapeamento efetuado, o que indica que o *CIS Controls* tem preponderâncias diferentes nas várias funções de segurança.

**Tabela 13 – Distribuição das questões *CIS Controls***

| Função de Segurança | Questões | % |
|---|---|---|
| **Identificar** | 6 | 12% |
| **Proteger** | 34 | 68% |
| **Detetar** | 1 | 2% |
| **Responder** | 6 | 12% |
| **Recuperar** | 3 | 6% |

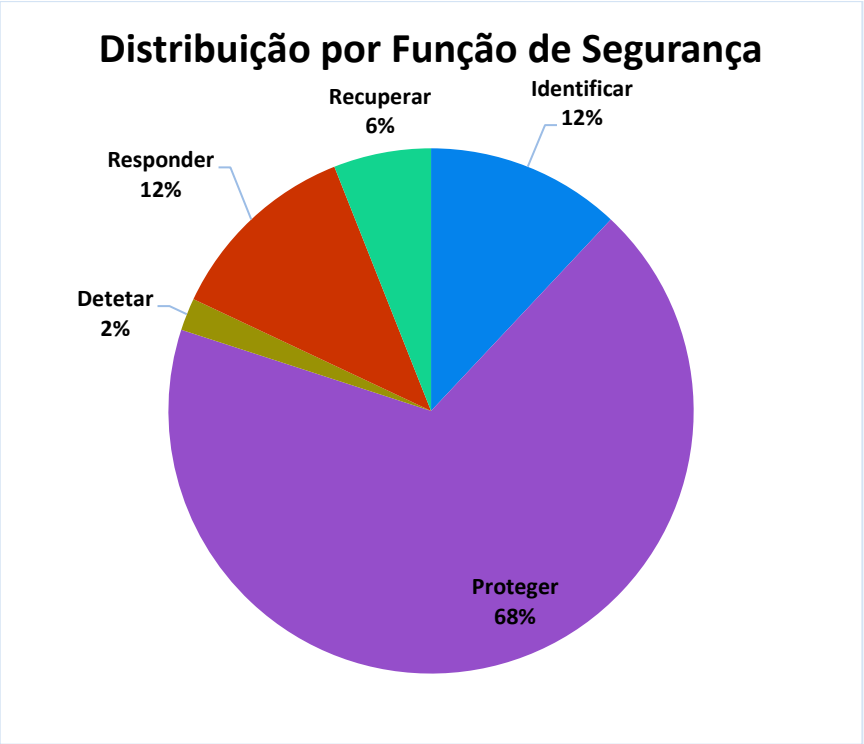



**Figura 20 – Distribuição das questões por Função de Segurança**

A função **Identificar -** apresenta 6 questões, representando 12% do total. Esta aborda a capacidade de uma organização de identificar e avaliar ativamente as ameaças à cibersegurança.

A função **Proteger -** domina a distribuição, com 34 questões, representando 68% do total. Destaca a importância atribuída à implementação de medidas de proteção para garantir a segurança dos sistemas e dados.

A função **Detetar –** possuí apenas 1 questão, representando 2% do total. A função de detetar é a menos representada na distribuição. A deteção precoce de ameaças é fundamental para minimizar o impacto de ataques.

A função **Responder -** apresenta 6 questões, representando 12% do total. Esta aborda a capacidade de uma organização de responder de maneira eficaz a incidentes, mais foco e investimento em capacidades de resposta a incidentes.

A função **Recuperar -** apresenta 3 questões, representando 6% do total. Abordando a capacidade de uma organização de recuperar-se de incidentes de cibersegurança e restaurar a operação normal.

### 5.5.4. Divisão do questionário por Áreas

Fazendo a relação com as 3 áreas: Organizacional, Técnica e Humana do SMD em Cibersegurança, verificamos que a área Técnica engloba mais questões comparativamente às outras 2 áreas juntas, como é possível observar na Tabela 14 e na Figura 21.

**Tabela 14 – Distribuição das questões por área de incidência dos Selos**

| Área | Questões | % |
|---|---|---|
| **Organizacional** | 13 | 26% |
| **Técnica** | 28 | 56% |
| **Humana** | 9 | 18% |

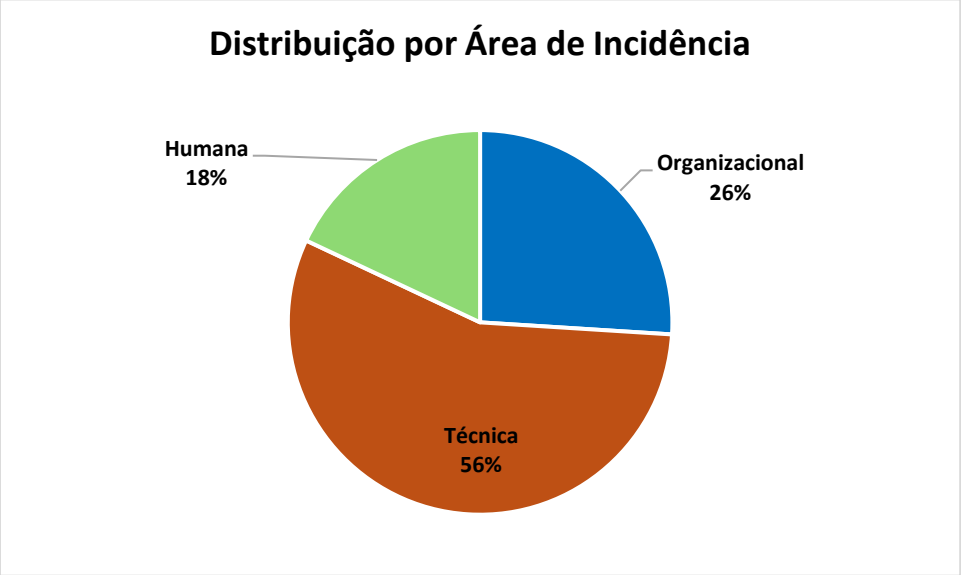



**Figura 21 – Distribuição das questões por Área de Incidência do SMD de Cibersegurança**

**Organizacional** - Com 13 questões, representando 26% do total, a área organizacional constitui uma parte significativa das preocupações em cibersegurança. Esta área inclui aspetos como políticas de segurança, *governance*, gestão de riscos e conformidade. A representação desta área sugere o reconhecimento da importância de estruturas organizacionais sólidas na implementação eficaz de medidas de cibersegurança.

**Técnica** - Com 28 questões, representando 56% do total, a área técnica domina a distribuição, indicando sua centralidade nas preocupações em cibersegurança. Esta área abrange tecnologias, sistemas de segurança, arquitetura de rede, criptografia e medidas técnicas de proteção. A predominância da área técnica destaca a necessidade crítica de investimento em infraestrutura e soluções tecnológicas para garantir a segurança dos sistemas e dados.

**Humana** - Com apenas 9 questões, representando 18% do total, a área humana é a menos representada na distribuição. Esta área aborda questões relacionadas à conscientização do utilizador, formação em cibersegurança, engenharia social e comportamento. Embora

menos numerosa, a importância da área humana não deve ser subestimada, pois os aspetos comportamentais e de conscientização desempenham um papel crucial na prevenção de ciberataques.

O questionário composto pelas 50 questões, encontra-se disponível no Anexo A.

# 6. Análise de Resultados

O estudo envolveu a participação de um total de 21 PMEs, da Zona Centro, de diversos sectores de atividade económica como: indústria extrativa; comércio; produção industrial; transformação alimentar; serviços e transportes. Como indicado no Perfil das Empresas referenciado na Secção 4.2.2, o inquérito foi enviado para um grupo de empresas com pessoas responsáveis dos departamentos de IT, com competências e conhecimentos na área informática, para que assim pudessem responder ao questionário tendo conhecimento técnico para tal. Em nenhum dos casos existiu acompanhamento no preenchimento para evitar algum tipo de condicionalismo nas respostas.

## 6.1. Resultados dos Questionários

O resultado deste questionário advém da participação voluntária das empresas, e neste procura-se partilhar os resultados de forma transparente e objetiva. Através da análise das respostas fornecidas, destacam-se as principais conclusões, tendências e recomendações identificadas ao longo do processo. Com estes resultados, pretende-se fornecer uma visão do panorama de cibersegurança de uma amostra representativa de PMEs do tecido empresarial português. A análise dos resultados é fundamental para orientar ações e estratégias de melhoria, capacitando as organizações para enfrentar desafios e apontar as áreas onde existe uma maior lacuna, por forma, a responder às ameaças cada vez mais complexas e dinâmicos do ambiente digital.

Para garantir a anonimização dos dados das empresas que responderam ao questionário, foi utilizada uma metodologia de codificação simples. A cada empresa foi atribuída uma letra do alfabeto como identificador único. As empresas participantes foram listadas sem qualquer ordenação específica para evitar qualquer possível identificação sequencial. A cada empresa na lista foi então atribuída a uma letra do alfabeto, começando pela letra **A** e seguindo em ordem alfabética (A, B, C, etc.). Nos dados recolhidos, a referência ao nome da empresa foi substituída pelo identificador da letra correspondente. Por fim nas tabelas, gráficos e relatórios, resultantes do inquérito, foram utilizadas apenas as letras atribuídas para referenciar as empresas, assegurando que a identidade das empresas permanecesse anónima.

Na Figura 22, são apresentados os resultados globais quantitativos por questão, associados a cada empresa, de acordo com o Nível apresentado anteriormente na Tabela 12.

| Empresa | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Identificar** | | | | | | | | | | | | | | | | | | | | | |
| I1 | 3 | 2 | 3 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 3 | 3 | 2 | 2 |
| I2 | 3 | 3 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 2 | 2 | 2 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 2 | 2 |
| I3 | 2 | 3 | 3 | 3 | 3 | 2 | 2 | 3 | 3 | 3 | 1 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 |
| I4 | 2 | 2 | 3 | 2 | 3 | 3 | 1 | 1 | 3 | 2 | 1 | 2 | 2 | 3 | 2 | 1 | 2 | 3 | 2 | 3 | 1 |
| I5 | 3 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 3 | 3 | 2 | 2 | 2 | 3 | 2 | 3 | 3 | 2 | 2 | 2 |
| I6 | 3 | 3 | 2 | 2 | 2 | 3 | 2 | 2 | 3 | 3 | 3 | 2 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 2 | 2 |
| **Proteger** | | | | | | | | | | | | | | | | | | | | | |
| P1 | 3 | 2 | 2 | 3 | 2 | 3 | 3 | 2 | 3 | 3 | 3 | 2 | 3 | 3 | 2 | 2 | 3 | 3 | 2 | 2 | 2 |
| P2 | 3 | 3 | 3 | 3 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | 1 |
| P3 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 2 | 2 | 2 | 3 | 3 | 2 | 3 | 3 | 3 | 2 | 2 |
| P4 | 2 | 2 | 3 | 3 | 3 | 3 | 2 | 2 | 3 | 2 | 1 | 2 | 1 | 3 | 3 | 2 | 3 | 3 | 2 | 2 | 1 |
| P5 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 3 | 3 |
| P6 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | 2 | 3 | 2 | 3 | 3 | 2 | 3 | 3 |
| P7 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 1 | 3 | 3 | 2 | 2 | 3 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 3 |
| P8 | 3 | 3 | 1 | 1 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | 1 | 3 | 2 | 3 | 2 | 3 | 3 | 2 | 3 | 3 |
| P9 | 3 | 3 | 2 | 3 | 2 | 3 | 2 | 3 | 3 | 3 | 2 | 1 | 2 | 2 | 1 | 2 | 2 | 3 | 3 | 2 | 3 |
| P10 | 3 | 3 | 3 | 3 | 2 | 3 | 2 | 2 | 3 | 3 | 2 | 1 | 3 | 2 | 3 | 2 | 2 | 3 | 3 | 2 | 2 |
| P11 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 2 | 2 | 3 | 2 | 3 | 3 | 3 | 2 | 2 |
| P12 | 3 | 2 | 3 | 2 | 3 | 2 | 2 | 3 | 3 | 3 | 3 | 1 | 3 | 2 | 2 | 2 | 3 | 3 | 2 | 2 | 3 |
| P13 | 3 | 3 | 2 | 2 | 2 | 2 | 3 | 1 | 2 | 3 | 1 | 1 | 3 | 1 | 1 | 2 | 3 | 3 | 3 | 1 | 2 |
| P14 | 2 | 3 | 2 | 3 | 3 | 2 | 2 | 1 | 2 | 3 | 1 | 1 | 2 | 2 | 1 | 2 | 3 | 2 | 2 | 2 | 2 |
| P15 | 3 | 1 | 3 | 3 | 3 | 1 | 2 | 1 | 2 | 3 | 1 | 1 | 2 | 1 | 1 | 3 | 3 | 2 | 3 | 2 | 3 |
| P16 | 2 | 2 | 3 | 3 | 3 | 1 | 2 | 1 | 3 | 3 | 1 | 1 | 2 | 2 | 1 | 1 | 3 | 2 | 2 | 2 | 3 |
| P17 | 3 | 3 | 3 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 1 | 2 |
| P18 | 2 | 3 | 1 | 1 | 2 | 2 | 2 | 2 | 2 | 2 | 2 | 1 | 1 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 2 |
| P19 | 3 | 3 | 2 | 3 | 2 | 3 | 2 | 3 | 3 | 3 | 3 | 1 | 1 | 3 | 3 | 2 | 3 | 3 | 2 | 3 | 3 |
| P20 | 3 | 3 | 3 | 3 | 2 | 1 | 3 | 3 | 3 | 3 | 3 | 1 | 2 | 2 | 3 | 1 | 3 | 2 | 3 | 2 | 2 |
| P21 | 3 | 3 | 3 | 3 | 2 | 3 | 1 | 3 | 3 | 3 | 3 | 1 | 1 | 3 | 3 | 2 | 3 | 3 | 2 | 2 | 2 |
| P22 | 3 | 2 | 3 | 3 | 3 | 3 | 1 | 2 | 3 | 3 | 3 | 1 | 1 | 3 | 3 | 2 | 3 | 3 | 2 | 2 | 2 |
| P23 | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 3 | 2 | 1 | 2 | 2 | 2 | 1 | 3 | 3 | 2 | 1 | 2 |
| P24 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 1 | 2 | 2 | 3 | 1 | 3 | 3 | 2 | 3 | 3 |
| P25 | 3 | 3 | 1 | 1 | 3 | 2 | 1 | 3 | 2 | 3 | 3 | 2 | 2 | 3 | 2 | 2 | 3 | 3 | 2 | 2 | 3 |
| P26 | 3 | 3 | 2 | 2 | 2 | 3 | 2 | 2 | 2 | 3 | 2 | 1 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 2 |
| P27 | 3 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 2 | 3 | 3 | 1 | 2 | 2 | 3 | 2 | 3 | 3 | 2 | 3 | 2 |
| P28 | 3 | 3 | 3 | 3 | 3 | 3 | 1 | 3 | 2 | 3 | 3 | 1 | 2 | 3 | 3 | 1 | 3 | 3 | 3 | 2 | 3 |
| P29 | 3 | 2 | 2 | 3 | 2 | 3 | 2 | 2 | 2 | 1 | 3 | 1 | 1 | 2 | 3 | 1 | 2 | 2 | 2 | 2 | 1 |
| P30 | 2 | 2 | 1 | 3 | 3 | 2 | 1 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 |
| P31 | 1 | 2 | 2 | 3 | 3 | 2 | 1 | 1 | 2 | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 |
| P32 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 1 | 2 | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 2 | 3 | 2 | 2 | 2 |
| P33 | 1 | 2 | 1 | 1 | 2 | 2 | 1 | 1 | 2 | 3 | 2 | 1 | 1 | 1 | 3 | 1 | 1 | 2 | 1 | 2 | 1 |
| P34 | 2 | 3 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | 3 | 3 | 1 | 2 | 2 | 2 | 1 | 2 | 2 | 2 | 2 | 2 |
| **Detetar** | | | | | | | | | | | | | | | | | | | | | |
| D1 | 2 | 2 | 1 | 1 | 3 | 3 | 1 | 1 | 2 | 3 | 3 | 1 | 2 | 1 | 1 | 1 | 2 | 3 | 2 | 1 | 2 |
| **Responder** | | | | | | | | | | | | | | | | | | | | | |
| R1 | 3 | 3 | 3 | 2 | 3 | 3 | 2 | 2 | 3 | 3 | 1 | 1 | 1 | 3 | 3 | 2 | 2 | 3 | 2 | 2 | 2 |
| R2 | 3 | 3 | 1 | 2 | 3 | 3 | 2 | 1 | 3 | 3 | 1 | 1 | 1 | 3 | 2 | 1 | 2 | 2 | 2 | 1 | 2 |
| R3 | 3 | 3 | 1 | 1 | 3 | 3 | 2 | 1 | 2 | 1 | 1 | 1 | 1 | 3 | 2 | 1 | 2 | 3 | 2 | 1 | 2 |
| R4 | 1 | 2 | 1 | 3 | 2 | 2 | 1 | 1 | 2 | 2 | 1 | 1 | 1 | 1 | 2 | 1 | 1 | 2 | 1 | 1 | 1 |
| R5 | 3 | 2 | 1 | 1 | 2 | 2 | 2 | 1 | 2 | 3 | 2 | 1 | 1 | 3 | 3 | 1 | 2 | 2 | 2 | 2 | 2 |
| R6 | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 | 2 | 2 | 3 | 1 | 2 | 2 | 3 | 1 | 2 | 3 | 2 | 2 | 2 |
| **Recuperar** | | | | | | | | | | | | | | | | | | | | | |
| Re1 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 2 | 2 | 3 | 3 | 3 | 3 | 3 | 3 | 3 | 2 |
| Re2 | 3 | 2 | 3 | 3 | 2 | 3 | 1 | 2 | 3 | 3 | 3 | 2 | 1 | 2 | 2 | 2 | 2 | 3 | 2 | 2 | 2 |
| Re3 | 3 | 3 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | 1 | 2 | 3 | 2 | 3 | 3 | 2 | 3 | 3 | 3 | 3 | 3 |

**Figura 22 – Resultado global das respostas**

A matriz representa assim um total de 1050 respostas, sendo que 165 (16%) das respostas correspondem ao Nível 1; 429 (41%) das respostas correspondem ao Nível 2 e 456 (43%) correspondem ao Nível 3, representado no gráfico da Figura 24.

| | Média |
|---|---|
| Nível 1 | 16% |
| Nível 2 | 41% |
| Nível 3 | 43% |

**Tabela 15 – Média de respostas por nível**

De verificar que o Nível 3, representa o maior número de respostas, sendo o único nível que cumpre integralmente os requisitos estabelecidos. Isso sugere que uma parcela significativa das organizações avaliadas demonstrou um nível alto de maturidade nas suas práticas de cibersegurança. As organizações que se autoavaliaram neste nível terão de ter implementados controlos de segurança e possuir processos robustos para proteger os seus ativos e dados contra ameaças. De realçar que o número de respostas com o Nível 1 acaba por conter a menor percentagem de respostas, o que indica que apenas uma pequena parte das organizações está num nível inicial de maturidade.

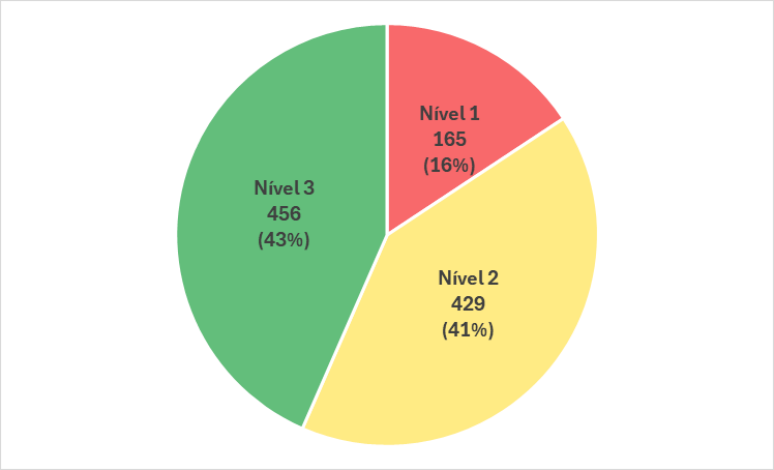



**Figura 23 – Total de respostas por Nível**

Na Figura 23, podemos observar a distribuição das respostas por nível, pelo conjunto de todas as empresas participantes.

Já no gráfico da Figura 24, é possível a percentagem de respostas por nível e por empresa.

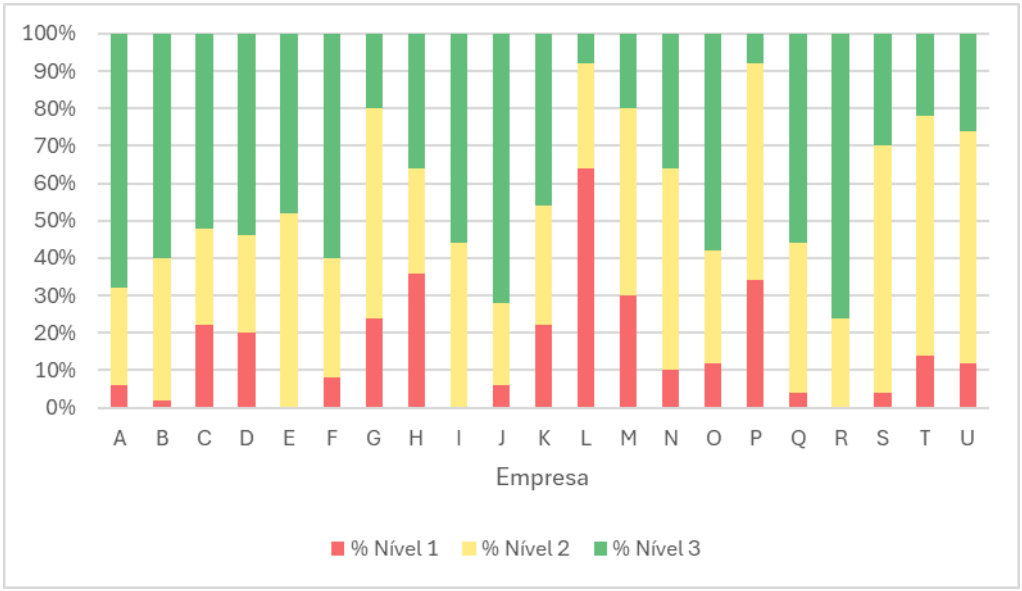



**Figura 24 – Gráfico das percentagens de respostas para cada empresa**

Fazendo uma análise da Tabela 16, verifica-se que existem apenas 10 empresas que apresentam mais de 50% das respostas no Nível 3, indicando um forte compromisso com a conformidade com os *CIS Controls*, correspondendo a metade dos requisitos de implementação. Pelo lado negativo verifica-se que existem 2 empresas com apenas 8% das repostas com o Nível 3.

Já numa análise para o Nível 1, identificam-se 3 empresas que apresentam mais de 33% de respostas do Nível 1, sendo que uma delas apresenta um total de respostas de Nível 1 de 64%.

**Tabela 16 – Percentagem de respostas para cada empresa**

| Empresa | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Nível 1 (Não Responde) | 6% | 2% | 22% | 20% | 0% | 8% | 24% | 36% | 0% | 6% | 22% | 64% | 30% | 10% | 12% | 34% | 4% | 0% | 4% | 14% | 12% |
| Nível 2 (Resp. Parcialmente) | 26% | 38% | 26% | 26% | 52% | 32% | 56% | 28% | 44% | 22% | 32% | 28% | 50% | 54% | 30% | 58% | 40% | 24% | 66% | 64% | 62% |
| Nível 3 (Resp. Totalmente) | 68% | 60% | 52% | 54% | 48% | 60% | 20% | 36% | 56% | 72% | 46% | 8% | 20% | 36% | 58% | 8% | 56% | 76% | 30% | 22% | 26% |

Na Figura 25, representa-se o resultado da avaliação global por empresa, utilizado o critério de classificação definido na Tabela 12, onde Nível 1 – 0%; Nível 2 – 50% e Nível 3 – 100%. Nesta análise global das avaliações por empresa observa-se um panorama variado de desempenho, onde a empresa **R**, apresenta um desempenho de 88% e a empresa **L** um desempenho de apenas 22%, sendo a média das empresas de 64%.

No desempenho geral, a média das avaliações sugere uma dispersão considerável no desempenho das empresas. Enquanto algumas empresas se destacam significativamente, outras enfrentam desafios críticos, de referenciar as empresas: **G** (48%), **H** (50%), **L** (22%), **M** (45%) e **P** (37%), que apresentam resultados igual ou abaixo dos 50%. Com um

desempenho médio entre 50% e 70%: encontram-se as empresas: **C** (65%), **D** (67%), **K** (62%), **N** (63%), **S** (63%), **T** (54%) e **U** (57%).

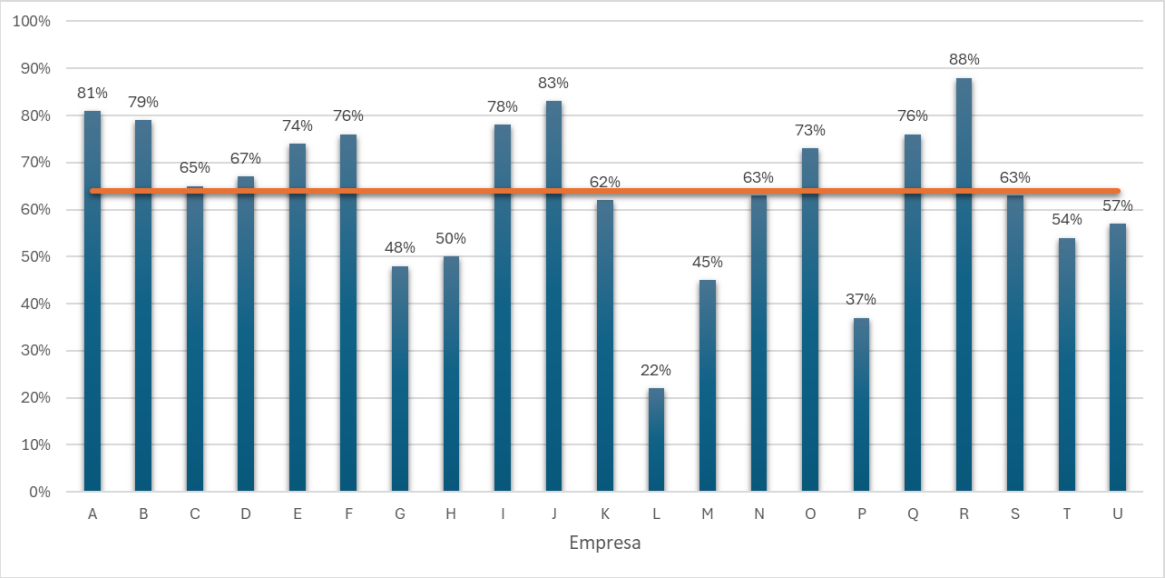



**Figura 25 – Gráfico da percentagem do resultado da avaliação por Empresa, com linha média**

Existem ainda 3 empresas com avaliações acima de 80%, a referenciar as empresas: **A** (81%), **J** (83%) e **R** (88%), podendo servir como *benchmark* para as restantes. Na Secção 6.2, realizada uma comparação entre a empresa **R** que obteve a pontuação mais elevada e os resultados médios obtidos.

De seguida apresenta-se uma análise mais refinada de acordo com os objetivos deste Estudo, onde será feita uma análise por Função de Segurança e Área de incidência.

### 6.1.1. Análise por Função de Segurança

No gráfico da Figura 26, pretende-se colocar o foco na análise das respostas pelas funções de segurança delineadas pelo *CIS Controls*. Esta abordagem permite uma visão de como as empresas participantes implementam e gerem as medidas, conforme os padrões estabelecidos pelos *CIS Controls.*

Assim, os dados indicam que a função de Recuperar obteve a pontuação mais alta, com uma média de 80%, seguida de Identificar com 69% e Proteger com 65%. Esses resultados sugerem uma ênfase maior das empresas na capacidade de recuperação de incidentes de segurança, seguida pela identificação e proteção de ativos e sistemas críticos.

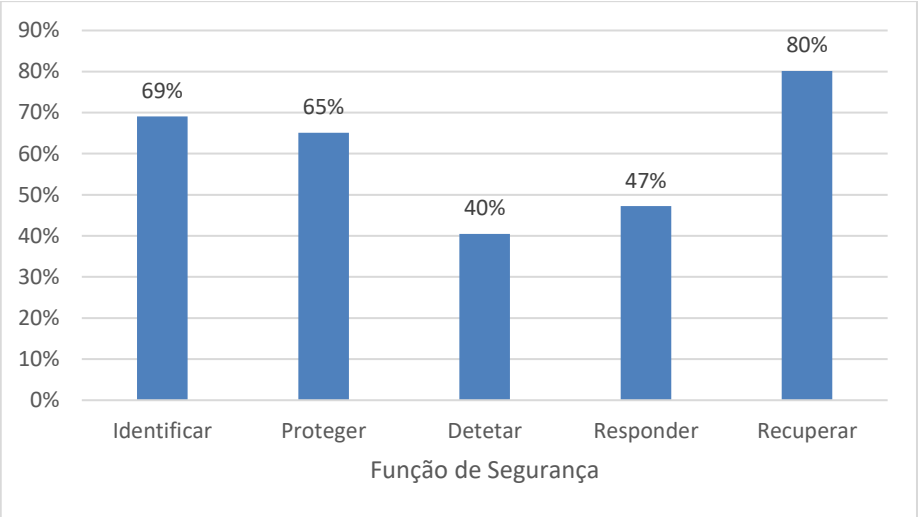



**Figura 26 – Gráfico da percentagem média da avaliação por Função de Segurança**

Por outro lado, as funções de Responder e Detetar apresentaram pontuações mais baixas, com médias de 47% e 40%, respetivamente, isso pode indicar uma menor prioritização por parte das empresas em termos de prontidão de deteção precoce de possíveis ameaças e em responder a incidentes de segurança, antes dos mesmos provocarem danos.

Os resultados sugerem que as empresas reconhecem a importância de investir em medidas de recuperação de incidentes e na identificação e proteção de ativos cruciais para as suas operações. No entanto, também destaca a necessidade de aumentar a atenção e os recursos direcionados para áreas como resposta a incidentes e deteção de ameaças, a fim de mitigar riscos potenciais.

Com base na análise do gráfico representado na Figura 27, podemos concluir que, em geral, a função de Recuperar obteve o melhor desempenho, com 65% das empresas a responder com o Nível 3. No extremo oposto, temos a função de Detetar teve o pior desempenho, com 43% das respostas a situarem-se no Nível 1.

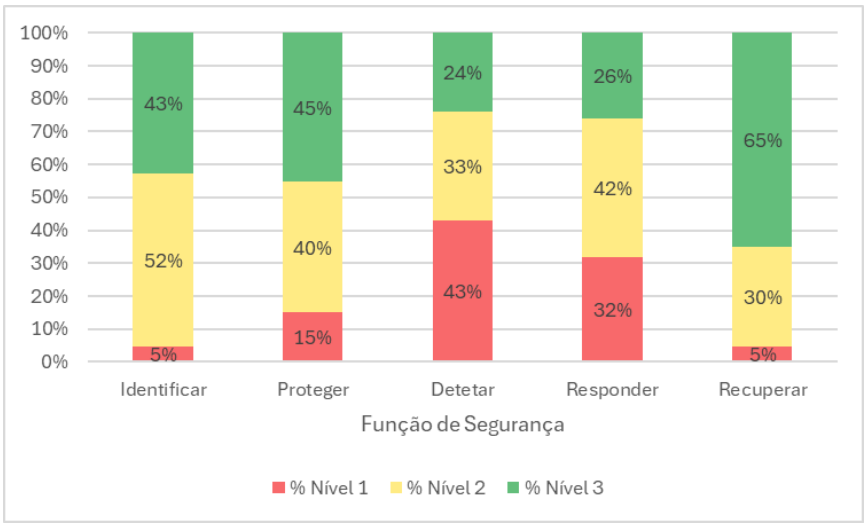



**Figura 27 – Gráfico da distribuição dos Níveis por Função de Segurança**

As funções Identificar e Proteger encontram-se muito semelhantes com o 43% e 45% respostas com o Nível 3, e curiosamente as funções de Detetar e Responder também apresentam resultados muito similares, correspondendo a 24% e 26% de respostas de Nível 3. Torna-se evidente que as empresas estão mais preocupadas com a fase de recuperar porque apenas 5% das respostas se encontram no Nível 1, sendo que têm mecanismos para executar uma recuperação em caso de ocorrência de um incidente de segurança.

Isso sugere que as organizações têm sido mais eficazes em planear e executar a recuperação após incidentes, mas podem precisar melhorar suas capacidades de deteção de ameaças.

**Identificar -** Sendo o processo de identificação de ameaças crucial para uma estratégia de cibersegurança eficaz, os dados revelam que a maioria das organizações está a identificar ameaças pelo menos num nível intermediário ou avançado (Níveis 2 e 3), indicando uma perceção considerável sobre os riscos.

**Proteger -** A implementação de medidas de proteção é essencial para mitigar os riscos. Os resultados mostram uma distribuição equilibrada entre os Níveis 2 e 3, sugerindo que muitas organizações estão adotando medidas sólidas para proteger os seus sistemas e dados.

**Detetar -** A capacidade de detetar ameaças de forma rápida e eficaz é crucial para minimizar o impacto dos ciberataques. Os dados revelam que neste ponto a quase maioria das organizações (43%) encontram-se no Nível 1. Isso destaca a necessidade de investimento em tecnologias e processos que permitam uma deteção proativa de ameaças.

**Responder -** Uma resposta eficaz a incidentes de cibersegurança é essencial para limitar os danos e restaurar a normalidade das operações. A maioria das organizações está posicionada nos Níveis 1 e 2 (32% e 42%) em termos de capacidade de resposta. Isso ressalta a importância de desenvolver e testar planos de resposta avançados para lidar com incidentes graves de cibersegurança.

**Recuperar -** A capacidade de recuperar após incidentes é crucial para garantir a continuidade do negócio. Os dados revelam uma concentração no Nível 3 (65%), indicando uma ênfase considerável na capacidade de recuperação.

Na análise dos resultados, segmentados por função de segurança do *CIS Controls,* revela que as empresas apresentam os piores resultados nas áreas de deteção e resposta. A incapacidade de detetar ameaças de maneira eficiente permite que ataques e atividades maliciosas permaneçam não identificados por períodos prolongados, aumentando a probabilidade de danos extensivos aos sistemas e dados da empresa. Além disso, a falta de uma resposta rápida e eficaz compromete a capacidade de mitigar os efeitos de incidentes de cibersegurança, resultando em maior tempo de inatividade, perda de dados e potenciais prejuízos financeiros e de reputação.

### 6.1.2. Análise por Área de Incidência

No gráfico representado na Figura 28, pretende-se analisar das respostas ao questionário com o foco nas 3 áreas de incidências dos SMD em Cibersegurança, esta avaliação, permite perceber como as empresas estão em cada uma das áreas. Assim, podemos concluir que, em geral, as áreas Técnica e Organizacional têm um desempenho muito próximo com 51% e 48% das empresas a responder com o Nível 3, respetivamente. Relativamente à área Humana, esta teve o pior desempenho, com 32% das respostas a situarem-se no Nível 1 e apenas 14% no Nível 3.

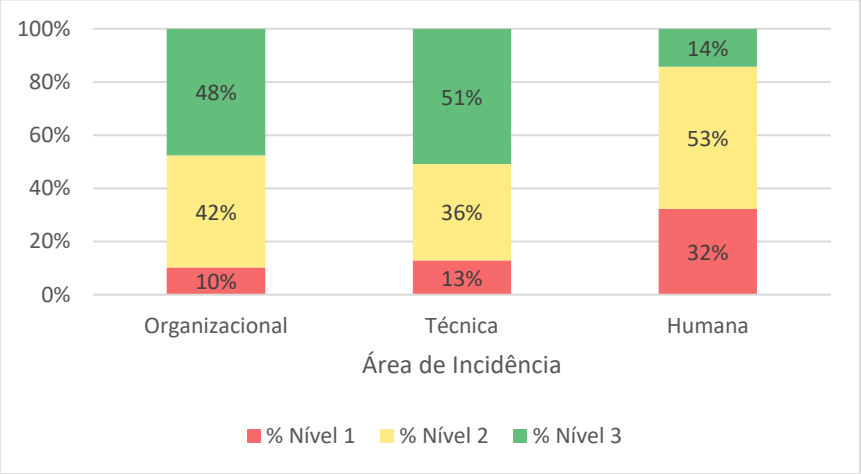



**Figura 28 – Gráfico da distribuição dos Níveis por Área de Incidência**

Numa análise um pouco mais detalhada:

**Organizacional -** observa-se que 10% das respostas estão no Nível 1, 42% estão no Nível 2 e 48% alcançaram o nível mais alto (Nível 3). Isso sugere um padrão positivo, com uma maioria significativa das empresas demonstrando um grau considerável de maturidade nas práticas organizacionais.

**Técnica** - os dados mostram que 13% das respostas estão no Nível 1, 36% no Nível 2 e 51% no Nível 3. Esses resultados indicam um desempenho semelhante ao da área Organizacional, mas com uma proporção maior de empresas atingindo o nível mais alto de maturidade.

**Humana** – aqui os dados revelam uma distribuição diferente, 32% das respostas estão no Nível 1, 53% no Nível 2 e apenas 14% no Nível 3. Isso sugere que, apesar de um bom desempenho nas áreas Organizacional e Técnica, muitas empresas enfrentam desafios significativos em termos de maturidade nas práticas relacionadas à dimensão humana da cibersegurança. A educação, a conscientização e a cultura de segurança digital podem ser áreas nas quais as empresas precisam investir mais esforços para melhorar sua postura geral de segurança.

Na Figura 29, apresentam-se os resultados médias por cada uma das 3 áreas, onde os dados indicam que as áreas Técnica e Organizacional obtiveram pontuações semelhantes, com médias de 69%. Isso sugere que as empresas reconhecem a importância tanto das medidas técnicas, quanto das práticas organizacionais, como políticas de segurança, para fortalecer sua postura de cibersegurança.

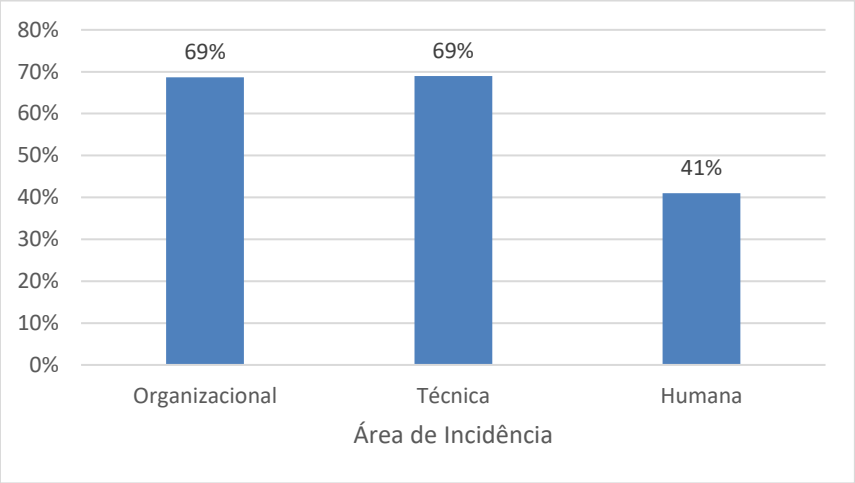



**Figura 29 – Gráfico da percentagem média da avaliação por Área de Incidência**

Por outro lado, a área Humana apresenta uma pontuação mais baixa, com um resultado de 41%. Isto sugere que as empresas podem não estar a dar a devida atenção às questões relacionadas à conscientização e formação dos colaboradores em cibersegurança. Sendo estes, frequentemente apontados como os elos mais vulneráveis na cadeia de segurança. Autores como Triplett [78], destacam a importância dos fatores humanos como um dos principais desafios para a cibersegurança. Estes fatores incluem a forma como os utilizadores interagem com sistemas de TI e os comportamentos suscetíveis que podem introduzir vulnerabilidades. Os erros humanos podem não ser intencionais, e resultantes de implementações estratégica inadequada ou da execução insuficiente dos planos.

Como resultado desta análise sugere que, embora as empresas estejam a investir em medidas técnicas e organizacionais de cibersegurança, ainda se verifica uma lacuna a ser preenchida na formação e conscientização dos utilizadores para mitigar os riscos, na componente humana. A CNCS[18] disponibiliza de forma gratuita e acessível na plataforma NAU[19], o curso Cidadão Ciberseguro direcionado para contextos pessoais e profissionais, onde são ensinadas boas práticas de ciberhigiene para proteger a navegação *online*. Não tendo sido possível encontrar dados oficiais referentes ao número de pessoas que concluíram com sucesso este curso, é possível verificar na plataforma, que até junho de 2024, existiu um total de 113.523 inscritos desde o seu lançamento em 2019. O que, na

[18] https://www.cncs.gov.pt/pt/cursos-e-learning/
[19] https://www.nau.edu.pt/

opinião do autor, é um número reduzido, tendo em conta a informação da Tabela 2 onde em Portugal em 2022 existiam 4.487.322 trabalhadores.

Outro aspeto relevante, e tendo em conta o âmbito das questões colocadas no questionário e os temas abordados, estes conteúdos são insuficientes, assim deve pode ser feito um trabalho adicional das organizações de standardização ou de apoio como o CNCS, de produzir mais recursos públicos e acessíveis, para auxiliar as empresas nesta tarefa, apresentando também um *roadmap* oficial capaz de preparar melhor os utilizadores por níveis de evolução.

Por fim, este trabalho não deve ser realizado apenas pelas empresas com foco nos adultos. O governo também pode implementar iniciativas de formação no ensino regular e obrigatório para os mais jovens, de forma a prepará-los desde cedo para os desafios da cibersegurança

## 6.2. Comparação dos Resultados Médios com a Empresa R

Sendo a empresa **R**, a que obteve melhores resultados na avaliação global do questionário, nesta Secção apresenta-se um trabalho comparativo dos resultados obtidos com a média das restantes empresas.

Assim ao comparar os resultados médios obtidos com a Empresa **R**, podemos identificar áreas de discrepância e oportunidades de melhoria em relação à média. A Figura 30, representa a comparação dos níveis das respostas da média das empresas com a empresa **R**. Numa análise comparativa da percentagem de resposta por nível entre a média das empresas e a Empresa **R** revela que, esta empresa, está claramente mais avançada em termos de maturidade de cibersegurança, com a maioria das suas respostas encontrarem-se no Nível 3 (76%) e nenhuma no Nível 1.

Esta análise comparativa permite identificar que existe uma implementação de mais medidas de cibersegurança da Empresa **R**, comparativamente a outras empresas.

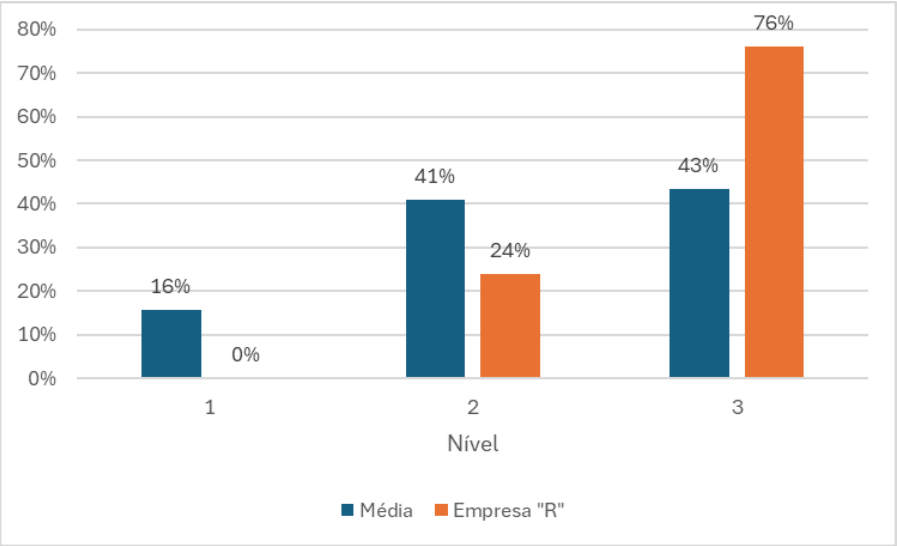



**Figura 30 – Comparação dos resultados médios com Empresa R**

Ao analisar os dados do gráfico da Figura 31, onde é apresentada a comparação média por Função de Segurança com a Empresa **R** podemos observar as pontuações médias para cada fase da segurança.

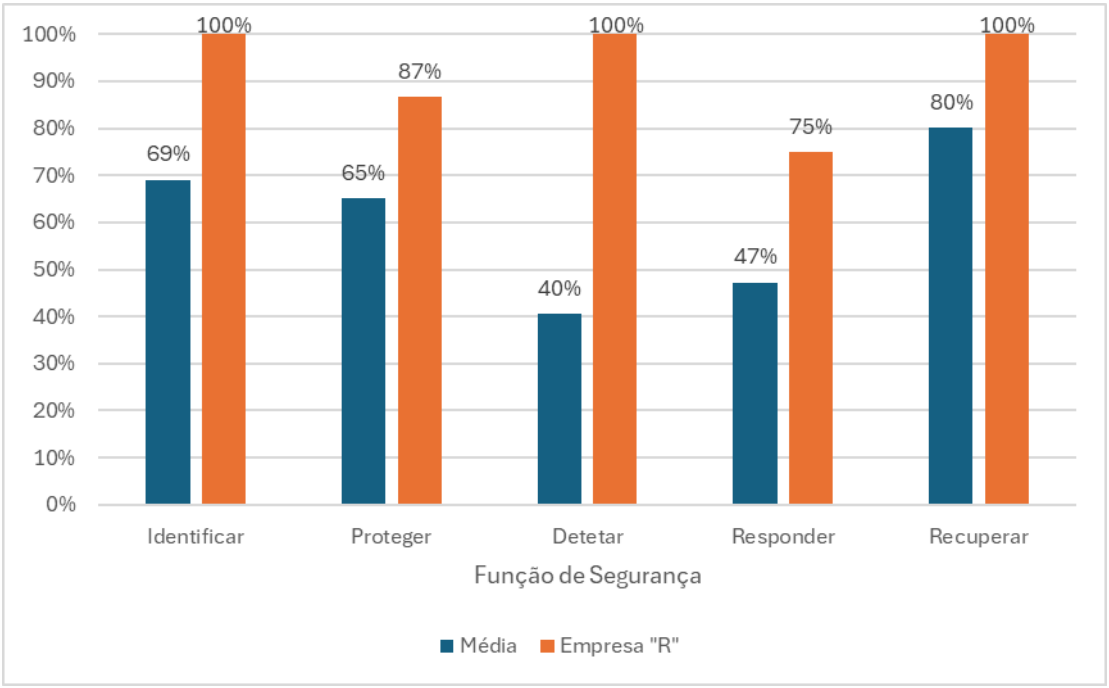



**Figura 31 – Comparação da percentagem média por Função de Segurança com a Empresa R**

**Identificar** - a Empresa **R** obteve uma pontuação 100% em comparação com a média geral de 69%, indicando uma compreensão mais clara das funções e atividades críticas em sua infraestrutura de TI.

**Proteger** – também nesta função a Empresa **R** destaca-se significativamente, obtendo uma pontuação consideravelmente maior 87% em comparação com a média geral 65%, sugere que a Empresa **R** possuí mais em medidas de proteção.

**Detetar** - a média de 40% é preocupantemente baixa, indicando que muitas empresas têm dificuldade em detetar ameaças de forma eficaz. Em contraste, a Empresa **R** atinge 100%, mostrando uma capacidade de deteção de ameaças.

**Responder** - a média de 47% revela que muitas empresas têm espaço para melhorar suas capacidades de resposta. A Empresa **R** apresenta um desempenho bem acima da média, com 75%, indicando uma capacidade de resposta.

**Recuperar** - ambas as médias foram relativamente altas, com a Empresa **R** 83% ligeiramente acima da média geral 80%, indicando uma boa capacidade de recuperação de sistemas e dados após incidentes de cibersegurança.

A análise dos dados revela que a Empresa **R** tem um desempenho alto em todas as funções de segurança do *CIS Controls*, atingindo 100% em Identificar, Detetar e Recuperar, e 87% e 75% em Proteger e Responder, respetivamente. Comparativamente, a média geral das empresas em cada função mostra que ainda há áreas significativas que necessitam de melhorias, especialmente em Detetar (40%) e Responder (47%).

Esta discrepância indica que, enquanto algumas empresas como a Empresa **R** estão na vanguarda das práticas de cibersegurança, a maioria das empresas precisa investir mais em suas capacidades de deteção e resposta para fortalecer sua postura de segurança geral.

A Figura 32, representa a análise dos dados de resposta ao questionário baseado nas três áreas de incidência do SMD em Cibersegurança, comparando a média das empresas com a média da empresa **R**.

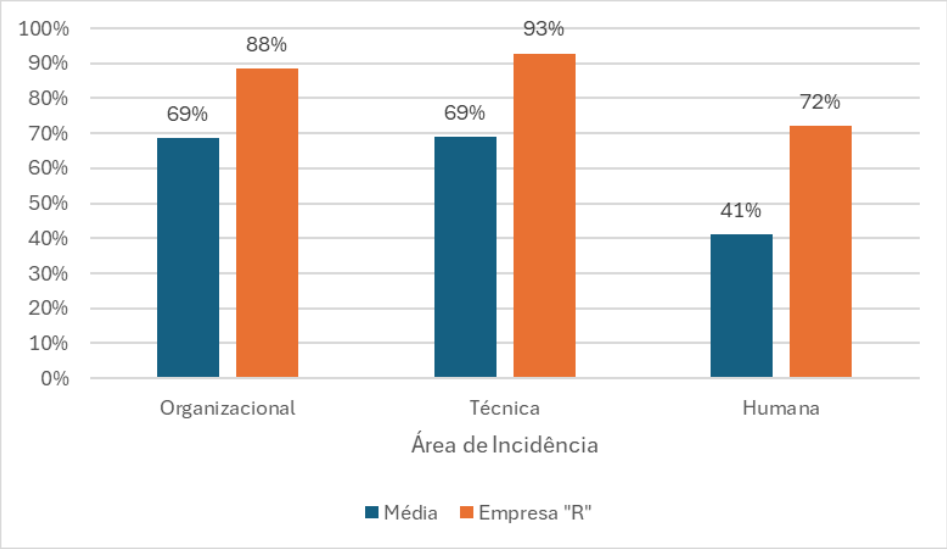



**Figura 32 – Comparação da percentagem média por Área de Incidência com a Empresa R**

**Organizacional** - a média das empresas é de 69%, enquanto a Empresa **R** apresenta uma pontuação significativamente mais alta, atingindo 88%. Isso sugere que a Empresa **R**

demonstra um nível mais avançado de maturidade organizacional em termos de práticas relacionadas à segurança digital, em comparação com a média geral das empresas.

**Técnica** – observa-se novamente uma diferença entre a média das empresas (69%) e a pontuação da Empresa **R** (93%). Indica que a Empresa **R** implementou medidas técnicas de segurança digital com um grau muito mais elevado de eficácia e abrangência do que a média das empresas.

**Humana** – a média de 41% é significativamente mais baixa do que nas outras áreas, destacando uma fraqueza comum entre as empresas: a falta de foco suficiente na preparação dos recursos humanos para enfrentar ameaças. A Empresa **R** tem um desempenho melhor, com 72%, sugerindo um maior investimento em formação e conscientização de segurança para seus funcionários, que a médias das empresas, mas não deixa de ser uma área que continua a precisar de atenção.

Como conclusão verifica-se que a Empresa **R** apresenta valores mais altos nas áreas organizacional e técnica, dado que a área humana tem a pontuação mais baixa, as empresas devem investir mais na formação contínua e programas de conscientização de cibersegurança para os utilizadores.

# 7. Conclusões

No contexto atual, a importância da informação não pode ser subestimada, num ambiente digital, a informação representa um dos ativos mais importantes para qualquer organização. Proteger a informação contra ameaças é fundamental para assegurar a continuidade dos negócios e manter a confiança dos clientes. Dado que as PMEs constituem a grande maioria das empresas no tecido empresarial português, é essencial que haja iniciativas direcionadas para este perfil empresarial, que enfrenta desafios distintos das empresas de maior dimensão.

Mesmo dentro das PMEs, estas possuem diversas configurações, uma abrangência muito ampla e com necessidades muito distintas também entre si. Sendo este trabalho direcionado para PMEs, pretendeu-se definir um *subset* mais específico, onde foram consideradas as PMEs que possuem mais de 50 ativos informáticos, e que contem com pelo menos uma pessoa afeta ao departamento de sistemas de informação. Assim considera-se que estas empresas podem ter competências básicas dos princípios de cibersegurança, mas serão capazes de compreender os conteúdos apresentados e que com orientação externa podem implementar medidas mais avançadas.

Para progredirem, estas empresas também necessitam da sensibilização da gestão de topo para o tema da cibersegurança, pois os líderes e executivos desempenham um papel essencial na definição das prioridades da organização e na alocação de recursos. Sem o compromisso e o apoio destes, iniciativas de implementar medidas de cibersegurança não irão receber a atenção, reconhecimento ou o investimento necessário para serem eficazes. A gestão de topo deve estar plenamente ciente dos riscos e comprometida com a implementação de medidas de segurança. Sendo também compromisso fundamental para estabelecer uma cultura de segurança transversal a toda a organização.

A falta de acesso a consultoria especializada para orientar as PMEs na implementação de práticas de segurança adequadas, aliada à diversidade de normas e *frameworks* de várias entidades, pode ser bastante confusa e exigente na sua interpretação. A existência de um guia que permita às empresas aceder a boas práticas ajustadas à sua dimensão é fundamental para a adoção de medidas de segurança eficazes. Embora haja uma quantidade significativa de informações disponíveis, estas estão dispersas entre diversas entidades e frequentemente não estão consolidadas de forma acessível.

Mais do que a consolidação de um guia, com este trabalho pretendeu-se que esse guia permitisse às empresas endereçar alguns dos desafios que estão inerentes às exigências de um processo de certificação. Daí surgiu a importância da utilização de uma ferramenta, que permitisse a validação e aplicabilidade à realidade das PMEs. Assim após o estudo realizado, o Selo de Maturidade Digital em Cibersegurança, apresentou-se com uma solução que permite através da adoção das boas práticas a obtenção de uma distinção

representativa do compromisso que a empresa tem com a Cibersegurança. Para tal, foi realizado um trabalho de mapeamento dos requisitos apresentados pelos Selos de Maturidade Digital em Cibersegurança do nível Bronze e Prata, com as *safeguards* do *CIS Controls*, que apresentam uma abordagem estruturada e prioritizada, com recomendações práticas e exemplos de implementação. O resultado deste mapeamento está apresentado no **Anexo C** – Guia da implementação de melhorias, como um documento autónomo, desenvolvido para ser uma ferramenta útil, neste contexto.

O resultado do mapeamento e a aplicação do inquérito a 21 empresas da Região de Leiria, permitiu identificar pontos fortes e áreas de melhoria nas práticas de segurança de forma agregada. A evidência mais significativa que resultou deste estudo, foi o défice na componente humana, destacando a necessidade de maior enfoque na formação e conscientização dos colaboradores para estarem mais preparados para enfrentarem as ameaças. Colaboradores informados e conscientes sobre os riscos são uma das mais importantes linhas de defesa contra os ataques. A sensibilização dos utilizadores é basilar para a construção de uma cultura de segurança robusta. A falta de conhecimento e atenção pode transformar o elemento humano numa vulnerabilidade crítica, independentemente de quão sofisticadas sejam as medidas técnicas adotadas. Assim, são necessários programas contínuos de formação e campanhas de conscientização para assegurar que todos os membros das organizações compreendam o seu papel na proteção dos ativos.

Além disso, pela análise do estudo, verificou-se que as empresas apresentam piores resultados nas áreas de deteção e resposta. Esta deficiência permite que ataques permaneçam não identificados por um maior período de tempo, o que compromete a mitigação eficaz dos incidentes, resultando em maior tempo de inatividade e potencial perda de dados. As PMEs devem investir em fortalecer as suas capacidades de deteção e resposta, além de melhorar a formação e conscientização de seus colaboradores, para melhorar a sua postura de segurança, e reduzir os riscos associados a incidentes de cibersegurança.

Os resultados obtidos, de forma geral, verificam-se ser mais positivos do que o inicialmente esperado, indicando que atualmente muitas empresas já começam a integrar boas práticas de segurança, embora com algumas limitações. Em termos do estudo realizado, a ausência da necessidade de apresentar evidências para confirmar o nível das respostas apresentado, pode ter levado a uma sobrevalorização do seu estado por parte de algumas empresas. Em trabalhos futuros pode ser interessante integrar uma abordagem onde seja necessário a incorporação de evidências, para confirmar o nível das respostas fornecidas, tendo em conta uma avaliação mais especifica de algumas áreas e não de uma forma tão abrangente como a metodologia seguida por este estudo.

De futuro, seria também interessante a realização de uma reavaliação das empresas após a utilização das medidas descritas no guia, para comparar o novo nível médio obtido após

a implementação das melhorias sugeridas. Esta reavaliação também ajudaria a identificar áreas que ainda necessitam de atenção ou aperfeiçoamento no guia apresentado.

Ao longo deste trabalho, o estudo mais aprofundado das *frameworks* de cibersegurança contribuiu para o aumento dos conhecimentos do autor, oferecendo a possibilidade de aplicar esses conceitos no contexto profissional e contribuir para o fortalecimento da cibersegurança nas organizações com quem trabalha diariamente.

# 8. Bibliografia


[1] 'ENISA Threat Landscape 2023', ENISA. Accessed: Jun. 13, 2024. [Online]. Available: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023

[2] R. A. Kemmerer, 'Cybersecurity', in *25th International Conference on Software Engineering, 2003. Proceedings.*, May 2003, pp. 705–715. doi: 10.1109/ICSE.2003.1201257.

[3] 'Jerome Powell: Transcrição completa da entrevista de 60 minutos de 2021 - CBS News'. Accessed: Jun. 13, 2024. [Online]. Available: https://www.cbsnews.com/news/jerome-powell-full-2021-60-minutes-interview-transcript/

[4] NIST, 'Framework Version 1.1', *NIST*, Apr. 2018, Accessed: Feb. 13, 2024. [Online]. Available: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

[5] ISO/IEC, 'Norma ISO/IEC 27001:2022'.

[6] CNCS, 'Quadro Nacional de Referência para a Cibersegurança'. Accessed: Nov. 26, 2023. [Online]. Available: https://www.cncs.gov.pt/pt/quadro-nacional/

[7] Center for Internet Security, Inc, 'CIS Controls Version 8'. Accessed: Oct. 25, 2023. [Online]. Available: https://www.cisecurity.org/controls/v8/

[8] U.S. Department of Energy (DOE), 'Cybersecurity Capability Maturity Model', Jun. 2022. [Online]. Available: https://www.energy.gov/sites/default/files/2022-06/C2M2%20Version%202.1%20June%202022.pdf

[9] ISACA, 'About ISACA | A Global Business & Technology Community', ISACA. Accessed: Jan. 10, 2024. [Online]. Available: https://www.isaca.org/about-us

[10] Instituto Português da Qualidade, 'Maturidade Digital - Selo Digital Parte 1: Cibersegurança'. 2021.

[11] Comissão das Comunidades Europeias, 'Recomendação da Comissão', 2003, [Online]. Available: https://www.iapmei.pt/getattachment/PRODUTOS-E-SERVICOS/Qualificacao-Certificacao/Certificacao-PME/Recomendacao-da-Comissao-2003-361-CE.pdf.aspx

[12] Comissão Europeia, 'Guia do utilizador relativo à definição de PME', 2020, [Online]. Available: https://www.iapmei.pt/getattachment/PRODUTOS-E-SERVICOS/Qualificacao-Certificacao/Certificacao-PME/Como-obter-uma-certificacao-PME/Guia-do-utilizador-relativo-a-definicao-de-PME-(Comissao-Europeia,-2020).pdf.aspx

[13] M. Wade, 'Digital Business Transformation - A Conceptual Framework', IMD.ORG, 2015. [Online]. Available: https://www.imd.org/uupload/IMD.WebSite/DBT/Digital%20Business%20Transformation%20Framework.pdf

[14] S. C. L. Estrela, 'A Gestão da Informação na Tomada de Decisão das PME da Região Centro', 2014, [Online]. Available: https://estudogeral.uc.pt/handle/10316/25956

[15] PricewaterhouseCoopers, 'PwC's 2022 Global Risk Survey: Embracing risk in the face of disruption', PwC. [Online]. Available: https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-risk-survey.html

[16] S. Kamiya, J.-K. Kang, J. Kim, A. Milidonis, and R. M. Stulz, 'Risk management, firm reputation, and the impact of successful cyberattacks on target firms', *J. Financ. Econ.*, vol. 139, no. 3, pp. 719–749, Mar. 2021, doi: 10.1016/j.jfineco.2019.05.019.
[17] Observatório de Cibersegurança, F. Carballo-Cruz, J. Cerejeira, and R. B. Esteves, 'Relatório Cibersegurança em Portugal Economia', May 2022. [Online]. Available: https://www.cncs.gov.pt/docs/relatorio-economia2022-obciber-cncs.pdf
[18] S. Samonas and D. Coss, 'The CIA Strikes Back: Redefining Confidentiality, Integrity and Availability in Security', Accessed: Feb. 12, 2024. [Online]. Available: https://www.proso.com/dl/Samonas.pdf
[19] D. E. Bell and L. J. La Padula, 'Secure Computer System: Unified Exposition and Multics Interpretation':, Defense Technical Information Center, Fort Belvoir, VA, Mar. 1976. Accessed: Feb. 12, 2024. [Online]. Available: https://csrc.nist.gov/files/pubs/conference/1998/10/08/proceedings-of-the-21st-nissc-1998/final/docs/early-cs-papers/bell76.pdf
[20] K. J. Bilba, 'Integrity Considerations for Secure Computer Systems', MITRE, Jun. 1975. [Online]. Available: https://seclab.cs.ucdavis.edu/projects/history/papers/biba75.pdf
[21] D. E. Denning, 'An Intrusion-Detection Model', *IEEE Trans. Softw. Eng.*, vol. SE-13, no. 2, pp. 222–232, Feb. 1987, doi: 10.1109/TSE.1987.232894.
[22] International Telecommunication Union, 'Overview of cybersecurity', Apr. 2008. [Online]. Available: https://www.itu.int/rec/T-REC-X.1205-200804-I/en
[23] National Initiative for Cybersecurity Careers and Studies, 'Vocabulary'. Accessed: Feb. 12, 2024. [Online]. Available: https://niccs.cisa.gov/cybersecurity-career-resources/vocabulary
[24] D. Schatz, R. Bashroush, and J. Wall, 'Towards a More Representative Definition of Cyber Security', *J. Digit. Forensics Secur. Law*, vol. 12, no. 2, Jun. 2017, doi: https://doi.org/10.15394/jdfsl.2017.1476.
[25] NIST, 'Cyber Security - Glossary | Computer Security Resource Center'. Accessed: Feb. 12, 2024. [Online]. Available: https://csrc.nist.gov/glossary/term/cyber_security
[26] União Europeia, 'Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho', Jul. 2016, [Online]. Available: https://www.cncs.gov.pt/docs/diretiva-2016.pdf
[27] Assembleia da República, 'Lei n.º 46/2018'. Accessed: Dec. 10, 2023. [Online]. Available: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384
[28] Presidência do Conselho de Ministros, 'Decreto-Lei n.º 65/2021'. Accessed: Dec. 10, 2023. [Online]. Available: https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988
[29] União Europeia, 'Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho', Dec. 2022, Accessed: Dec. 02, 2023. [Online]. Available: http://data.europa.eu/eli/dir/2022/2555/oj/por
[30] NIST, 'NIST History', *NIST*, Feb. 2019, Accessed: Nov. 19, 2023. [Online]. Available: https://www.nist.gov/history
[31] NIST, 'Framework Version 1.0', Feb. 2014, Accessed: Feb. 12, 2024. [Online]. Available: https://www.nist.gov/cyberframework/framework-version-10
[32] NIST, 'Cybersecurity Framework Overview'. Accessed: Dec. 03, 2023. [Online]. Available: https://www.nist.gov/system/files/documents/2019/03/06/2018_cybersecurity_framework_overview.pdf

[33] NIST, 'The NIST Cybersecurity Framework 2.0 (Draft)', U.S. Department of Commerce, NIST CSWP 29, Aug. 2023. Accessed: Nov. 19, 2023. [Online]. Available: https://csrc.nist.gov/pubs/cswp/29/the-nist-cybersecurity-framework-20/ipd
[34] ISO, 'What is ISO/IEC 27001?', ISO. Accessed: Nov. 18, 2023. [Online]. Available: https://www.iso.org/standard/27001
[35] APCER, 'ISO/IEC 27001 - Sistema de Gestão da Segurança da Informação'. Accessed: Nov. 18, 2023. [Online]. Available: https://apcergroup.com/pt/certificacao/pesquisa-de-normas/187/iso-iec-27001
[36] BSI, 'ISO/IEC 27001 - Information Security Management System'. Accessed: Nov. 18, 2023. [Online]. Available: https://www.bsigroup.com/en-GB/iso-27001-information-security/
[37] IPAC, 'Base de Dados Nacional - Sistemas de Gestão Certificados'. Accessed: Nov. 18, 2023. [Online]. Available: http://www.ipac.pt/pesquisa/pesq_empcertif.asp
[38] THE ISO COUNCIL, 'What is PDCA cycle in ISO 27001', THE ISO COUNCIL. [Online]. Available: https://isocouncil.com.au/plan-do-check-act-iso-27001/
[39] ISACA, 'COBIT 5'. Accessed: Jan. 07, 2024. [Online]. Available: https://store.isaca.org/s/store#/store/browse/detail/a2S4w000004KoCDEA0
[40] CNCS, 'Quadro de Avaliação de Capacidade de Cibersegurança', Jan. 2020. [Online]. Available: https://www.cncs.gov.pt/docs/cncs-quadrodeavaliacao.pdf
[41] Center for Internet Security, Inc, 'About us'. Accessed: Dec. 16, 2023. [Online]. Available: https://www.cisecurity.org/about-us/
[42] SANS Institute, 'CIS Controls v8 Released'. Accessed: Dec. 16, 2023. [Online]. Available: https://www.sans.org/blog/cis-controls-v8/
[43] 'CIS Critical Security Controls FAQ', CIS. Accessed: Dec. 16, 2023. [Online]. Available: https://www.cisecurity.org/controls/cis-controls-faq/
[44] Center for Internet Security, Inc, 'The 18 CIS Controls'. Accessed: Dec. 16, 2023. [Online]. Available: https://www.cisecurity.org/controls/cis-controls-list/
[45] Center for Internet Security, Inc, 'Implementation Guide for Small and Medium Sized Enterprises CIS Controls IG1'. Accessed: Dec. 16, 2023. [Online]. Available: https://www.cisecurity.org/insights/white-papers/implementation-guide-for-small-and-medium-sized-enterprises-cis-controls-ig1
[46] Center for Internet Security, Inc, 'CIS SecureSuite®'. Accessed: Jan. 09, 2024. [Online]. Available: https://www.cisecurity.org/cis-securesuite/pricing-and-categories/
[47] National Cyber Security Center UK, 'Maturity models in cyber security: what's happening to the IAMM?' Accessed: Nov. 26, 2023. [Online]. Available: https://www.ncsc.gov.uk/blog-post/maturity-models-cyber-security-whats-happening-iamm
[48] ISACA, 'Instituto CMMI'. Accessed: Jan. 10, 2024. [Online]. Available: https://cmmiinstitute.com/
[49] CMMI Institute, 'CMMI Levels of Capability and Performance'. Accessed: Jan. 10, 2024. [Online]. Available: https://cmmiinstitute.com/learning/appraisals/levels
[50] Impresa Nacional Casa da Moeda, 'Certificação'. Accessed: Dec. 17, 2023. [Online]. Available: https://selosmaturidadedigital.incm.pt/SMD/About
[51] Impresa Nacional Casa da Moeda, 'Selo Cibersegurança'. Accessed: Dec. 17, 2023. [Online]. Available: https://selosmaturidadedigital.incm.pt/SMD/Cybersecurity

[52] APCER, ‘Maturidade Digital das Organizações | Selo Digital de Cibersegurança’. Accessed: Feb. 14, 2024. [Online]. Available: https://go.apcergroup.com/ebook_SDCiber
[53] J. Galvin, ‘60 Percent of Small Businesses Fold Within 6 Months of a Cyber Attack. Here’s How to Protect Yourself’, Inc.com. Accessed: Feb. 02, 2024. [Online]. Available: https://www.inc.com/joe-galvin/60-percent-of-small-businesses-fold-within-6-months-of-a-cyber-attack-heres-how-to-protect-yourself.html
[54] A. Alahmari and B. Duncan, ‘Cybersecurity Risk Management in Small and Medium-Sized Enterprises: A Systematic Review of Recent Evidence’, in *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*, Jun. 2020, pp. 1–5. doi: 10.1109/CyberSA49311.2020.9139638.
[55] Alberto García Pérez, Antonio López Martínez, and Manuel Gil Pérez, ‘Adaptive vulnerability-based risk identification software with virtualization functions for dynamic management’, vol. 219, pp. 103728–103728, Oct. 2023, doi: 10.1016/j.jnca.2023.103728.
[56] Shreepal Jain, Arunabha Mukhopadhyay, and S. K. Jain, ‘Can Cyber Risk of Health Care Firms be Insured? A Multinomial Logistic Regression Model’, vol. 33, no. 1–2, pp. 41–69, Apr. 2023, doi: 10.1080/10919392.2023.2244386.
[57] Arun Sukumar, Hannan Amoozad Mahdiraji, and Vahid Jafari-Sadeghi, ‘Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors’, vol. 43, no. 10, pp. 2082–2098, Jan. 2023, doi: 10.1111/risa.14092.
[58] D. O. Ouma, ‘A Cybersecurity Maturity Model and Toolkit for Self-assessment’, Thesis, University of Nairobi, 2021. Accessed: Jan. 14, 2024. [Online]. Available: http://erepository.uonbi.ac.ke/handle/11295/155796
[59] A. Shojaifar and H. Järvinen, ‘Classifying SMEs for Approaching Cybersecurity Competence and Awareness’, in *Proceedings of the 16th International Conference on Availability, Reliability and Security*, in ARES ’21. New York, NY, USA: Association for Computing Machinery, Aug. 2021, pp. 1–7. doi: 10.1145/3465481.3469200.
[60] B. Y. Ozkan and M. Spruit, ‘Cybersecurity Standardisation Essentials for European SMEs’, [Online]. Available: https://webspace.science.uu.nl/~sprui107/download/Cybersecurity%20Standardisation%20Essentials%20for%20European%20SMEs.pdf
[61] M. Benz and D. Chatterjee, ‘Calculated risk? A cybersecurity evaluation tool for SMEs’, *Bus. Horiz.*, vol. 63, no. 4, pp. 531–540, Jul. 2020, doi: 10.1016/j.bushor.2020.03.010.
[62] M. Figueredo Franco, F. Martins Lacerda, and B. Stiller, ‘A framework for the planning and management of cybersecurity projects in small and medium-sized enterprises’, *Gest. E Proj. GeP*, 2022, Accessed: Jan. 14, 2024. [Online]. Available: https://dialnet.unirioja.es/servlet/articulo?codigo=8771946
[63] B. Azinheira, M. Antunes, M. Maximiano, and R. Gomes, ‘A methodology for mapping cybersecurity standards into governance guidelines for SME in Portugal’, *Procedia Comput. Sci.*, vol. 219, pp. 121–128, Jan. 2023, doi: 10.1016/j.procs.2023.01.272.
[64] S. A. Pawar and H. Palivela, ‘Importance of Least Cybersecurity Controls for Small and Medium Enterprises (SMEs) for Better Global Digitalised Economy’, in *Smart Analytics, Artificial Intelligence and Sustainable Performance Management in a*

*Global Digitalised Economy*, vol. 110B, P. Tyagi, S. Grima, K. Sood, B. Balamurugan, E. Özen, and T. Eleftherios, Eds., in Contemporary Studies in Economic and Financial Analysis, vol. 110B. , Emerald Publishing Limited, 2023, pp. 21–53. doi: 10.1108/S1569-37592023000110B002.

[65] R. Sasidharan, 'A Case Study to Implement Windows System Hardening using CIS Controls', *Int. J. Comput. Trends Technol.*, vol. 70, pp. 1–7, Jul. 2022, doi: 10.14445/22312803/IJCTT-V70I7P101.

[66] Center for Internet Security, Inc, 'CIS SecureSuite Build Kit Content', CIS. Accessed: Mar. 17, 2024. [Online]. Available: https://www.cisecurity.org/cis-securesuite/cis-securesuite-build-kit-content/

[67] A. Chidukwani, S. Zander, and P. Koutsakis, 'A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations', *IEEE Access*, vol. 10, pp. 85701–85719, 2022, doi: 10.1109/ACCESS.2022.3197899.

[68] Mohamed Noordin Yusuff Marican, S. Razak, A. Selamat, and S. H. Othman, 'Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review', *IEEE Access*, 2023, doi: 10.1109/access.2022.3229766.

[69] Tahereh Hasani, Norm O'Reilly, Ali Dehghantanha, Davar Rezania, and Nadège Levallet, 'Evaluating the adoption of cybersecurity and its influence on organizational performance', vol. 3, no. 5, Apr. 2023, doi: 10.1007/s43546-023-00477-6.

[70] Khalifa AL-Dosari and Noora Fetais, 'Risk-Management Framework and Information-Security Systems for Small and Medium Enterprises (SMEs): A Meta-Analysis Approach', vol. 12, no. 17, pp. 3629–3629, Aug. 2023, doi: 10.3390/electronics12173629.

[71] Patrick Wake, Sue Black, and J. A. Young, 'Work in Progress: Evaluation of Security Standards through a Cyber Range using Hackers' Tactics, Techniques and Procedures', Jul. 2023, doi: 10.1109/eurospw59978.2023.00076.

[72] S. Groš, 'A Critical View on CIS Controls', in *2021 16th International Conference on Telecommunications (ConTEL)*, Jun. 2021, pp. 122–128. doi: 10.23919/ConTEL52528.2021.9495982.

[73] M. N. Y. Marican, S. A. Razak, A. Selamat, and S. H. Othman, 'Cyber Security Maturity Assessment Framework for Technology Startups: A Systematic Literature Review', *IEEE Access*, vol. 11, pp. 5442–5452, 2023, doi: 10.1109/ACCESS.2022.3229766.

[74] S. Vasudevan, 'DeFi: A risky business or silver bullet for SMEs?', in *2022 International Conference on Cyber Resilience (ICCR)*, Oct. 2022, pp. 1–5. doi: 10.1109/ICCR56254.2022.9995866.

[75] S. Pawar and H. Palivela, 'LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs)', *Int. J. Inf. Manag. Data Insights*, vol. 2, p. 100080, Apr. 2022, doi: 10.1016/j.jjimei.2022.100080.

[76] Center for Internet Security, Inc, 'Acceptable Use Policy Template for the CIS Controls', CIS. Accessed: Jun. 10, 2024. [Online]. Available: https://www.cisecurity.org/insights/white-papers/acceptable-use-policy-template-for-the-cis-controls

[77] Center for Internet Security, Inc, 'White Paper: CIS Password Policy Guide', CIS. Accessed: Jun. 12, 2024. [Online]. Available: https://www.cisecurity.org/white-papers/cis-password-policy-guide/

[78] W. Triplett, 'Addressing Human Factors in Cybersecurity Leadership', *J. Cybersecurity Priv.*, vol. 2, pp. 573–586, Jul. 2022, doi: 10.3390/jcp2030029.

# 9. Anexos

# A Anexo A – Questionário

Este anexo apresenta o questionário elaborado para as PMEs, tendo como objetivo primordial a obtenção de respostas de autoavaliação. O questionário foi aplicado de forma eficaz através da plataforma online QuestionPro, como destacado no relatório, visando garantir a qualidade e a precisão dos dados coletados.


**Avaliação da Maturidade em Cibersegurança**

O presente questionário integra uma investigação académica no âmbito de um projeto de **Mestrado em Cibersegurança e Informática Forense**, do Instituto Politécnico de Leiria, para a avaliação da maturidade em cibersegurança de Pequenas e Médias Empresas (PMEs). Sendo a cibersegurança uma preocupação crescente para as organizações de todos as dimensões, é crucial compreender em que medida as PMEs estão preparadas para enfrentar os desafios e ameaças no cenário atual.

O objetivo desta avaliação é analisar os diferentes aspetos relacionados com a cibersegurança, identificando pontos fortes, áreas de melhoria e possíveis lacunas na proteção dos ativos digitais. Os resultados obtidos serão utilizados exclusivamente para fins académicos, visando contribuir para o desenvolvimento de estratégias e políticas que fortaleçam a cibersegurança nas organizações.

Todas as informações fornecidas neste questionário são estritamente confidenciais e serão tratadas de forma anónima e agregada. Os nomes das empresas não serão divulgados, garantindo assim a privacidade e confidencialidade das respostas, sendo apenas pedido o endereço de *e-mail* de quem responde para validação das respostas.

Agradecemos desde já a sua participação e colaboração neste estudo, que certamente contribuirá para um melhor entendimento e fortalecimento da cibersegurança.

Endereço de *e-mail*:

Para cada uma das questões colocadas são apresentadas 3 opções de resposta. Deve selecionar, a que melhor caracteriza a sua organização.

O questionário é composto por 50 questões, tendo um tempo estimado de resposta entre 20 e 30 minutos.


**Identificar** - Inventariação e gestão de todos os ativos de *hardware* e *software* dentro da rede da organização, incluindo dispositivos móveis, servidores, aplicações e dados.

**I1:** Na sua organização são identificadas as funções ou atividades críticas e respetiva dependência das TIC?

- **Nível 1** (Básico) Não existe identificação das dependências das TIC nas funções ou atividades críticas do negócio.
- **Nível 2** (Intermédio) As dependências das TIC nas funções ou atividades críticas são reconhecidas de forma geral, mas a identificação completa está incompleta ou desatualizada.
- **Nível 3** (Avançado) A organização possuí um processo contínuo para identificar e rever regularmente funções ou atividades críticas. Além de um documento formal, a organização utiliza ferramentas automatizadas para pesquisar e gerir as relações entre funções críticas, ativos e dependências de TIC.

**I2:** Na sua organização é estabelecido e mantido um inventário detalhado dos ativos corporativos?

- **Nível 1** (Básico) Não existe um inventário de ativos corporativos.
- **Nível 2** (Intermédio) Existe um inventário de ativos, mas ele não é detalhado ou atualizado regularmente, as informações essenciais, estão ausentes ou desatualizadas.

- **Nível 3** (Avançado) Existe um inventário detalhado e atualizado de todos os ativos corporativos, incluindo dispositivos de rede (ex: *router*, *switch*), dispositivos IoT, Servidores. Este incluí informações como endereço de *hardware* (MAC), nome da máquina, proprietário e departamento para cada ativo. O inventário é revisto e atualizado semestralmente ou com maior frequência.

**I3:** Na sua organização é estabelecido e mantido um inventário detalhado dos *softwares* corporativos?

- **Nível 1** (Básico) Não existe um inventário de *software* instalado em ativos corporativos.
- **Nível 2** (Intermédio) Existe um inventário de *software*, mas ele não é detalhado ou atualizado regularmente. As informações essenciais estão incompletas ou desatualizadas.
- **Nível 3** (Avançado) Existe um inventário detalhado e atualizado de todos os *softwares* licenciados e instalados em ativos corporativos. Este incluí informações como nome, produtor, data de instalação, URL, versão e data de ativação. O inventário é revisto e atualizado semestralmente ou com maior frequência.

**I4:** Na sua organização existe um processo para utilização exclusiva de *software* autorizado?

- **Nível 1** (Básico) Não existe um processo para verificar o *software* autorizado.
- **Nível 2** (Intermédio) Existe um processo para verificar o *software* no inventário, mas não é realizado regularmente. O inventário de *software* é revisto periodicamente, mas ainda existe *software* não suportado sem documentação de exceção.
- **Nível 3** (Avançado) Está estabelecido um processo para verificar regularmente o inventário de *software*. O inventário de *software* é revisto pelo menos uma vez por mês para garantir que apenas *software* suportado seja designado como autorizado. S*oftware* não suportado é documentado com exceções detalhadas, incluindo controlos de mitigação e aceitação do risco residual.

**I5:** Na sua organização existe um diagrama de arquitetura do Sistema de Rede?

- **Nível 1** (Básico) Não existem diagramas de arquitetura ou outra documentação da estrutura da rede.

- **Nível 2** (Intermédio) Existe alguma documentação da estrutura de rede, mas não é revista ou atualizada regularmente.
- **Nível 3** (Avançado) Os diagramas de arquitetura e outra documentação de sistema de rede são mantidos e atualizados regularmente. As alterações significativas são prontamente refletidas na documentação, que é revista anualmente.

**I6:** Na sua organização existe um inventário de contas de sistemas de TI?

- **Nível 1** (Básico) Não existe um inventário das contas geridas na empresa.
- **Nível 2** (Intermédio) Existe um inventário de contas geridas na empresa, mas está incompleto ou desatualizado. Algumas informações básicas, como nome de utilizador e departamento, estão registadas, mas não existe validação regular para garantir a precisão dos registos.
- **Nível 3** (Avançado) É mantido um inventário abrangente de todas as contas geridas na empresa. O inventário inclui detalhes como nome da pessoa, datas de início/término, assim como o departamento. As contas ativas são validadas regularmente para garantir que estejam autorizadas, com uma periodicidade recorrente de no mínimo trimestralmente ou com maior frequência.


**Proteger** - Implementação de controlos de segurança para proteger os ativos contra ameaças internas e externas, incluindo antivírus, *firewalls*, deteção de intrusões e prevenção de malware.

**P1:** Na sua organização existe uma Política de Uso Aceitável (PUA) dos Sistemas Informáticos?

- **Nível 1** (Básico) A organização não possui uma Política de Utilização Aceitável dos recursos de TI.
- **Nível 2** (Intermédio) Existe uma Política de Utilização Aceitável, porém, ela não está formalizada num documento. As diretrizes para o uso seguro dos recursos de TI estão disponíveis de forma dispersa ou não são claramente comunicadas a todos os colaboradores.

- **Nível 3** (Avançado) A organização possui uma Política de Utilização Aceitável formalizada e documentada. As diretrizes para o uso seguro dos recursos de TI são claramente definidas e comunicadas a todos os colaboradores. A política aborda uma variedade de cenários, incluindo uso de dispositivos pessoais, acesso a redes Wi-Fi externas, uso de *e-mail* e *internet*, entre outros. As consequências do não cumprimento da política são claras e aplicadas de forma consistente.

**P2:** Na sua organização existe um processo de proteção dos dados de *backup*?

- **Nível 1** (Básico) Os dados de *backup* não são protegidos adequadamente e não se encontram cifrados.
- **Nível 2** (Intermédio) Existem medidas para proteger os dados de *backup*, mas os controlos não são equivalentes aos dos dados originais. Existe o uso de cifragem ou segregação de dados, mas não está implementado consistentemente.
- **Nível 3** (Avançado) Os dados de *backup* são protegidos com controlos equivalentes aos dos dados originais. A cifragem e segregação de dados é implementada de forma consistente e adequada para garantir a sua segurança.

**P3:** Na sua organização existe uma gestão automatizada de *updates* dos Sistemas Operativos?

- **Nível 1** (Básico) As atualizações do sistema operativo não são realizadas regularmente ou são feitas de forma manual.
- **Nível 2** (Intermédio) As atualizações do sistema operativo são realizadas regularmente, mas não são automatizadas. Existe um processo informal para aplicar *patches* de segurança, mas não é feito mensalmente ou com maior frequência de forma consistente.
- **Nível 3** (Avançado) As atualizações do sistema operativo são realizadas regularmente e de forma automatizada. Existe um processo formal estabelecido para aplicar *patches* de segurança mensalmente ou com maior frequência, garantindo a proteção contínua dos ativos corporativos.

**P4:** Na sua organização existe uma gestão automatizada de *updates* das aplicações?

- **Nível 1** (Básico) As atualizações das aplicações não são realizadas regularmente ou são feitas de forma manual.

- **Nível 2** (Intermédio) As atualizações das aplicações são realizadas regularmente, mas não são automatizadas. Existe um processo informal para aplicar *patches* das aplicações, mas não é feito mensalmente ou com maior frequência de forma consistente.

- **Nível 3** (Avançado) As atualizações das aplicações são realizadas regularmente e de forma automatizada. Existe um processo formal estabelecido para aplicar *patches* das aplicações mensalmente ou com maior frequência, garantindo a segurança contínua dos ativos corporativos

**P5:** Na sua organização existe uma solução de anti-*malware*?

- **Nível 1** (Básico) O *software* anti-*malware* não está instalado em todos os ativos corporativos.

- **Nível 2** (Intermédio) O *software* anti-*malware* está instalado em todos os ativos corporativos, mas não é mantido regularmente ou atualizado automaticamente.

- **Nível 3** (Avançado) O *software* anti-malware está instalado em todos os ativos corporativos e é mantido regularmente e atualizado automaticamente. Existe um processo formal estabelecido para manter e atualizar o *software* anti-*malware*, garantindo a proteção contínua contra ameaças de segurança.

**P6:** Na sua organização a solução de anti-*malware* tem atualizações das assinaturas automáticas?

- **Nível 1** (Básico) As atualizações automáticas das definições de assinatura anti-*malware* não estão configuradas em todos os ativos corporativos, ou não existe esta informação centralmente.

- **Nível 2** (Intermédio) As atualizações automáticas das definições de assinatura anti-*malware* estão parcialmente configuradas em alguns ativos corporativos, mas não são consistentes em toda a organização.

- **Nível 3** (Avançado) As atualizações automáticas das definições de assinatura anti-*malware* estão configuradas em todos os ativos corporativos e são aplicadas regularmente. Há um processo formal estabelecido para garantir que as atualizações de assinatura anti-*malware* sejam aplicadas automaticamente em todos os ativos corporativos, garantindo a proteção contínua contra ameaças de segurança.

**P7:** Na sua organização nos servidores encontra-se aplicada a *firewall* do Sistema Operativo (SO)?

- **Nível 1** (Básico) A *firewall* do SO (ou outra ferramenta de filtragem de portos) não está implementada em nenhum servidor.
- **Nível 2** (Intermédio) A *firewall* do SO (ou outra ferramenta de filtragem de portos) está implementada em alguns servidores onde é suportada, mas não é consistente em toda a infraestrutura.
- **Nível 3** (Avançado) A *firewall* do SO (ou outra ferramenta de filtragem de portos) está implementada em todos os servidores onde é suportada e é gerida de forma proativa. Existe um plano estabelecido para implementar e gerir a *firewall* nos servidores.

**P8:** Na sua organização nos postos dos utilizadores encontra-se aplicada a *firewall* do Sistema Operativo (SO)?

- **Nível 1** (Básico) A *firewall* do SO (ou outra ferramenta de filtragem de portos) não está implementada nos dispositivos dos utilizadores finais.
- **Nível 2** (Intermédio) A *firewall* do SO (ou outra ferramenta de filtragem de portos) está implementada em alguns dispositivos dos utilizadores finais, mas não está aplicada de forma uniforme em todos os dispositivos.
- **Nível 3** (Avançado) A *firewall* do SO (ou outra ferramenta de filtragem de portos) está implementada em todos os dispositivos dos utilizadores finais e é gerida de forma proativa. Existe uma regra de negação padrão configurada que bloqueia todo o tráfego, exceto os serviços e portos explicitamente permitidos.

**P9:** Na sua organização os protocolos de gestão inseguros encontram-se desabilitados?

- **Nível 1** (Básico) Protocolos de gestão inseguros, como *telnet* e HTTP, são utilizados para acesso às interfaces administrativas.
- **Nível 2** (Intermédio) Protocolos seguros, como SSH e HTTPS, são usados em algumas interfaces administrativas, mas ainda existem instâncias de *telnet* e HTTP a serem usadas. Há algumas medidas para gerir os ativos e *software* corporativos de forma segura, mas são inconsistentes.

- **Nível 3** (Avançado) Todas as interfaces administrativas são acedidas usando protocolos seguros, como SSH e HTTPS. São tomadas medidas para evitar o uso de protocolos inseguros, a menos que estritamente necessário para operações críticas.

**P10:** Na sua organização as contas padrão encontram-se desabilitadas?

- **Nível 1** (Básico) As contas padrão permanecem ativas e não são monitorizadas quanto a atividades suspeitas.
- **Nível 2** (Intermédio) Existe uma tentativa de desativar ou tornar inutilizáveis algumas contas padrão, mas isso não é feito de forma sistemática em todos os ativos e *software* corporativos.
- **Nível 3** (Avançado) Todas as contas padrão encontram-se desativadas ou tornadas inutilizáveis em todos os ativos e *software* corporativos.

**P11:** Na sua organização é mantida uma arquitetura de rede segura?

- **Nível 1** (Básico) A arquitetura de rede não é projetada com foco na segurança. Não existe segmentação adequada da rede e os princípios de privilégio mínimo não são aplicados.
- **Nível 2** (Intermédio) São tomadas algumas medidas para estabelecer uma arquitetura de rede segura, mas são inconsistentes. Existe alguma segmentação na rede, mas os princípios de privilégio mínimo não são totalmente implementados.
- **Nível 3** (Avançado) A arquitetura de rede é projetada e mantida com foco na segurança. Há uma segmentação clara e bem definida da rede, juntamente com a aplicação dos princípios de privilégio mínimo para garantir que apenas as partes autorizadas tenham acesso apenas aos recursos necessários.

**P12:** Na sua organização é aplicado a *Sender Policy Framework* (SPF) e *Hyper Text Transfer Protocol Secure* (HTTPS)?

- **Nível 1** (Básico) A política de SPF não se encontra implementada para o *e-mail* e não estão implementados certificados digitais para acesso a recursos HTTPS corporativos.
- **Nível 2** (Intermédio) A política de SPF encontra-se parcialmente implementada e estão implementados certificados digitais para acesso a recursos HTTPS corporativos.

- **Nível 3** (Avançado) A política de SPF encontra-se corretamente implementada e estão implementados certificados digitais para acesso a recursos HTTPS corporativos.

**P13:** Na sua organização é aplicado o *DomainKeys Identified Mail* (DKIM) e HTTP *Strict Transport Security* (HSTS)?

- **Nível 1** (Básico) Não se encontra implementada uma política de DKIM nem mecanismos HSTS para acesso aos ativos corporativos.
- **Nível 2** (Intermédio) Existe política de DKIM e/ou o mecanismo HSTS, mas não se encontram devidamente implementados.
- **Nível 3** (Avançado) A política de DKIM encontra-se corretamente implementada e está implementado o mecanismo HSTS para acesso aos ativos corporativos.

**P14:** Na sua organização é exigido Multifator de Autenticação (MFA) para aplicações expostas externamente?

- **Nível 1** (Básico) O MFA não é exigido para nenhuma aplicação corporativa exposta externamente.
- **Nível 2** (Intermédio) O MFA é exigido em algumas aplicações corporativas ou de terceiros expostas externamente, mas não é aplicado consistentemente em todas.
- **Nível 3** (Avançado) O MFA é exigido em todas as aplicações corporativas ou de terceiros expostas externamente, onde suportado. Existe um processo formal estabelecido para garantir que o MFA seja implementado de forma consistente e eficaz em todas as aplicações.

**P15:** Na sua organização é exigido Multifator de Autenticação (MFA) para acesso remoto à rede?

- **Nível 1** (Básico) O MFA não é exigido para acesso remoto à rede.
- **Nível 2** (Intermédio) O MFA está implementado para alguns métodos de acesso remoto, mas não para todos. Existe uma política parcial para exigir MFA em determinadas situações de acesso remoto, mas não é aplicada consistentemente.

- **Nível 3** (Avançado) O MFA é exigido para todos os métodos de acesso remoto à rede. Existe uma política que garante que todos os utilizadores se autentiquem com MFA ao aceder remotamente à rede corporativa.

**P16:** Na sua organização é exigido Multifator de Autenticação (MFA) para acesso de administração?

- **Nível 1** (Básico) O MFA não é exigido nas contas com privilégios de administração.
- **Nível 2** (Intermédio) O MFA é implementado para algumas contas com privilégios de administração.
- **Nível 3** (Avançado) O MFA é exigido para todas as contas de acesso de administração em todos os ativos corporativos, independentemente de serem geridos localmente ou por meio de um fornecedor externo. Existe uma política que garante que todas as contas com privilégios de administração sejam protegidas por MFA, independentemente de onde os ativos estão localizados.

**P17:** Na sua organização existe um programa de consciencialização de segurança?

- **Nível 1** (Básico) Os utilizadores não recebem formação regular sobre segurança da informação.
- **Nível 2** (Intermédio) Existe um programa de consciencialização de segurança, mas é inconsistente ou não obrigatório. A formação é fornecida aquando do processo de contratação, mas não regularmente.
- **Nível 3** (Avançado) A empresa possui um programa de consciencialização de segurança obrigatório para todos os utilizadores. A formação é realizada na contratação e anualmente, o conteúdo é regularmente analisado e atualizado para refletir as mudanças nas ameaças de segurança e nas políticas da empresa.

**P18:** Na sua organização existe um programa de consciencialização para reconhecer ataques de engenharia social?

- **Nível 1** (Básico) Os utilizadores não estão cientes dos sinais de *phishing* ou de outras formas de engenharia social.
- **Nível 2** (Intermédio) Os utilizadores recebem formação básica sobre reconhecimento de ataques de engenharia social.

- **Nível 3** (Avançado)Todos os utilizadores são treinados para reconhecer e responder a ataques de engenharia social, incluindo os vários tipos *phishing*. A formação é contínua e abrangente, com simulações regulares e outros exercícios práticos para reforçar a consciencialização.

**P19:** Na sua organização são utilizadas palavras-passe exclusivas para os ativos corporativos?

- **Nível 1** (Básico) Não são implementadas palavras-passe exclusivas e podem ser fracas ou partilhadas entre vários ativos.
- **Nível 2** (Intermédio) São implementadas palavras-passe exclusivas para os ativos corporativos, não apresentam os requisitos mínimos de comprimento, ou não serem suficientemente complexas.
- **Nível 3** (Avançado) São usadas palavras-passe exclusivas para todos os ativos corporativos, seguindo as melhores práticas de implementação. Estas possuem um comprimento adequado e parâmetros de complexidade.

**P20:** Na sua organização existem listas de controlo de acesso a dados?

- **Nível 1** (Básico) Não existem listas de controlo de acesso configuradas.
- **Nível 2** (Intermédio) Existem listas de controlo de acesso, mas não são consistentemente aplicadas em todos os sistemas e aplicações. As permissões de acesso são definidas de forma genérica, sem considerar adequadamente a necessidade de conhecimento do utilizador.
- **Nível 3** (Avançado)Existem listas de controlo de acesso configuradas e aplicadas em todos os sistemas de ficheiros, bases de dados e aplicações. As permissões de acesso são geridas de acordo com a necessidade de conhecimento do utilizador, garantindo que apenas utilizadores autorizados tenham acesso aos dados relevantes para as suas funções. As políticas de controlo de acesso são revistas regularmente e ajustadas conforme necessário para garantir a segurança contínua dos dados corporativos.

**P21:** Na sua organização existe um processo de concessão de acessos?

- **Nível 1** (Básico) Não existe um processo formal estabelecido para conceder acesso aos ativos corporativos.

- **Nível 2** (Intermédio) Existe um processo para conceder acesso aos ativos corporativos, manual e sujeito a inconsistências.
- **Nível 3** (Avançado) Existe um processo formal, para conceder acesso aos ativos corporativos. O processo garante que novas contratações, concessões de direitos ou mudanças de função de utilizadores são rapidamente refletidas no acesso aos recursos corporativos, reduzindo assim o tempo de inatividade e o risco de acesso não autorizado.

**P22:** Na sua organização existe um processo de revogação de acessos?

- **Nível 1** (Básico) Não existe um processo formal estabelecido para revogar o acesso aos ativos corporativos.
- **Nível 2** (Intermédio) Existe um processo para revogar o acesso aos ativos corporativos, manual e sujeito a erros. A desativação de contas é realizada, mas existe falta de automação ou atrasos na revogação de direitos de acesso.
- **Nível 3** (Avançado) Existe um processo formal, para revogar o acesso aos ativos corporativos. As contas são desativadas imediatamente após o encerramento, revogação de direitos ou mudança de função de um utilizador, enquanto os registos de auditoria são mantidos. O processo garante que o acesso não autorizado seja prontamente removido, reduzindo assim o risco de violações de segurança e conformidade.

**P23:** Na sua organização são utilizados gestores de credenciais?

- **Nível 1** (Básico) Os utilizadores não utilizam um gestor de credenciais.
- **Nível 2** (Intermédio) Alguns utilizadores utilizam gestor de credenciais, mas de forma inconsistente.
- **Nível 3** (Avançado)A maioria ou todos os utilizadores utiliza um gestor de credenciais de forma consistente. São utilizadas palavras-passe complexas e exclusivas. Os utilizadores têm formação regularmente sobre as melhores práticas de segurança relacionadas com o uso de gestor de credenciais.

**P24:** Na sua organização existem contas de Administração dedicadas?

- **Nível 1** (Básico) Não existe distinção clara entre contas de administrador e contas de utilizador comuns.

- **Nível 2** (Intermédio) As contas de administrador são reservadas apenas para tarefas que exigem privilégios elevados, como instalação de *software* ou alterações de configuração. Os utilizadores são incentivados a usar contas de utilizador comuns para atividades gerais.
- **Nível 3** (Avançado) As contas de administrador são separadas e atribuídas apenas a pessoal autorizado. Está implementada uma política, instruindo os utilizadores a realizar as atividades gerais com a sua conta não privilegiada.

**P26:** Na sua organização os dispositivos dos utilizadores finais encontram-se cifrados?

- **Nível 1** (Básico) Os dispositivos dos utilizadores finais não se encontram cifrados.
- **Nível 2** (Intermédio) Alguns dispositivos dos utilizadores finais que contêm dados sensíveis são cifrados, mas a implementação é inconsistente.
- **Nível 3** (Avançado) As políticas de segurança incluem requisitos específicos para a cifragem de dispositivos do utilizador final e são aplicadas de forma rigorosa em toda a organização. São utilizadas soluções de cifragem como *BitLocker, FileVault, dm-crypt*, entre outras, garantindo uma proteção eficaz dos dados em repouso, preferencialmente com uma gestão centralizadas das chaves.

**P27:** Na sua organização existe um processo de gestão de configurações que permite a definição de uma base segura para os dispositivos dos utilizadores finais?

- **Nível 1** (Básico) Não existe um processo formal estabelecido para configuração segura de ativos corporativos.
- **Nível 2** (Intermédio) Existe um processo básico de configuração segura, mas é inconsistente ou incompleto. As configurações padrão são ajustadas para melhorar a segurança, mas não são abordadas todas as melhores práticas recomendadas.
- **Nível 3** (Avançado) Existe um processo formal de configuração segura para todos os ativos corporativos e *software*. As configurações são revistas regularmente para garantir que estão alinhadas com as melhores práticas de segurança e conformidade. A documentação do processo é atualizada anualmente ou quando ocorrem mudanças significativas na empresa, garantindo que a segurança seja mantida em níveis adequados.

**P28:** Na sua organização existe um processo de configuração segura para os ativos de rede?

- **Nível 1** (Básico) Não existe um processo formal estabelecido para configuração segura dos dispositivos de rede.
- **Nível 2** (Intermédio) Existe um processo básico de configuração segura para dispositivos de rede, mas é inconsistente ou incompleto. As configurações padrão são ajustadas em alguns dispositivos, mas não são abordadas todas as melhores práticas de segurança.
- **Nível 3** (Avançado) Existe um processo formal de configuração segura para todos os dispositivos de rede. As configurações dos dispositivos de rede são revistas regularmente para garantir que estão alinhadas com as melhores práticas de segurança e conformidade. A documentação do processo é atualizada anualmente ou quando ocorrem mudanças significativas na empresa, garantindo que a segurança da rede seja mantida em níveis adequados.

**P29:** Na sua organização existe um processo de bloqueio automático da sessão?

- **Nível 1** (Básico) Não existe configuração de bloqueio automático de sessão nos ativos corporativos após períodos de inatividade.
- **Nível 2** (Intermédio) Existe uma configuração básica de bloqueio automático de sessão, mas os períodos de inatividade são excessivamente longos.
- **Nível 3** (Avançado) O bloqueio automático de sessão é configurado adequadamente em todos os ativos corporativos. A configuração é regularmente revista e atualizada para garantir que permaneça alinhada com as melhores práticas de segurança.

**P30:** Na sua organização podem apenas ser utilizados browser de internet e clientes de *e-mail* suportados?

- **Nível 1** (Básico) Não existe política para restringir o uso de *browser* de *internet* e clientes de *e-mail*.
- **Nível 2** (Intermédio) A maioria dos utilizadores utiliza *browser* de *internet* e clientes de *e-mail* suportados, mas existem exceções.
- **Nível 3** (Avançado) É aplicada uma política rigorosa para permitir apenas *browser* de *internet* e clientes de *e-mail* suportados, usando apenas as versões mais recentes fornecidas pelo fornecedor.

**P31:** Na sua organização existe um processo de formação dos utilizadores sobre as melhores práticas de tratamento de dados?

- **Nível 1** (Básico) Não existe formação sobre o manuseamento adequado de dados sensíveis.
- **Nível 2** (Intermédio) Existe alguma formação sobe o manuseamento de dados sensíveis, mas está incompleto. As práticas recomendadas de mesa e ecrã limpos são comunicadas, mas não são seguidas por todos os utilizadores.
- **Nível 3** (Avançado) É realizada formação prática regularmente e abrangente sobre o manuseamento adequado de dados sensíveis para todos os membros da equipa. Os utilizadores têm um entendimento claro dos procedimentos para identificar, armazenar, transferir, arquivar e destruir dados sensíveis de maneira segura. As práticas recomendadas de mesa e ecrã limpos são comunicadas e amplamente seguidas por todos os utilizadores.

**P32:** Na sua organização existe um processo de formação dos utilizadores sobre exposição não intencional de dados?

- **Nível 1** (Básico) Os membros da equipa não receberam formação a possíveis causas da exposição não intencional de dados.
- **Nível 2** (Intermédio) Os utilizadores têm uma compreensão razoável das diferentes maneiras pelas quais os dados sensíveis podem ser expostos inadvertidamente, como a perda de dispositivos e divulgação não autorizada.
- **Nível 3** (Avançado) A formação é detalhada e inclui uma exploração das causas da exposição não intencional de dados. Os utilizadores têm um entendimento completo das diferentes maneiras pelas quais os dados sensíveis podem ser expostos inadvertidamente, desde os cenários mais comuns até os mais complexos. São fornecidos casos de estuado e simulações de cenários para capacitar os utilizadores a reconhecer, prevenir e responder efetivamente a incidentes de exposição não intencional de dados.

**P33:** Na sua organização existe um processo de formação dos utilizadores sobre reconhecimento e comunicação de incidentes de segurança?

- **Nível 1** (Básico) Os membros da equipa não receberam formação sobre os sinais comuns de um potencial incidente de segurança.

- **Nível 2** (Intermédio) Os utilizadores têm uma compreensão dos sinais de alerta que podem indicar a presença de um incidente de segurança. A formação aborda aspetos básicos sobre indicadores de incidentes em potencial e como reconhecê-los.
- **Nível 3** (Avançado) Os utilizadores são treinados para reconhecer até mesmo os sinais mais subtis de atividade maliciosa ou anómala nos sistemas e redes da empresa. A formação pode incluir simulações de incidentes para fornecer aos utilizadores uma experiência prática no reconhecimento e resposta a incidentes.

**P34:** Na sua organização existe um processo de formação dos utilizadores sobre como identificar e comunicar se os seus ativos têm falta de atualizações de segurança?

- **Nível 1** (Básico) Os membros da equipa têm visão geral básica sobre a importância de manter o *software* atualizado.
- **Nível 2** (Intermédio) Os utilizadores conseguem identificar e relatar proactivamente a falta de atualizações de segurança, comunicando com a equipa de TI para a sua aplicação.
- **Nível 3** (Avançado) Os utilizadores são treinados para identificar e relatar não apenas falhas óbvias, mas também possíveis vulnerabilidades ou áreas de melhoria nos processos e ferramentas.

**P35:** Na sua organização existe um processo de formação dos utilizadores sobre os perigos de se ligarem e transmitirem dados corporativos em redes inseguras?

- **Nível 1** (Básico) Os membros da equipa não têm perceção dos perigos.
- **Nível 2** (Intermédio) Existe uma formação básica que aborda os perigos específicos de se ligarem a redes Wi-Fi não seguras e os métodos comuns pelos quais os invasores podem comprometer os dados transmitidos nessas redes.
- **Nível 3** (Avançado) Existe uma formação prática e abrangente que inclui instruções detalhadas sobre como utilizar e configurar redes Wi-Fi seguras, usando métodos seguros de cifragem e autenticação. Estes aprendem a utilizar Redes Virtuais Privadas (VPNs), para proteger os dados transmitidos quando trabalham remotamente.


**Detetar** - Monitorização contínua da rede e dos sistemas procurando identificar atividades suspeitas ou indicadores de comprometimento, permitindo à organização detetar e responder a incidentes de segurança de forma proativa.

**D1:** Na sua organização existe um processo de gestão de *logs*?

- **Nível 1** (Básico) Não existe processo formal de gestão de *log* de auditoria definido e não existe informação dos requisitos de *log* da empresa.
- **Nível 2** (Intermédio) Existe um processo definido para a gestão de *log* de auditoria, mas não é totalmente abrangente ou aplicado consistentemente em toda a organização. A recolha, revisão e retenção de *logs* são tratadas para alguns dos ativos corporativos.
- **Nível 3** (Avançado) Existe um processo implementado em toda a organização para a gestão de *log* de auditoria. A recolha, revisão e retenção de *logs* são tratadas de forma abrangente e consistente para todos os ativos corporativos. Os requisitos de *log* da empresa são claramente definidos, documentados e revistos regularmente para garantir a conformidade contínua com as mudanças na empresa e nas regulamentações.


**Responder** - Resposta rápida e eficaz a incidentes de segurança quando ocorrem, garantindo que a organização possa conter e mitigar os danos causados por uma violação de segurança.

**R1:** Na sua organização existe a designação do responsável (interno ou externo) pelo tratamento e Gestão de Incidentes de Segurança?

- **Nível 1** (Básico) Não existe uma pessoa designada responsável pelo tratamento de incidentes.
- **Nível 2** (Intermédio) Existe uma pessoa designada responsável pelo tratamento de incidentes. A análise do processo de tratamento de incidentes é realizada, mas não é feita regularmente ou de forma sistemática.
- **Nível 3** (Avançado) A empresa designou uma pessoa responsável e pelo menos uma redundante para gerir o processo de tratamento de incidentes. A análise do processo de tratamento de incidentes é realizada regularmente e sempre que ocorrem mudanças significativas na empresa.

**R2:** Na sua organização existe uma lista de contatos para comunicação de Incidentes de Segurança?

- **Nível 1** (Básico) A organização não possuí uma lista de contatos das partes interessadas.
- **Nível 2** (Intermédio) A organização mantém uma lista básica de contatos incluindo utilizadores internos, fornecedores externos, agências governamentais relevantes.
- **Nível 3** (Avançado) A organização mantém uma lista completa e atualizada de contatos de todas as partes interessadas relevantes, incluindo utilizadores internos, fornecedores externos, agências governamentais e seguros de cibersegurança. Além de revisões anuais, há um processo contínuo de verificação e atualização das informações de contato sempre que ocorrerem mudanças relevantes nas partes interessadas. A organização realiza exercícios regulares de simulação de incidentes para testar a eficácia das informações de contato e os procedimentos de resposta.

**R3:** Na sua organização existe um plano de comunicação de incidentes de segurança?

- **Nível 1** (Básico) Não existe definido um processo para comunicar incidentes de segurança.
- **Nível 2** (Intermédio) Existe um processo estabelecido para comunicar incidentes de segurança, mas pode não ser amplamente divulgado ou compreendido.
- **Nível 3** (Avançado) Existe um processo claro e bem divulgado para comunicar incidentes de segurança. O processo inclui um cronograma definido para relatórios, procedimentos claros sobre quem deve comunicar, mecanismos para comunicar e informações mínimas necessárias para os relatórios.

**R4:** Na sua organização existe um plano de recolha de informação sobre eventos de segurança de fontes fidedignas?

- **Nível 1** (Básico) A organização não possuí um plano de informação.
- **Nível 2** (Intermédio) A organização possui um plano que aborda algumas fontes de informação, incluindo *feeds* RSS, alertas de segurança por *e-mail* e grupos de discussão da indústria.
- **Nível 3** (Avançado) A organização mantém um plano de recolha de informação, que inclui o monitorização contínuo de fontes de externas, como *feeds* de inteligência de ameaças, grupos de segurança online e redes sociais. Existe uma abordagem proativa para disseminar informações sobre ameaças à segurança da informação.

**R5:** Na sua organização existe um processo de resposta a incidentes de segurança?

- **Nível 1** (Básico) Não existe definido um processo estabelecido para resposta a incidentes de segurança.
- **Nível 2** (Intermédio) Existe um processo básico de resposta a incidentes de segurança, mas pode ser inconsistente ou incompleto. As funções e responsabilidades estão vagamente definidas, e pode haver falta de requisitos de conformidade.
- **Nível 3** (Avançado) Existe um processo formal de resposta a incidentes, as funções e responsabilidades durante um incidente são claramente definidas, juntamente com requisitos de conformidade e um plano de comunicação abrangente. O processo é revisto anualmente ou quando ocorrem mudanças significativas na empresa, garantindo que esteja sempre atualizado e eficaz na mitigação de incidentes de segurança.

**R6:** Na sua organização existe um processo de remoção de *software* não autorizado?

- **Nível 1** (Básico) Não existe definido um processo para identificar e remover *software* não autorizado.
- **Nível 2** (Intermédio) Existe um processo para identificar e remover *software* não autorizado, mas pode não ser implementado de forma consistente. O *software* não autorizado é identificado ocasionalmente, mas sua remoção nem sempre é realizada prontamente.

- **Nível 3** (Avançado) Existe um processo para identificar e remover prontamente o *software* não autorizado, o processo é executado regularmente, com análises mensais ou até mesmo com maior frequência para garantir a conformidade contínua. O *software* não autorizado é removido prontamente dos ativos corporativos, a menos que uma exceção documentada seja concedida, incluindo uma justificativa e planos de mitigação para reduzir o risco associado.


**Recuperar** - Implementação de planos de recuperação de desastres e a proteção dos dados críticos da organização contra perda, corrupção ou acesso não autorizado, garantindo a continuidade dos negócios após um incidente de segurança.

**Re1:** Na sua organização existe um processo de *backups* automatizados?

- **Nível 1** (Básico) Não existe uma solução de *backup* automatizada e não são realizados regularmente.
- **Nível 2** (Intermédio) São realizados *backups* automatizados, mas a sua frequência pode não ser suficiente para garantir a proteção adequada dos dados.
- **Nível 3** (Avançado) São realizados *backups* automatizado regularmente, com base na sensibilidade dos dados, a frequência de *backup* é ajustada conforme necessário para garantir a proteção adequada dos dados mais sensíveis.

**Re2:** Na sua organização existe um processo de recuperação de dados?

- **Nível 1** (Básico) A organização possuí um processo rudimentar de recuperação de dados, e não está documentado.
- **Nível 2** (Intermédio)A organização possuí um processo documentado de recuperação de dados que aborda o âmbito das atividades de recuperação, incluindo procedimentos para restauração de dados de *backup*.
- **Nível 3** (Avançado) A organização possuí um processo de recuperação de dados detalhado e abrangente, devidamente documentado e acessível a todos os membros relevantes da equipa. O âmbito das atividades de recuperação é

claramente definido, com procedimentos específicos para diferentes tipos de incidentes e sistemas afetados. A priorização da recuperação é cuidadosamente planeada, com uma compreensão clara dos impactos nos negócios e requisitos de tempo de recuperação para diferentes tipos de dados. A segurança dos dados de *backup* é uma prioridade, com medidas robustas de proteção, como cifragem forte, controlo de acesso e armazenamento *offsite* seguro. A documentação é revista e atualizada regularmente, para garantir que permaneça relevante e eficaz diante de mudanças no ambiente de negócios ou nos requisitos regulamentares.

**Re3:** Na sua organização existe uma instância isolada com os dados de *backup*?

- **Nível 1** (Básico) Não há uma instância isolada de dados de recuperação.
- **Nível 2** (Intermédio) Os *backups* estão armazenados no mesmo local ou na mesma rede que os dados originais, existe uma tentativa de manter uma instância isolada de dados de recuperação, mas pode não ser totalmente eficaz.
- **Nível 3** (Avançado) Os *backups* são armazenados em sistemas ou serviços *offline*, na nuvem ou *offsite*, garantindo a sua segurança e disponibilidade mesmo em caso de eventos adversos no local principal.

# B Anexo B – Respostas do Questionário

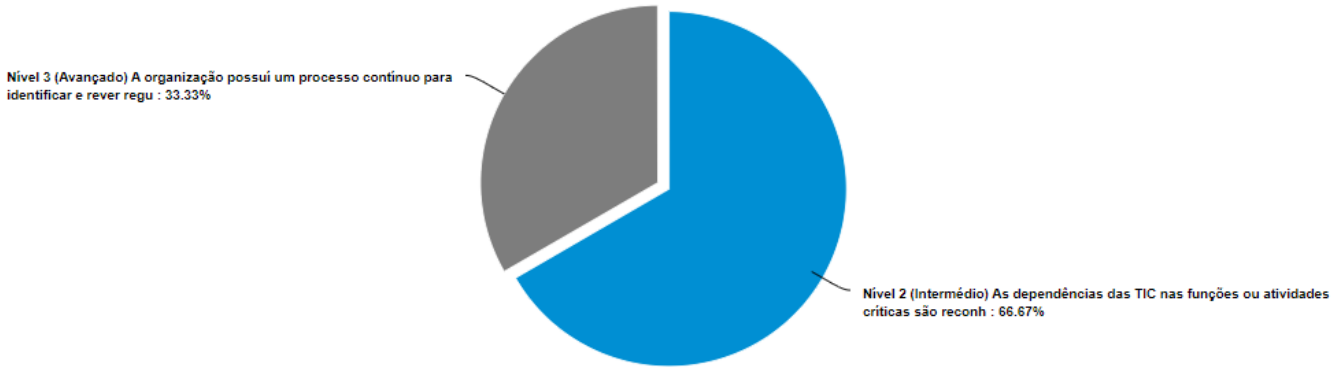
Resumo

| 27 | 23 | 21 | 91.3% | 2 | 15 min |
|---|---|---|---|---|---|
| Visto em | Total de respostas | Concluído | Taxa de conclusão | Desistências | Tempo médio |


| Países | Respostas |
|---|---|
| PT | 100.00% |
| Total | 100.00% |

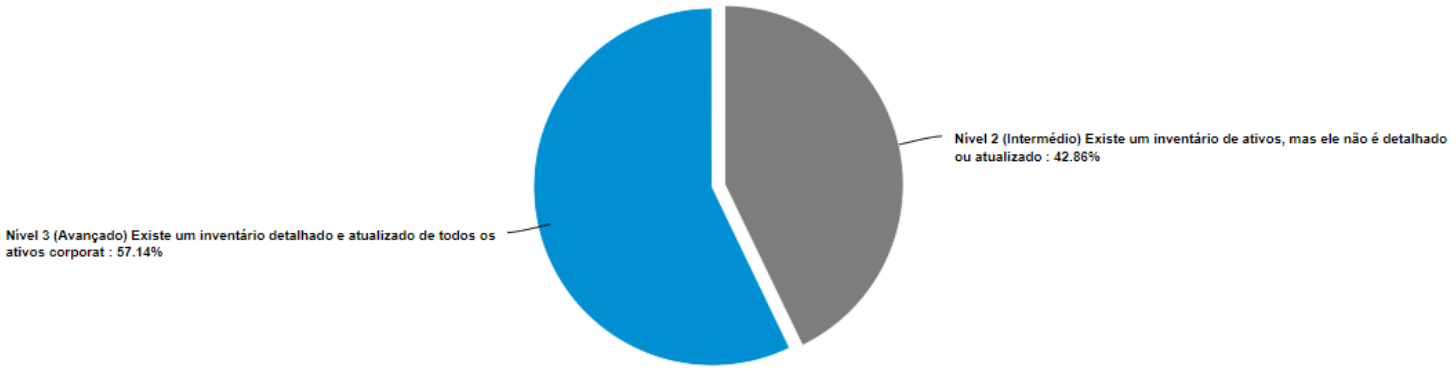
| | | | | |
|---|---|---|---|---|
| 91% Desktop / LAPTOP | 81% Windows | 14% Mac | 5% Linux | 0% Outros |
| 9% SMARTPHONES | 100% Android | 0% iPhone | 0% Windows | 0% Outros |
| 0% TABLETS | 0% iPad | 0% Android | 0% Windows | 0% Outros |

Na sua organização são identificadas as funções ou atividades críticas e respetiva dependência das TIC?



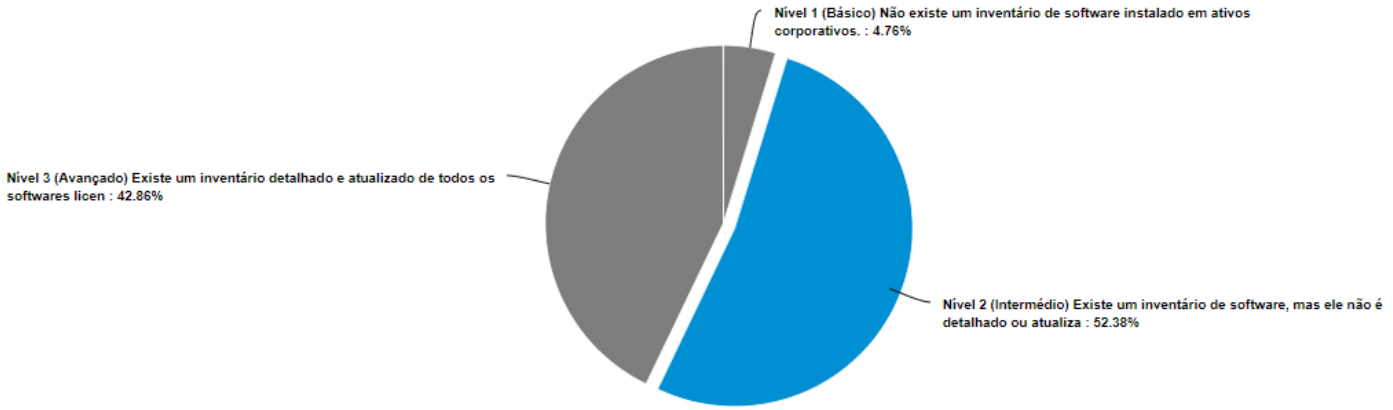

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe identificação das dependências das TIC nas funções ou atividades críticas do negócio. | 0 | 0% | | | | | |
| Nível 2 (Intermédio) As dependências das TIC nas funções ou atividades críticas são reconhecidas de forma geral, mas a identificação completa está incompleta ou desatualizada. | 14 | 66.67% | | | | | |
| Nível 3 (Avançado) A organização possuí um processo contínuo para identificar e rever regularmente funções ou atividades críticas. Além de um documento formal, a organização utiliza ferramentas automatizadas para pesquisar e gerir as relações entre funções críticas, ativos e dependências de TIC. | 7 | 33.33% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização é estabelecido e mantido um inventário detalhado dos ativos corporativos?



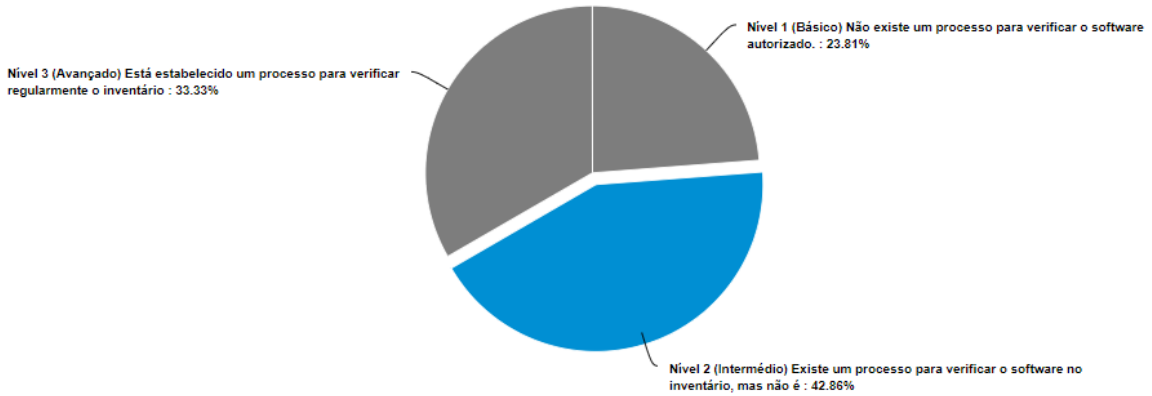

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe um inventário de ativos corporativos. | 0 | 0% | | | | | |
| Nível 2 (Intermédio) Existe um inventário de ativos, mas ele não é detalhado ou atualizado regularmente, as informações essenciais, estão ausentes ou desatualizadas. | 9 | 42.86% | | | | | |
| Nível 3 (Avançado) Existe um inventário detalhado e atualizado de todos os ativos corporativos, incluindo dispositivos de rede (ex: router, switch), dispositivos IoT, Servidores. Este incluí informações como endereço de hardware (MAC), nome da máquina, proprietário e departamento para cada ativo. O inventário é revisto e atualizado semestralmente ou com maior frequência. | 12 | 57.14% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização é estabelecido e mantido um inventário detalhado dos softwares corporativos?




| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe um inventário de software instalado em ativos corporativos. | 1 | 4.76% | | | | | |
| Nível 2 (Intermédio) Existe um inventário de software, mas ele não é detalhado ou atualizado regularmente. As informações essenciais estão incompletas ou desatualizadas. | 11 | 52.38% | | | | | |
| Nível 3 (Avançado) Existe um inventário detalhado e atualizado de todos os softwares licenciados e instalados em ativos corporativos. Este incluí informações como nome, produtor, data de instalação, URL, versão e data de ativação. O inventário é revisto e atualizado semestralmente ou com maior frequência. | 9 | 42.86% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo para utilização exclusiva de software autorizado?

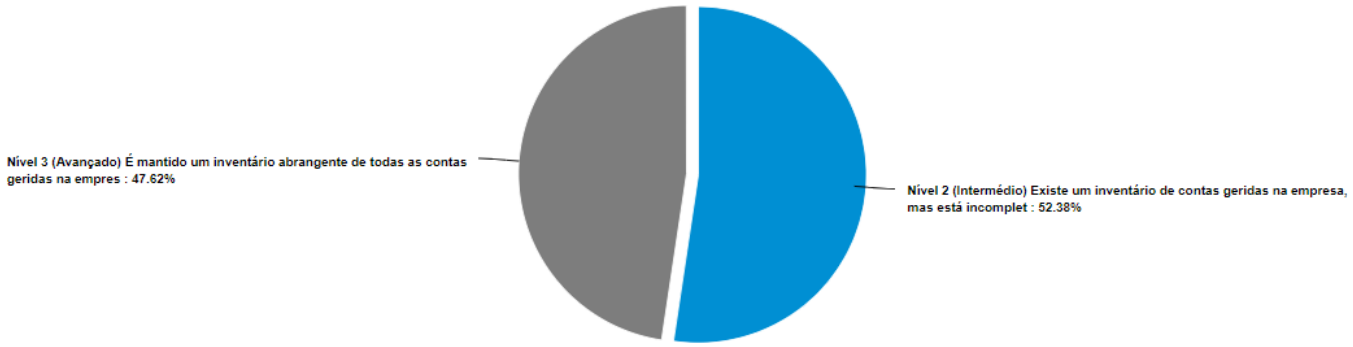



| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe um processo para verificar o software autorizado. | 5 | 23.81% | | | | | |
| Nível 2 (Intermédio) Existe um processo para verificar o software no inventário, mas não é realizado regularmente. O inventário de software é revisto periodicamente, mas ainda existe software não suportado sem documentação de exceção. | 9 | 42.86% | | | | | |
| Nível 3 (Avançado) Está estabelecido um processo para verificar regularmente o inventário de software. O inventário de software é revisto pelo menos uma vez por mês para garantir que apenas software suportado seja designado como autorizado. Softwares não suportado é documentado com exceções detalhadas, incluindo controlos de mitigação e aceitação do risco residual. | 7 | 33.33% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um diagrama de arquitetura do Sistema de Rede?

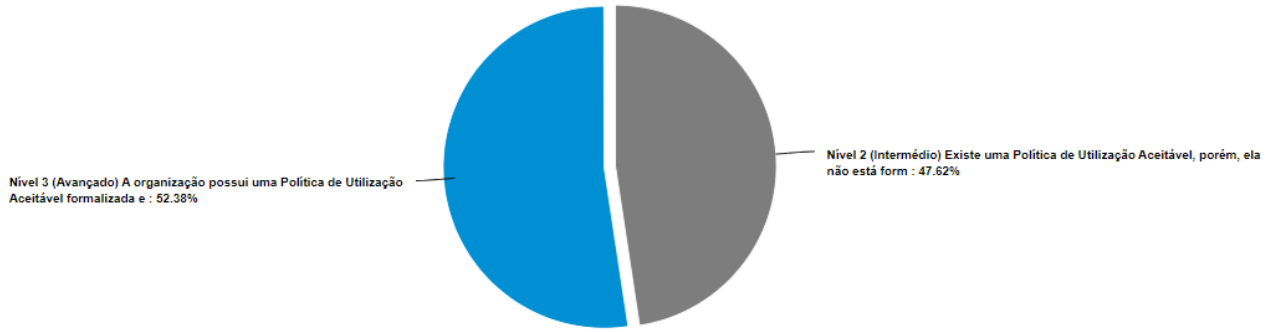

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existem diagramas de arquitetura ou outra documentação da estrutura da rede. | 0 | 0% | | | | | |
| Nível 2 (Intermédio) Existe alguma documentação da estrutura de rede, mas não é revista ou atualizada regularmente. | 12 | 57.14% | | | | | |
| Nível 3 (Avançado) Os diagramas de arquitetura e outra documentação de sistema de rede são mantidos e atualizados regularmente. As alterações significativas são prontamente refletidas na documentação, que é revista anualmente. | 9 | 42.86% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um inventário de contas de sistemas de TI?



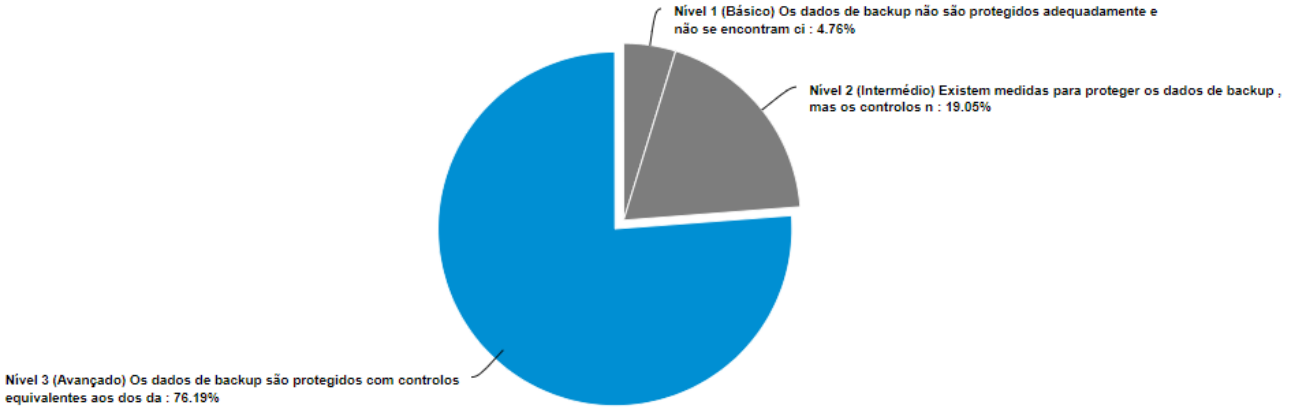

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe um inventário das contas geridas na empresa. | 0 | 0% | | | | | |
| Nível 2 (Intermédio) Existe um inventário de contas geridas na empresa, mas está incompleto ou desatualizado. Algumas informações básicas, como nome de utilizador e departamento, estão registadas, mas não existe validação regular para garantir a precisão dos registos. | 11 | 52.38% | | | | | |
| Nível 3 (Avançado) É mantido um inventário abrangente de todas as contas geridas na empresa. O inventário inclui detalhes como nome da pessoa, datas de início/término, assim como o departamento. As contas ativas são validadas regularmente para garantir que estejam autorizadas, com uma periodicidade recorrente de no mínimo trimestralmente ou com maior frequência. | 10 | 47.62% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe uma Política de Uso Aceitável dos Sistemas Informáticos?



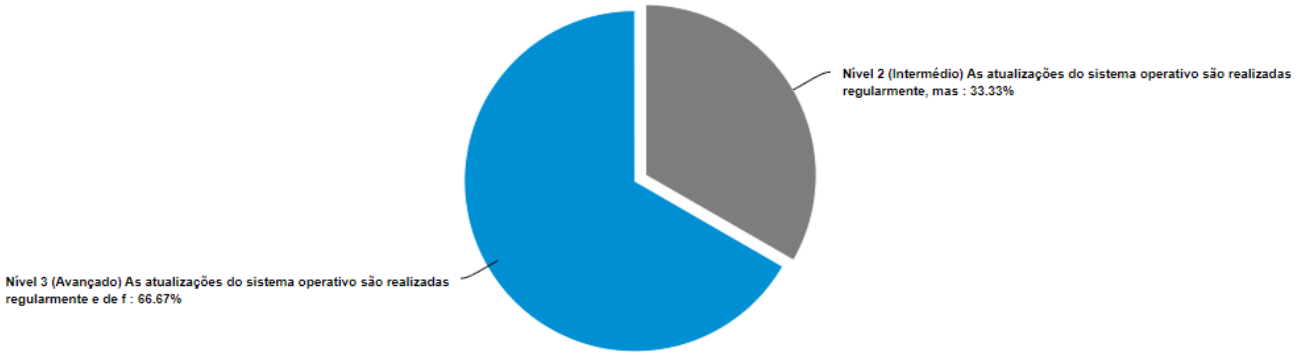

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) A organização não possui uma Política de Utilização Aceitável dos recursos de TI. | 0 | 0% | | | | | |
| Nível 2 (Intermédio) Existe uma Política de Utilização Aceitável, porém, ela não está formalizada num documento. As diretrizes para o uso seguro dos recursos de TI estão disponíveis de forma dispersa ou não são claramente comunicadas a todos os colaboradores. | 10 | 47.62% | | | | | |
| Nível 3 (Avançado) A organização possui uma Política de Utilização Aceitável formalizada e documentada. As diretrizes para o uso seguro dos recursos de TI são claramente definidas e comunicadas a todos os colaboradores. A política aborda uma variedade de cenários, incluindo uso de dispositivos pessoais, acesso a redes Wi-Fi externas, uso de e-mail e internet, entre outros. As consequências do não cumprimento da política são claras e aplicadas de forma consistente. | 11 | 52.38% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de proteção dos dados de backup?



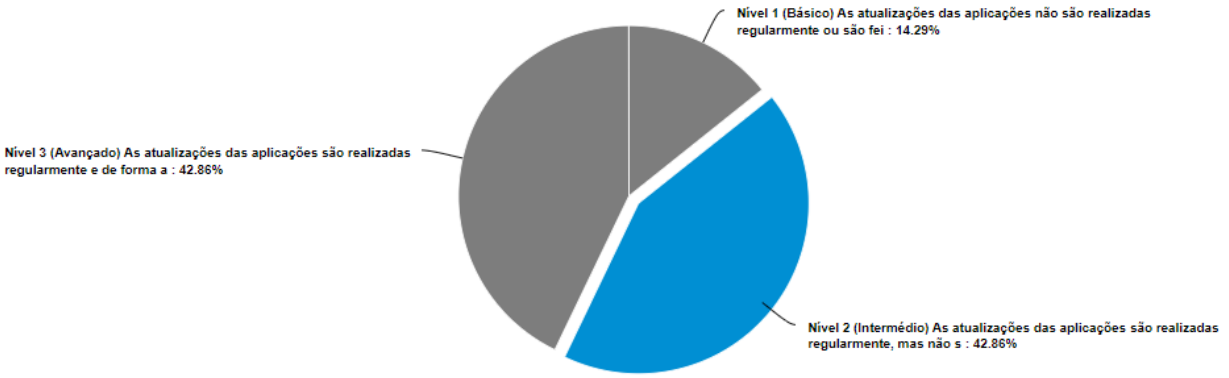

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Os dados de backup não são protegidos adequadamente e não se encontram cifrados. | 1 | 4.76% | | | | | |
| Nível 2 (Intermédio) Existem medidas para proteger os dados de backup , mas os controlos não são equivalentes aos dos dados originais. Existe o uso de cifragem ou segregação de dados, mas não está implementado consistentemente. | 4 | 19.05% | | | | | |
| Nível 3 (Avançado) Os dados de backup são protegidos com controlos equivalentes aos dos dados originais. A cifragem e segregação de dados é implementada de forma consistente e adequada para garantir a sua segurança. | 16 | 76.19% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe uma gestão automatizada de updates dos Sistemas Operativos?



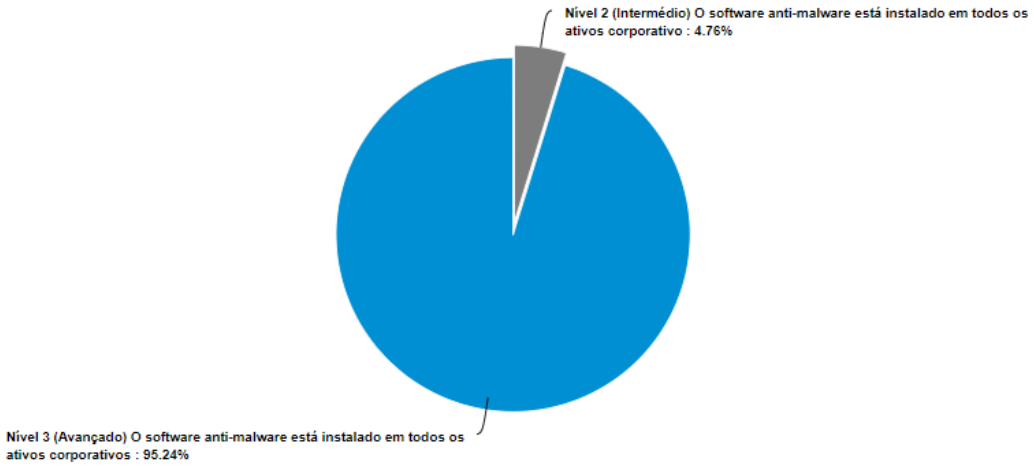

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) As atualizações do sistema operativo não são realizadas regularmente ou são feitas de forma manual. | 0 | 0% | | | | | |
| Nível 2 (Intermédio) As atualizações do sistema operativo são realizadas regularmente, mas não são automatizadas. Existe um processo informal para aplicar patches de segurança, mas não é feito mensalmente ou com maior frequência de forma consistente. | 7 | 33.33% | | | | | |
| Nível 3 (Avançado) As atualizações do sistema operativo são realizadas regularmente e de forma automatizada. Existe um processo formal estabelecido para aplicar patches de segurança mensalmente ou com maior frequência, garantindo a proteção contínua dos ativos corporativos. | 14 | 66.67% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe uma gestão automatizada de updates das aplicações?



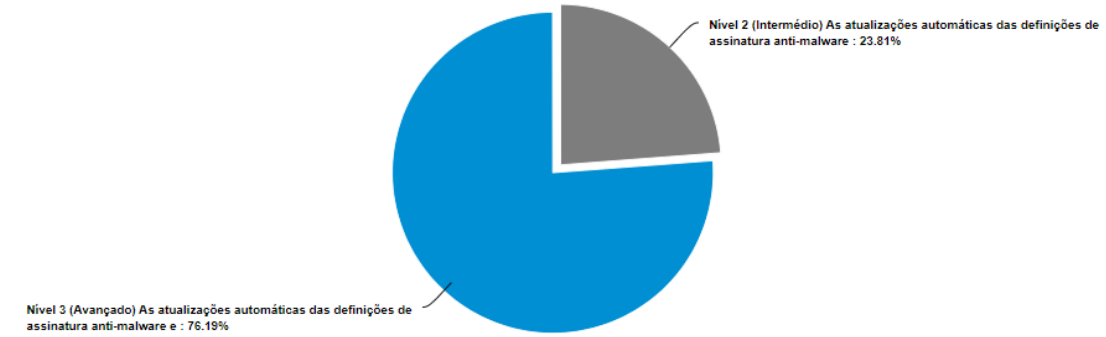

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) As atualizações das aplicações não são realizadas regularmente ou são feitas de forma manual. | 3 | 14.29% | | | | | |
| Nível 2 (Intermédio) As atualizações das aplicações são realizadas regularmente, mas não são automatizadas. Existe um processo informal para aplicar patches das aplicações, mas não é feito mensalmente ou com maior frequência de forma consistente. | 9 | 42.86% | | | | | |
| Nível 3 (Avançado) As atualizações das aplicações são realizadas regularmente e de forma automatizada. Existe um processo formal estabelecido para aplicar patches das aplicações mensalmente ou com maior frequência, garantindo a segurança contínua dos ativos corporativos | 9 | 42.86% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe uma solução de anti-malware?



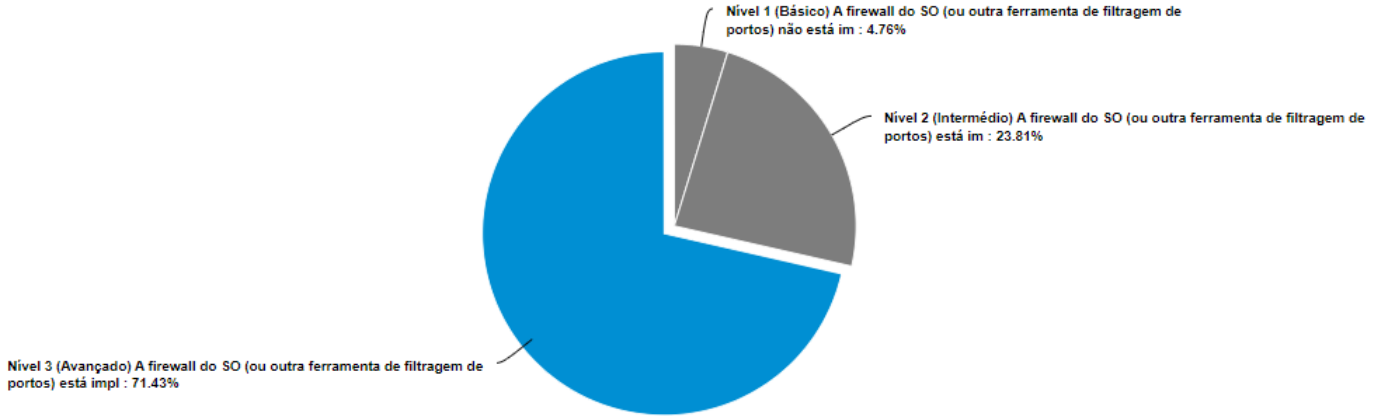

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) O software anti-malware não está instalado em todos os ativos corporativos. | 0 | 0% | | | | | |
| Nível 2 (Intermédio) O software anti-malware está instalado em todos os ativos corporativos, mas não é mantido regularmente ou atualizado automaticamente. | 1 | 4.76% | | | | | |
| Nível 3 (Avançado) O software anti-malware está instalado em todos os ativos corporativos e é mantido regularmente e atualizado automaticamente. Existe um processo formal estabelecido para manter e atualizar o software anti-malware, garantindo a proteção contínua contra ameaças de segurança. | 20 | 95.24% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização a solução de anti-malware tem atualizações das assinaturas automáticas?



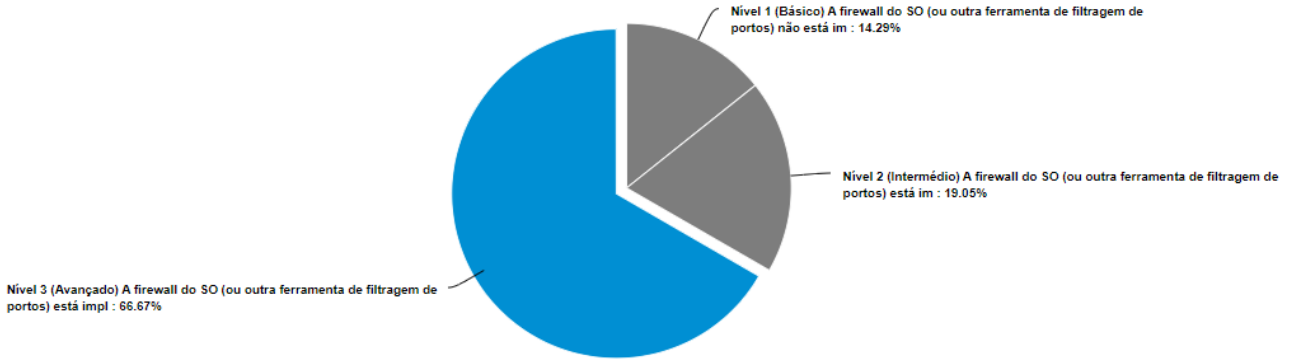

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) As atualizações automáticas das definições de assinatura anti-malware não estão configuradas em todos os ativos corporativos, ou não existe essa informação centralmente. | 0 | 0% | | | | | |
| Nível 2 (Intermédio) As atualizações automáticas das definições de assinatura anti-malware estão parcialmente configuradas em alguns ativos corporativos, mas não são consistentes em toda a organização. | 5 | 23.81% | | | | | |
| Nível 3 (Avançado) As atualizações automáticas das definições de assinatura anti-malware estão configuradas em todos os ativos corporativos e são aplicadas regularmente. Há um processo formal estabelecido para garantir que as atualizações de assinatura anti-malware sejam aplicadas automaticamente em todos os ativos corporativos, garantindo a proteção contínua contra ameaças de segurança. | 16 | 76.19% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização nos servidores encontra-se aplicada a firewall do Sistema Operativo (SO)?



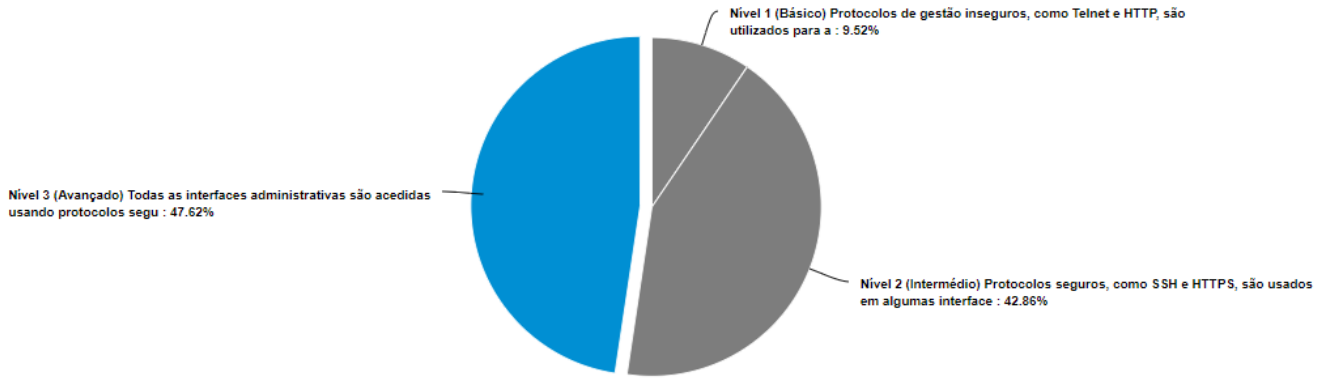

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) A firewall do SO (ou outra ferramenta de filtragem de portos) não está implementada em nenhum servidor. | 1 | 4.76% | | | | | |
| Nível 2 (Intermédio) A firewall do SO (ou outra ferramenta de filtragem de portos) está implementada em alguns servidores onde é suportada, mas não é consistente em toda a infraestrutura. | 5 | 23.81% | | | | | |
| Nível 3 (Avançado) A firewall do SO (ou outra ferramenta de filtragem de portos) está implementada em todos os servidores onde é suportada e é gerida de forma proativa. Existe um plano estabelecido para implementar e gerir a firewall nos servidores. | 15 | 71.43% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização nos postos dos utilizadores encontra-se aplicada a firewall do Sistema Operativo (SO)?



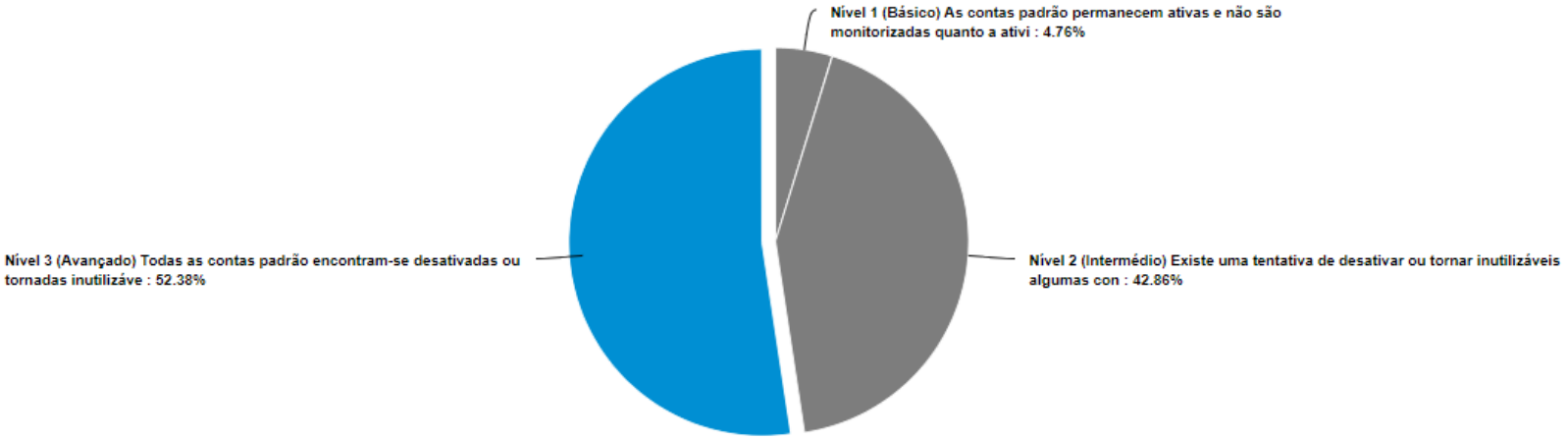

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) A firewall do SO (ou outra ferramenta de filtragem de portos) não está implementada nos dispositivos dos utilizadores finais. | 3 | 14.29% | | | | | |
| Nível 2 (Intermédio) A firewall do SO (ou outra ferramenta de filtragem de portos) está implementada em alguns dispositivos dos utilizadores finais, mas não está aplicada de forma uniforme em todos os dispositivos. | 4 | 19.05% | | | | | |
| Nível 3 (Avançado) A firewall do SO (ou outra ferramenta de filtragem de portos) está implementada em todos os dispositivos dos utilizadores finais e é gerida de forma proativa. Existe uma regra de negação padrão configurada que bloqueia todo o tráfego, exceto os serviços e portos explicitamente permitidos. | 14 | 66.67% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização os protocolos de gestão inseguros encontram-se desabilitados?



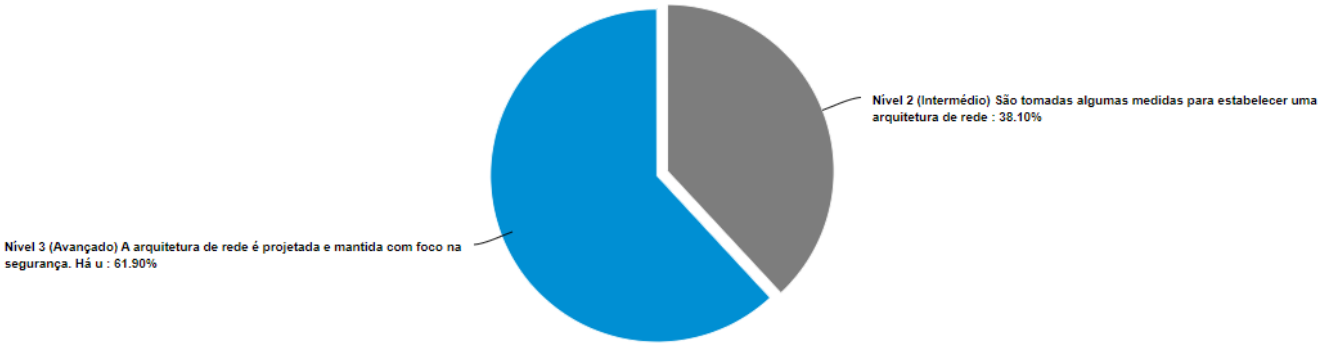

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Protocolos de gestão inseguros, como Telnet e HTTP, são utilizados para acesso às interfaces administrativas. | 2 | 9.52% | | | | | |
| Nível 2 (Intermédio) Protocolos seguros, como SSH e HTTPS, são usados em algumas interfaces administrativas, mas ainda existem instâncias de Telnet e HTTP a serem usadas. Há algumas medidas para gerir os ativos e software corporativos de forma segura, mas são inconsistentes. | 9 | 42.86% | | | | | |
| Nível 3 (Avançado) Todas as interfaces administrativas são acedidas usando protocolos seguros, como SSH e HTTPS. São tomadas medidas para evitar o uso de protocolos inseguros, a menos que estritamente necessário para operações críticas. | 10 | 47.62% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

## Na sua organização as contas padrão encontram-se desabilitadas?



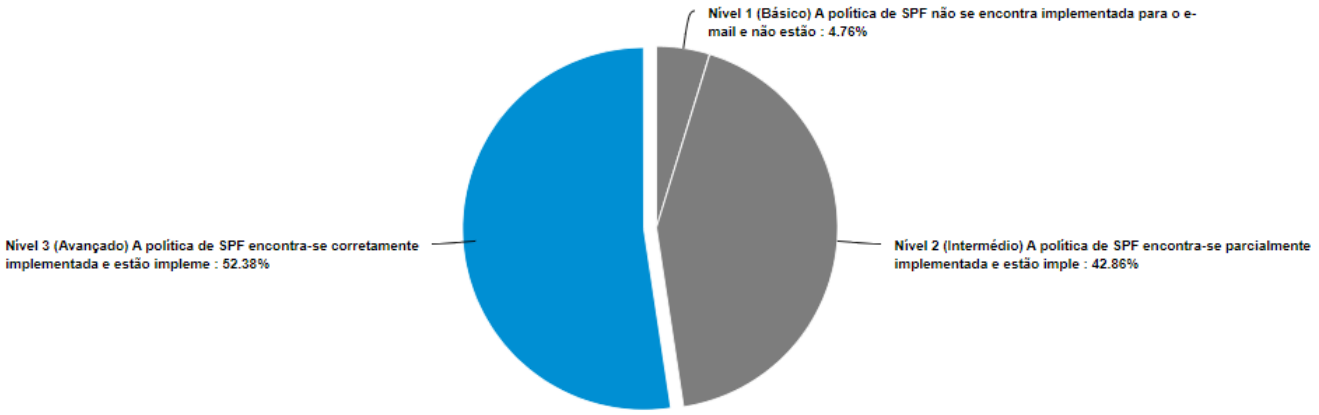

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) As contas padrão permanecem ativas e não são monitorizadas quanto a atividades suspeitas. | 1 | 4.76% | | | | | |
| Nível 2 (Intermédio) Existe uma tentativa de desativar ou tornar inutilizáveis algumas contas padrão, mas isso não é feito de forma sistemática em todos os ativos e software corporativos. | 9 | 42.86% | | | | | |
| Nível 3 (Avançado) Todas as contas padrão encontram-se desativadas ou tornadas inutilizáveis em todos os ativos e software corporativos. | 11 | 52.38% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização é mantida uma arquitetura de rede segura?



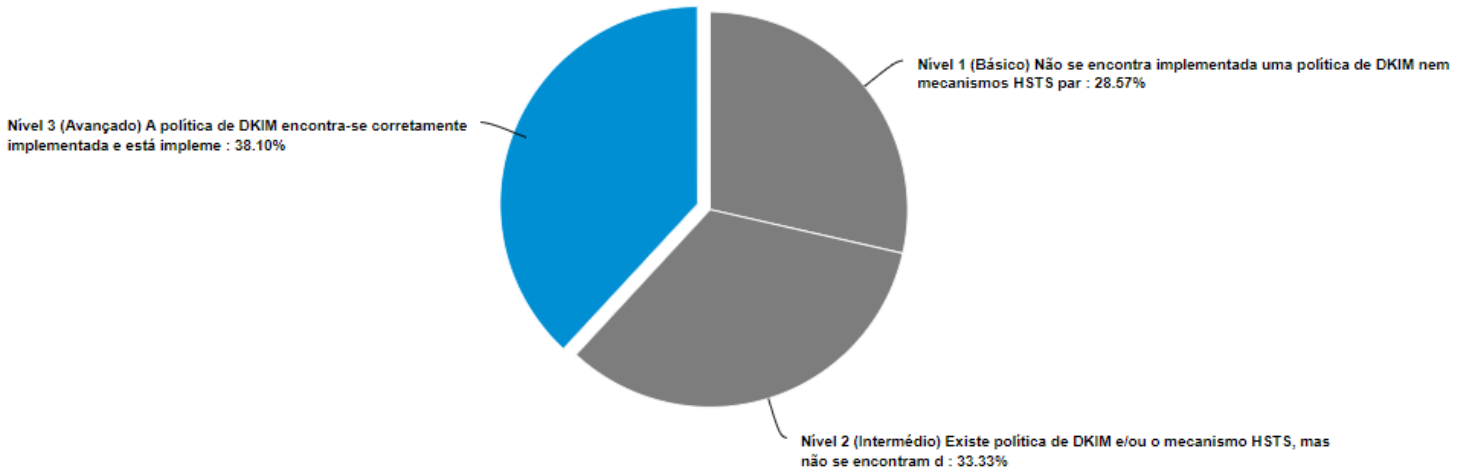

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) A arquitetura de rede não é projetada com foco na segurança. Não existe segmentação adequada da rede e os princípios de privilégio mínimo não são aplicados. | 0 | 0% | | | | | |
| Nível 2 (Intermédio) São tomadas algumas medidas para estabelecer uma arquitetura de rede segura, mas são inconsistentes. Existe alguma segmentação na rede, mas os princípios de privilégio mínimo não são totalmente implementados. | 8 | 38.1% | | | | | |
| Nível 3 (Avançado) A arquitetura de rede é projetada e mantida com foco na segurança. Há uma segmentação clara e bem definida da rede, juntamente com a aplicação dos princípios de privilégio mínimo para garantir que apenas as partes autorizadas tenham acesso apenas aos recursos necessários. | 13 | 61.9% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização é aplicado a Sender Policy Framework (SPF) e HTTPS?



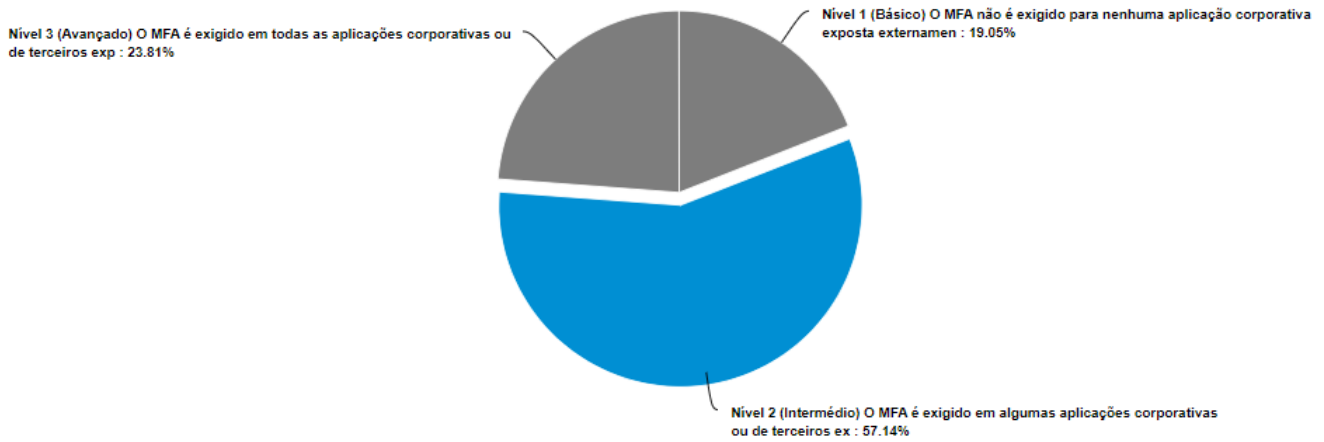

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) A política de SPF não se encontra implementada para o e-mail e não estão implementados certificados digitais para acesso a recursos HTTPS corporativos. | 1 | 4.76% | | | | | |
| Nível 2 (Intermédio) A política de SPF encontra-se parcialmente implementada e estão implementados certificados digitais para acesso a recursos HTTPS corporativos. | 9 | 42.86% | | | | | |
| Nível 3 (Avançado) A política de SPF encontra-se corretamente implementada e estão implementados certificados digitais para acesso a recursos HTTPS corporativos. | 11 | 52.38% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização é aplicado o DomainKeys Identified Mail (DKIM) e HTTP Strict Transport Security (HSTS)?



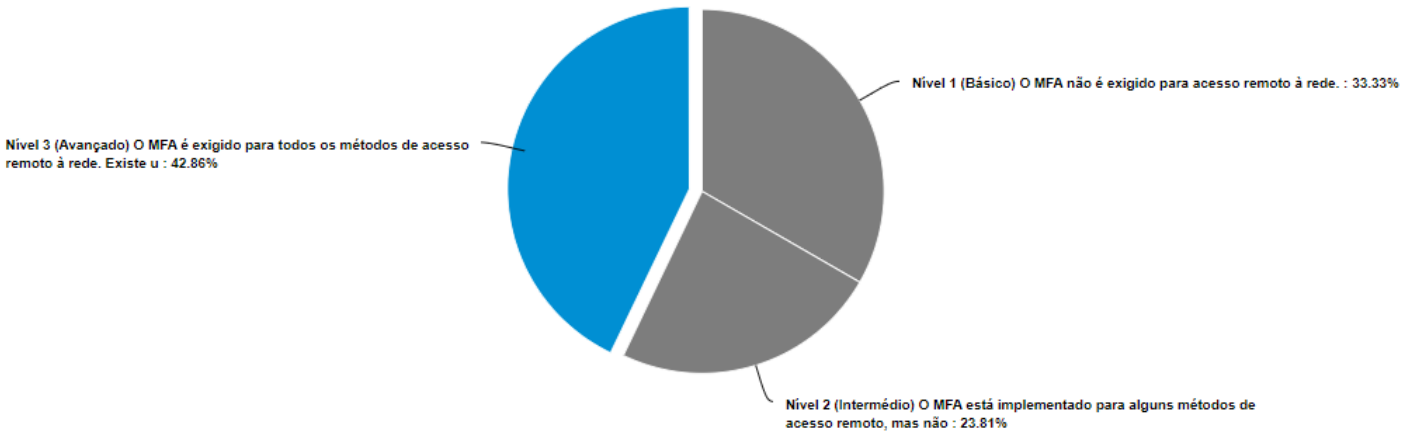

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não se encontra implementada uma política de DKIM nem mecanismos HSTS para acesso aos ativos corporativos. | 6 | 28.57% | | | | | |
| Nível 2 (Intermédio) Existe política de DKIM e/ou o mecanismo HSTS, mas não se encontram devidamente implementados. | 7 | 33.33% | | | | | |
| Nível 3 (Avançado) A política de DKIM encontra-se corretamente implementada e está implementado o mecanismo HSTS para acesso aos ativos corporativos. | 8 | 38.1% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização é exigido Multifator de Autenticação (MFA) para aplicações expostas externamente?



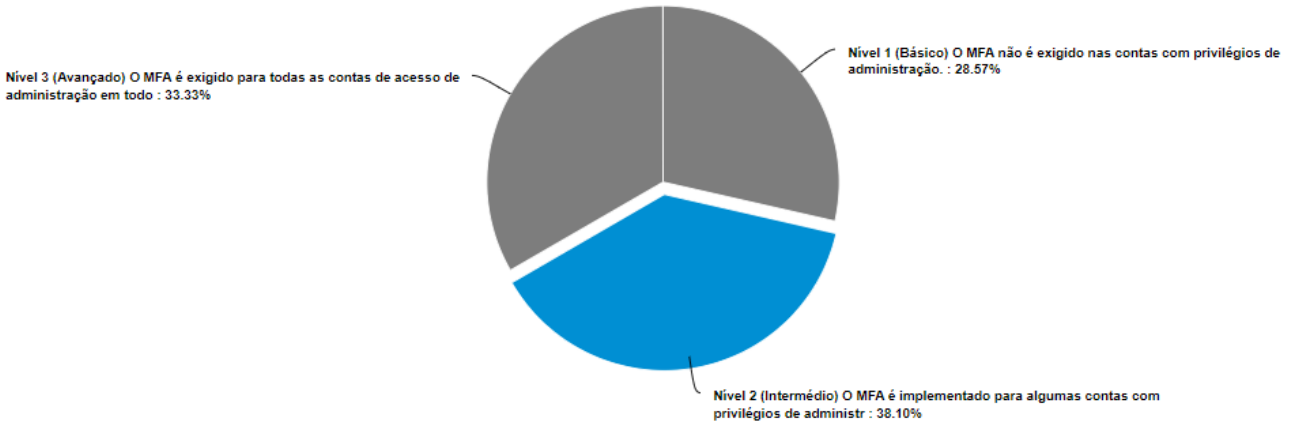

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) O MFA não é exigido para nenhuma aplicação corporativa exposta externamente. | 4 | 19.05% | | | | | |
| Nível 2 (Intermédio) O MFA é exigido em algumas aplicações corporativas ou de terceiros expostas externamente, mas não é aplicado consistentemente em todas. | 12 | 57.14% | | | | | |
| Nível 3 (Avançado) O MFA é exigido em todas as aplicações corporativas ou de terceiros expostas externamente, onde suportado. Existe um processo formal estabelecido para garantir que o MFA seja implementado de forma consistente e eficaz em todas as aplicações. | 5 | 23.81% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização é exigido Multifator de Autenticação (MFA) para acesso remoto à rede?



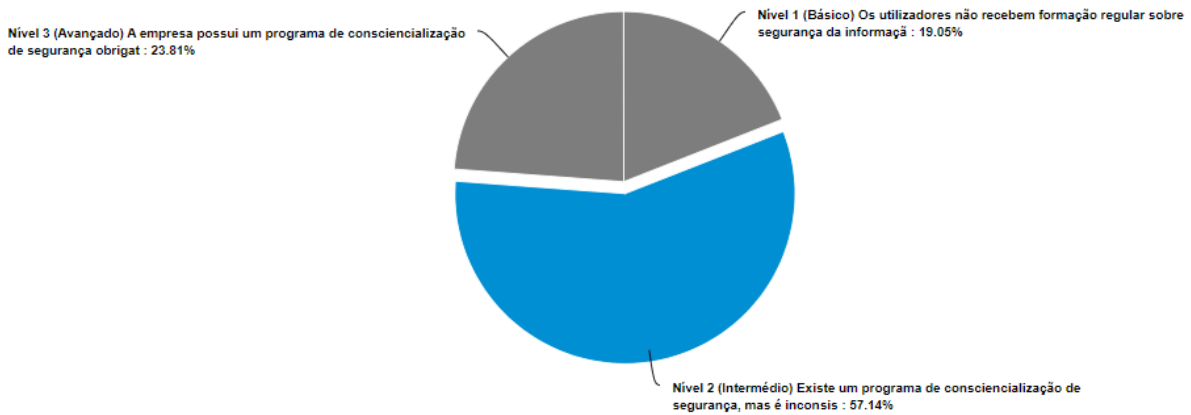

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) O MFA não é exigido para acesso remoto à rede. | 7 | 33.33% | | | | | |
| Nível 2 (Intermédio) O MFA está implementado para alguns métodos de acesso remoto, mas não para todos. Existe uma política parcial para exigir MFA em determinadas situações de acesso remoto, mas não é aplicada consistentemente. | 5 | 23.81% | | | | | |
| Nível 3 (Avançado) O MFA é exigido para todos os métodos de acesso remoto à rede. Existe uma política que garante que todos os utilizadores se autentiquem com MFA ao aceder remotamente à rede corporativa. | 9 | 42.86% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização é exigido Multifator de Autenticação (MFA) para acesso de administração?



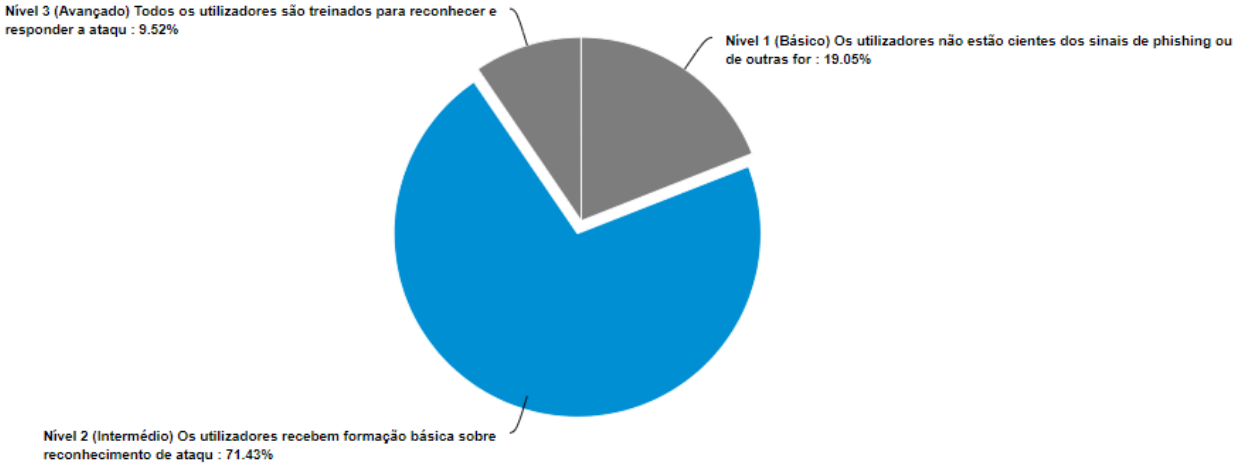

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) O MFA não é exigido nas contas com privilégios de administração. | 6 | 28.57% | | | | | |
| Nível 2 (Intermédio) O MFA é implementado para algumas contas com privilégios de administração. | 8 | 38.1% | | | | | |
| Nível 3 (Avançado) O MFA é exigido para todas as contas de acesso de administração em todos os ativos corporativos, independentemente de serem geridos localmente ou por meio de um fornecedor externo. Existe uma política que garante que todas as contas com privilégios de administração sejam protegidas por MFA, independentemente de onde os ativos estão localizados. | 7 | 33.33% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um programa de consciencialização de segurança?



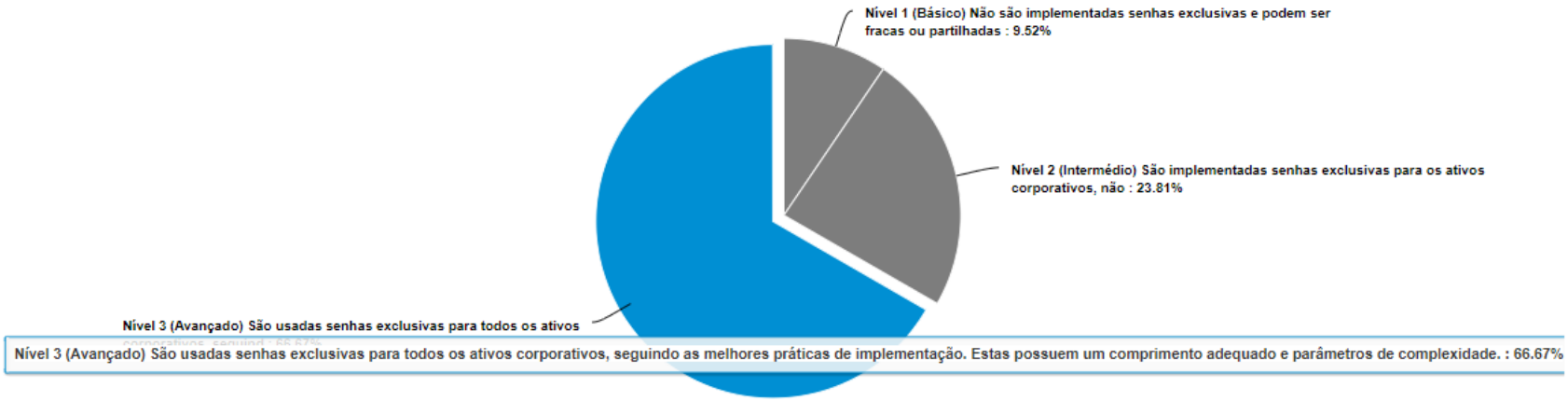

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Os utilizadores não recebem formação regular sobre segurança da informação. | 4 | 19.05% | | | | | |
| Nível 2 (Intermédio) Existe um programa de consciencialização de segurança, mas é inconsistente ou não obrigatório. A formação é fornecida aquando do processo de contratação, mas não regularmente. | 12 | 57.14% | | | | | |
| Nível 3 (Avançado) A empresa possui um programa de consciencialização de segurança obrigatório para todos os utilizadores. A formação é realizada na contratação e anualmente, o conteúdo é regularmente analisado e atualizado para refletir as mudanças nas ameaças de segurança e nas políticas da empresa. | 5 | 23.81% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um programa de consciencialização para reconhecer ataques de engenharia social?



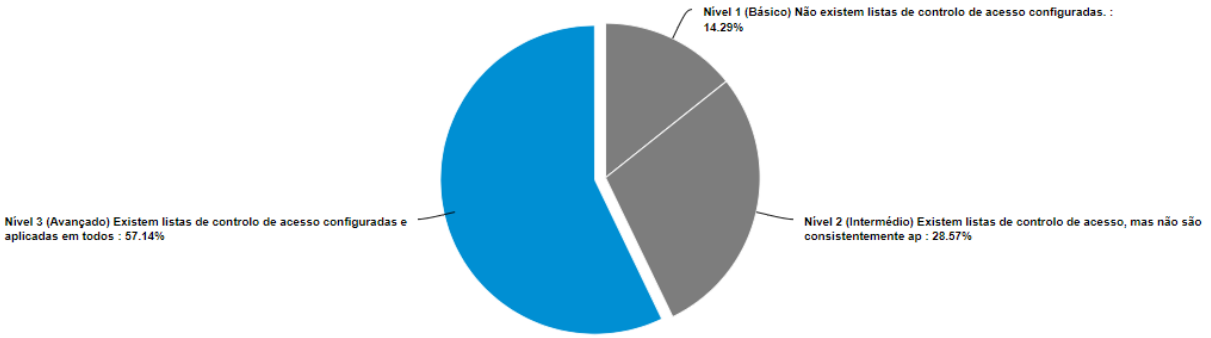

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Os utilizadores não estão cientes dos sinais de phishing ou de outras formas de engenharia social. | 4 | 19.05% | | | | | |
| Nível 2 (Intermédio) Os utilizadores recebem formação básica sobre reconhecimento de ataques de engenharia social. | 15 | 71.43% | | | | | |
| Nível 3 (Avançado) Todos os utilizadores são treinados para reconhecer e responder a ataques de engenharia social, incluindo os vários tipos phishing . A formação é contínua e abrangente, com simulações regulares e outros exercícios práticos para reforçar a consciencialização. | 2 | 9.52% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização são utilizadas senhas exclusivas para os ativos corporativos?



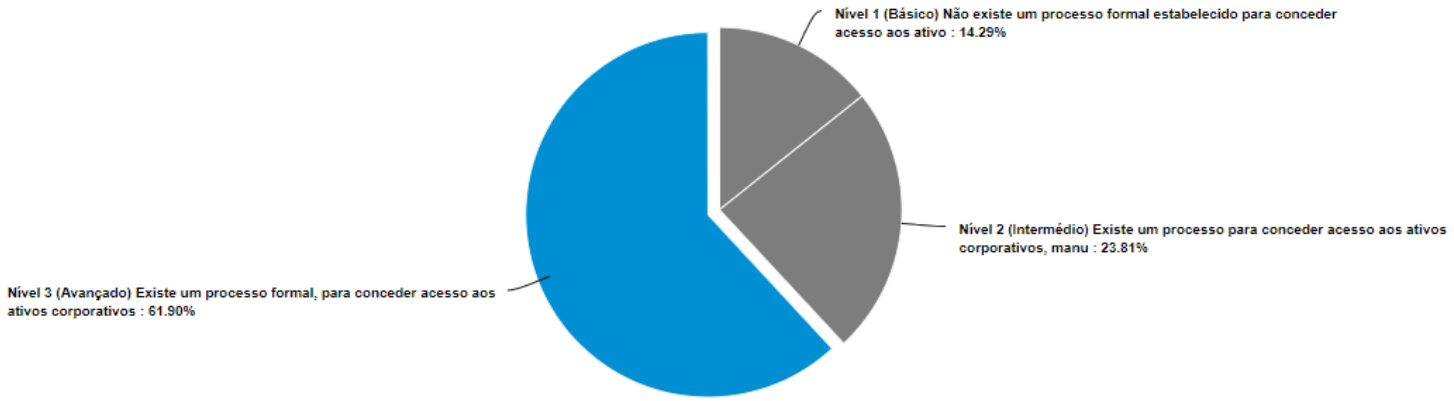

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não são implementadas senhas exclusivas e podem ser fracas ou partilhadas entre vários ativos. | 2 | 9.52% | | | | | |
| Nível 2 (Intermédio) São implementadas senhas exclusivas para os ativos corporativos, não apresentam os requisitos mínimos de comprimento, ou não serem suficientemente complexas. | 5 | 23.81% | | | | | |
| Nível 3 (Avançado) São usadas senhas exclusivas para todos os ativos corporativos, seguindo as melhores práticas de implementação. Estas possuem um comprimento adequado e parâmetros de complexidade. | 14 | 66.67% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existem listas de controlo de acesso a dados?



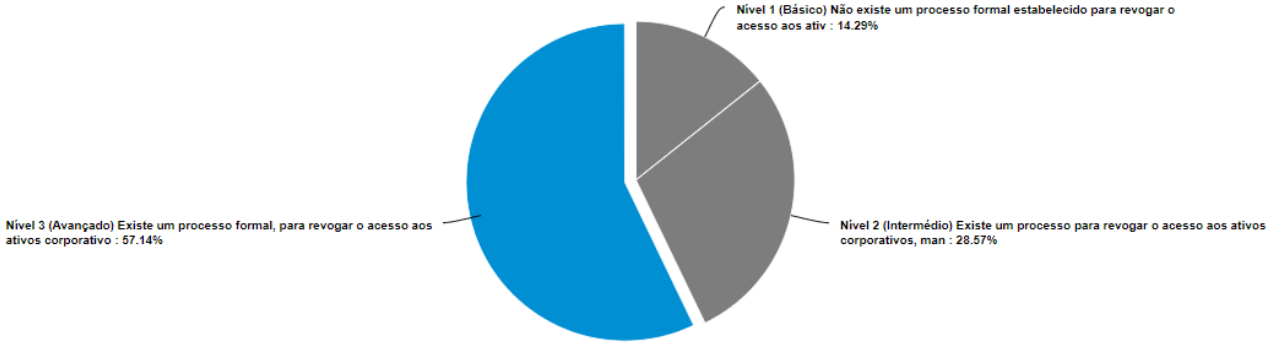

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existem listas de controlo de acesso configuradas. | 3 | 14.29% | | | | | |
| Nível 2 (Intermédio) Existem listas de controlo de acesso, mas não são consistentemente aplicadas em todos os sistemas e aplicações. As permissões de acesso são definidas de forma genérica, sem considerar adequadamente a necessidade de conhecimento do utilizador. | 6 | 28.57% | | | | | |
| Nível 3 (Avançado) Existem listas de controlo de acesso configuradas e aplicadas em todos os sistemas de ficheiros, bases de dados e aplicações. As permissões de acesso são geridas de acordo com a necessidade de conhecimento do utilizador, garantindo que apenas utilizadores autorizados tenham acesso aos dados relevantes para as suas funções. As políticas de controlo de acesso são revistas regularmente e ajustadas conforme necessário para garantir a segurança contínua dos dados corporativos. | 12 | 57.14% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de concessão de acessos?



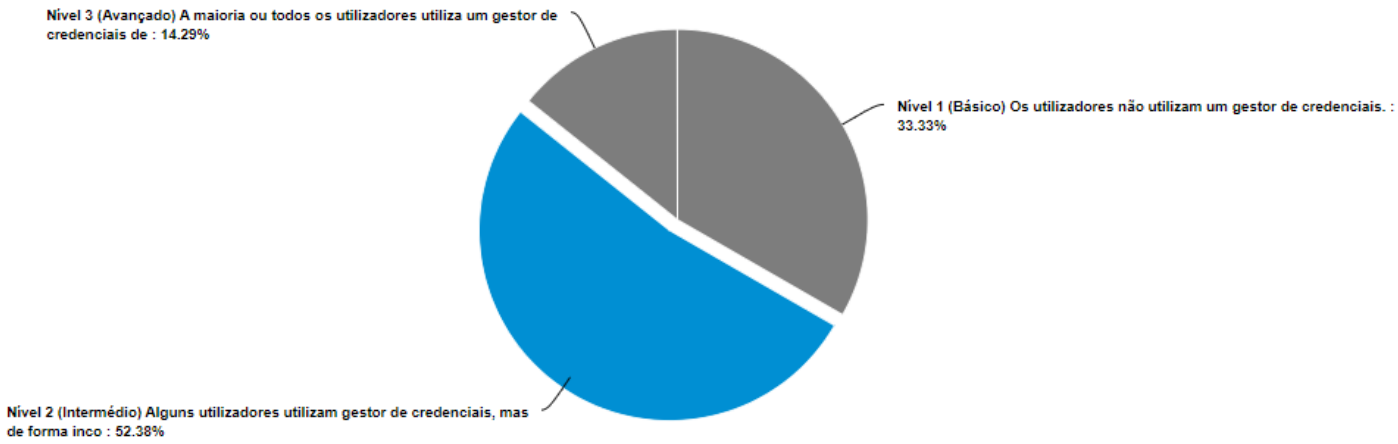

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe um processo formal estabelecido para conceder acesso aos ativos corporativos. | 3 | 14.29% | | | | | |
| Nível 2 (Intermédio) Existe um processo para conceder acesso aos ativos corporativos, manual e sujeito a inconsistências. | 5 | 23.81% | | | | | |
| Nível 3 (Avançado) Existe um processo formal, para conceder acesso aos ativos corporativos. O processo garante que novas contratações, concessões de direitos ou mudanças de função de utilizadores são rapidamente refletidas no acesso aos recursos corporativos, reduzindo assim o tempo de inatividade e o risco de acesso não autorizado. | 13 | 61.9% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de revogação de acessos?



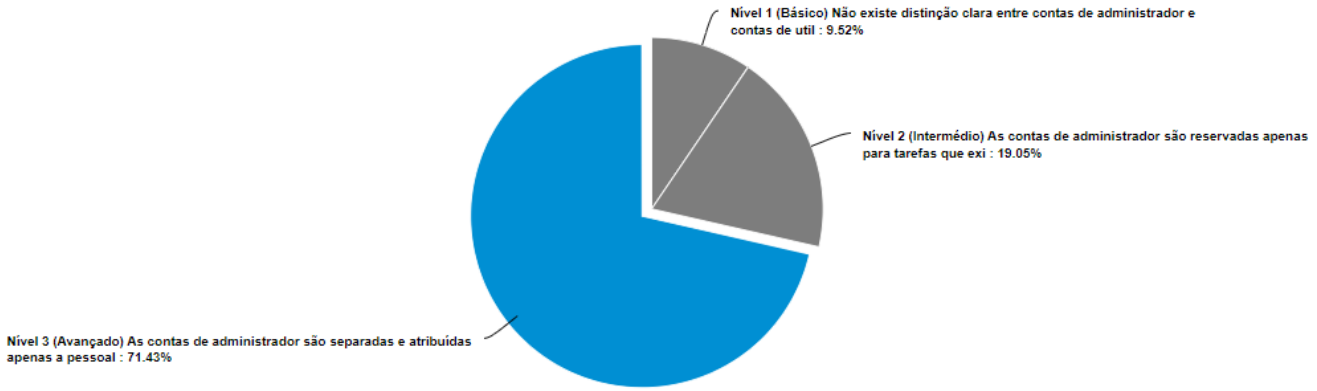

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe um processo formal estabelecido para revogar o acesso aos ativos corporativos. | 3 | 14.29% | | | | | |
| Nível 2 (Intermédio) Existe um processo para revogar o acesso aos ativos corporativos, manual e sujeito a erros. A desativação de contas é realizada, mas existe falta de automação ou atrasos na revogação de direitos de acesso. | 6 | 28.57% | | | | | |
| Nível 3 (Avançado) Existe um processo formal, para revogar o acesso aos ativos corporativos. As contas são desativadas imediatamente após o encerramento, revogação de direitos ou mudança de função de um utilizador, enquanto os registos de auditoria são mantidos. O processo garante que o acesso não autorizado seja prontamente removido, reduzindo assim o risco de violações de segurança e conformidade. | 12 | 57.14% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização são utilizados gestores de credenciais?



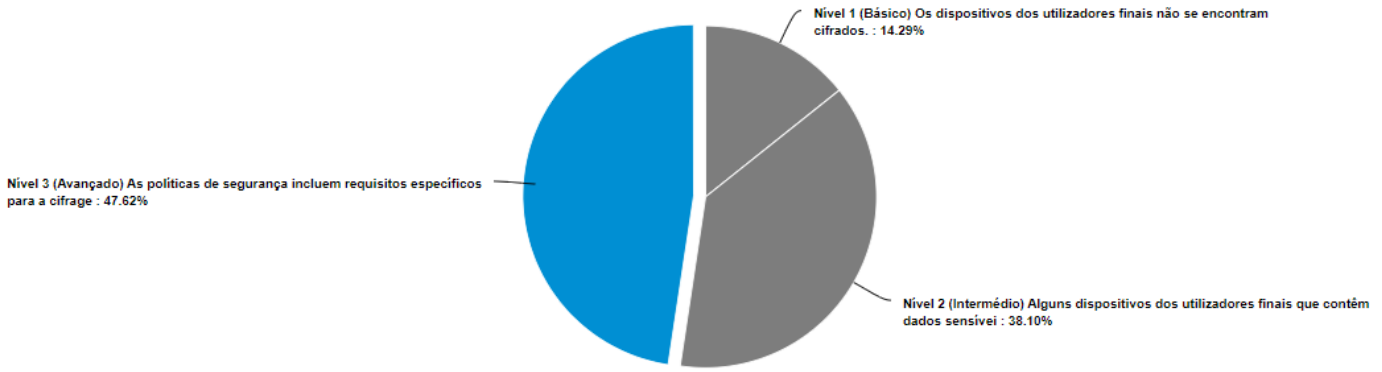

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Os utilizadores não utilizam um gestor de credenciais. | 7 | 33.33% | | | | | |
| Nível 2 (Intermédio) Alguns utilizadores utilizam gestor de credenciais, mas de forma inconsistente. | 11 | 52.38% | | | | | |
| Nível 3 (Avançado) A maioria ou todos os utilizadores utiliza um gestor de credenciais de forma consistente. São utilizadas senhas complexas e exclusivas. Os utilizadores têm formação regularmente sobre as melhores práticas de segurança relacionadas com o uso de gestor de credenciais. | 3 | 14.29% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existem contas de Administração dedicadas?



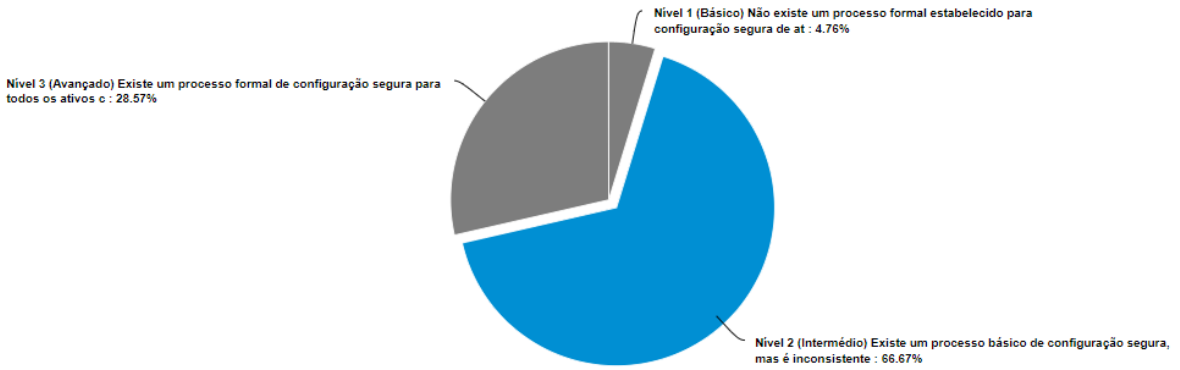

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe distinção clara entre contas de administrador e contas de utilizador comuns. | 2 | 9.52% | | | | | |
| Nível 2 (Intermédio) As contas de administrador são reservadas apenas para tarefas que exigem privilégios elevados, como instalação de software ou alterações de configuração. Os utilizadores são incentivados a usar contas de utilizador comuns para atividades gerais. | 4 | 19.05% | | | | | |
| Nível 3 (Avançado) As contas de administrador são separadas e atribuídas apenas a pessoal autorizado. Está implementada uma política, instruindo os utilizadores a realizar as atividades gerais com a sua conta não privilegiada. | 15 | 71.43% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização os dispositivos dos utilizadores finais encontram-se cifrados?



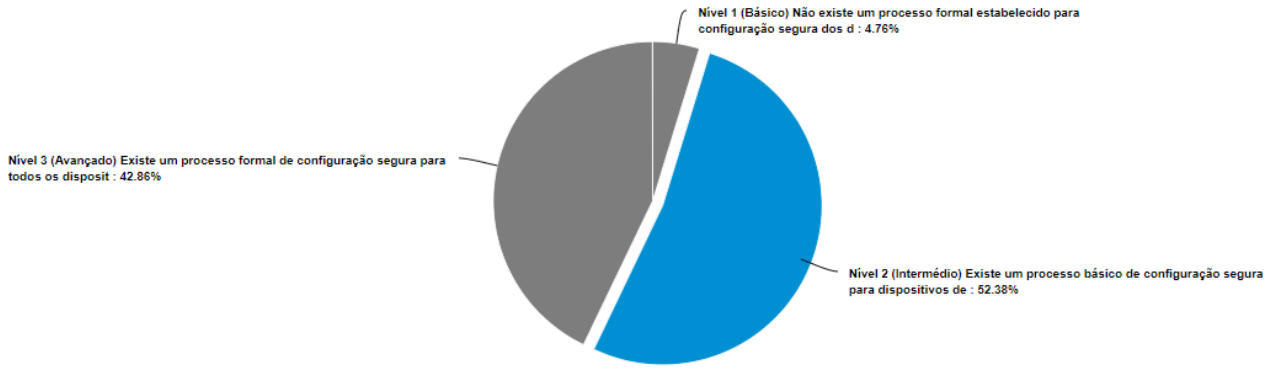

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Os dispositivos dos utilizadores finais não se encontram cifrados. | 3 | 14.29% | | | | | |
| Nível 2 (Intermédio) Alguns dispositivos dos utilizadores finais que contêm dados sensíveis são cifrados, mas a implementação é inconsistente. | 8 | 38.1% | | | | | |
| Nível 3 (Avançado) As políticas de segurança incluem requisitos específicos para a cifragem de dispositivos do utilizador final e são aplicadas de forma rigorosa em toda a organização. São utilizadas soluções de cifragem como BitLocker, FileVault, dm-crypt, entre outras, garantindo uma proteção eficaz dos dados em repouso, preferencialmente com uma gestão centralizadas das chaves. | 10 | 47.62% | | | | | |
| Total | 21 | 100 % | | | | | |

Na sua organização existe um processo de gestão de configurações que permite a definição de uma base segura para os dispositivos dos utilizadores finais?



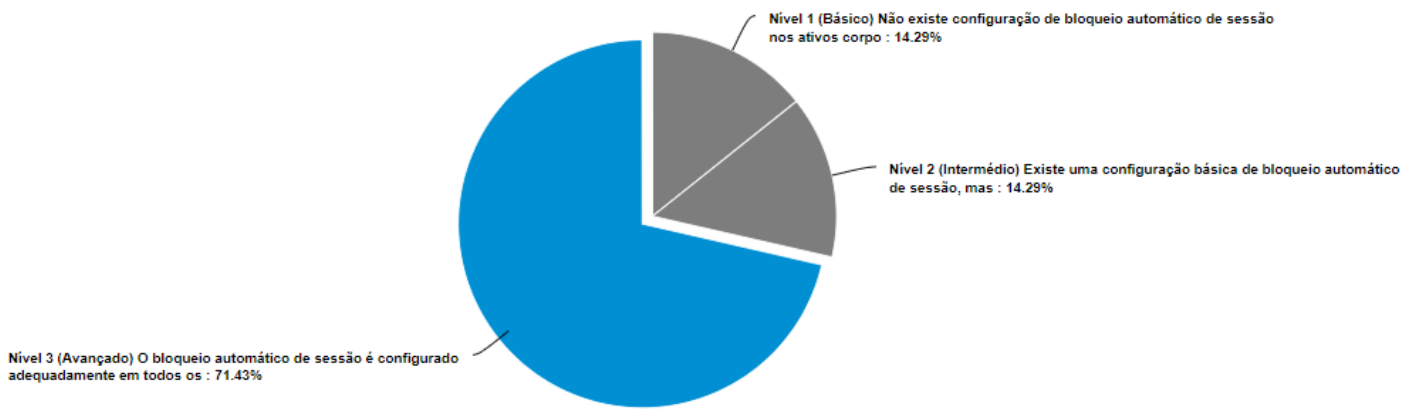

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe um processo formal estabelecido para configuração segura de ativos corporativos. | 1 | 4.76% | | | | | |
| Nível 2 (Intermédio) Existe um processo básico de configuração segura, mas é inconsistente ou incompleto. As configurações padrão são ajustadas para melhorar a segurança, mas não são abordadas todas as melhores práticas recomendadas. | 14 | 66.67% | | | | | |
| Nível 3 (Avançado) Existe um processo formal de configuração segura para todos os ativos corporativos e software. As configurações são revistas regularmente para garantir que estão alinhadas com as melhores práticas de segurança e conformidade. A documentação do processo é atualizada anualmente ou quando ocorrem mudanças significativas na empresa, garantindo que a segurança seja mantida em níveis adequados. | 6 | 28.57% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de configuração segura para os ativos de rede?



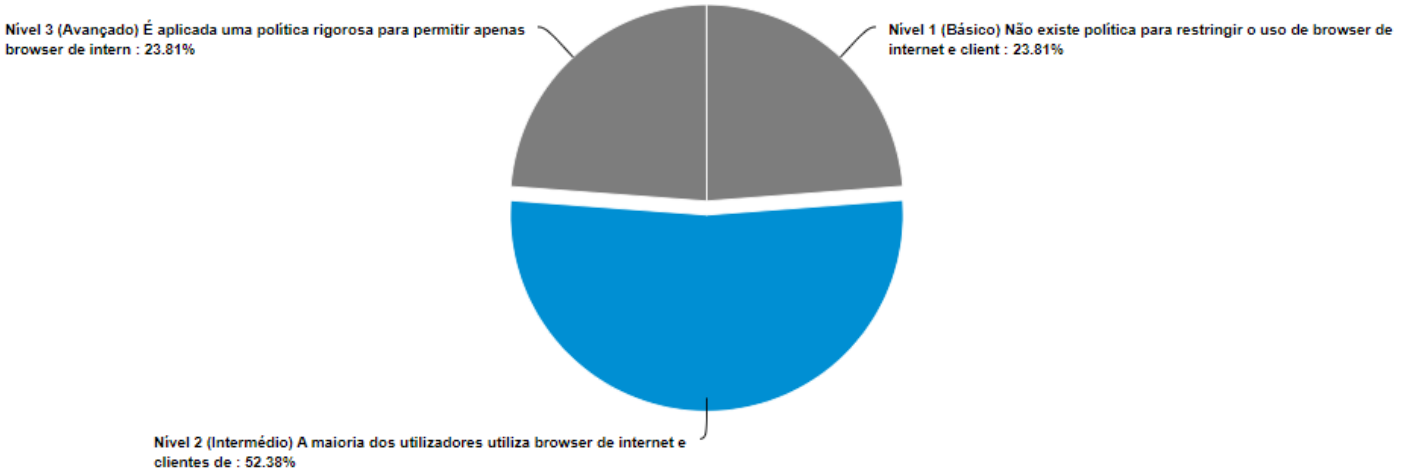

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe um processo formal estabelecido para configuração segura dos dispositivos de rede. | 1 | 4.76% | | | | | |
| Nível 2 (Intermédio) Existe um processo básico de configuração segura para dispositivos de rede, mas é inconsistente ou incompleto. As configurações padrão são ajustadas em alguns dispositivos, mas não são abordadas todas as melhores práticas de segurança. | 11 | 52.38% | | | | | |
| Nível 3 (Avançado) Existe um processo formal de configuração segura para todos os dispositivos de rede. As configurações dos dispositivos de rede são revistas regularmente para garantir que estão alinhadas com as melhores práticas de segurança e conformidade. A documentação do processo é atualizada anualmente ou quando ocorrem mudanças significativas na empresa, garantindo que a segurança da rede seja mantida em níveis adequados. | 9 | 42.86% | | | | | |
| Total | 21 | 100 % | | | | | |

Na sua organização existe um processo de bloqueio automático da sessão?



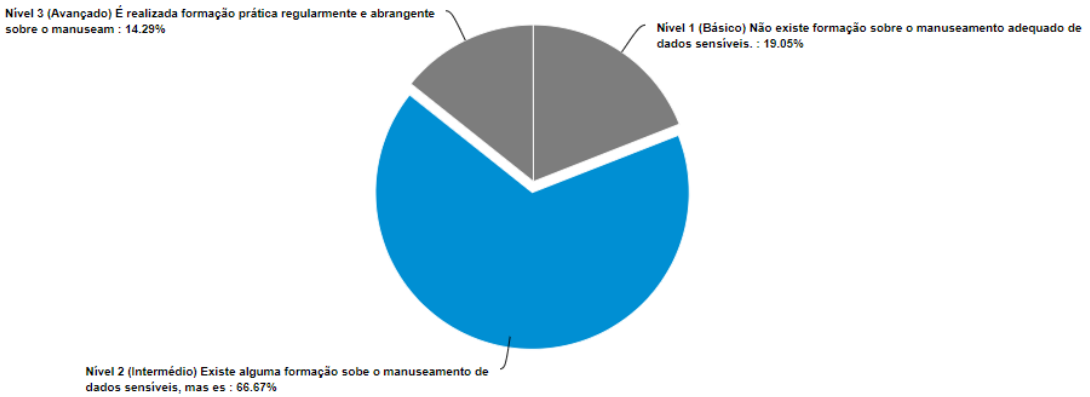

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe configuração de bloqueio automático de sessão nos ativos corporativos após períodos de inatividade. | 3 | 14.29% | | | | | |
| Nível 2 (Intermédio) Existe uma configuração básica de bloqueio automático de sessão, mas os períodos de inatividade são excessivamente longos. | 3 | 14.29% | | | | | |
| Nível 3 (Avançado) O bloqueio automático de sessão é configurado adequadamente em todos os ativos corporativos. A configuração é regularmente revista e atualizada para garantir que permaneça alinhada com as melhores práticas de segurança. | 15 | 71.43% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização podem apenas ser utilizados browser de internet e clientes de email suportados?



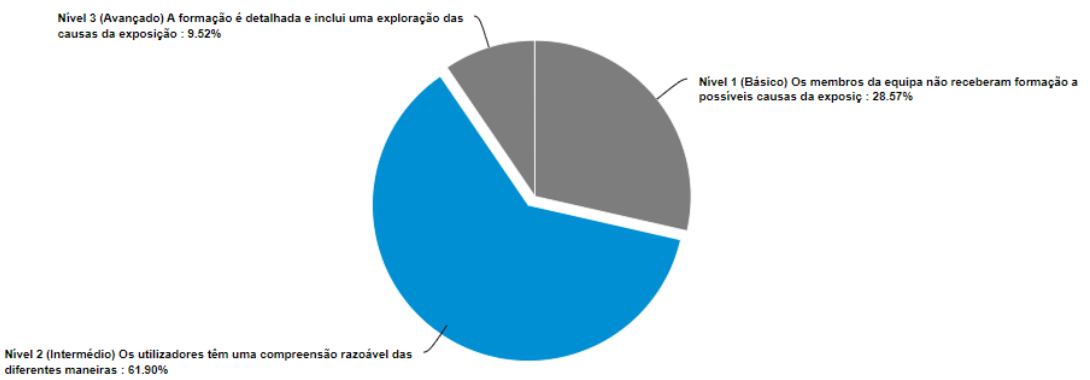

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe política para restringir o uso de browser de internet e clientes de e-mail. | 5 | 23.81% | | | | | |
| Nível 2 (Intermédio) A maioria dos utilizadores utiliza browser de internet e clientes de e-mail suportados, mas existem exceções. | 11 | 52.38% | | | | | |
| Nível 3 (Avançado) É aplicada uma política rigorosa para permitir apenas browser de internet e clientes de e-mail suportados, usando apenas as versões mais recentes fornecidas pelo fornecedor. | 5 | 23.81% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de formação dos utilizadores sobre as melhores práticas de tratamento de dados?



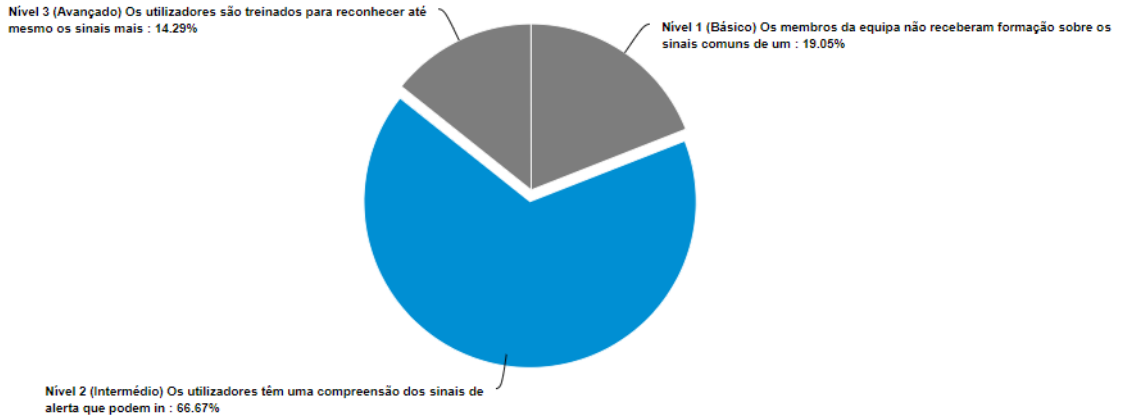

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe formação sobre o manuseamento adequado de dados sensíveis. | 4 | 19.05% | | | | | |
| Nível 2 (Intermédio) Existe alguma formação sobe o manuseamento de dados sensíveis, mas está incompleto. As práticas recomendadas de mesa e ecrã limpos são comunicadas, mas não são seguidas por todos os utilizadores. | 14 | 66.67% | | | | | |
| Nível 3 (Avançado) É realizada formação prática regularmente e abrangente sobre o manuseamento adequado de dados sensíveis para todos os membros da equipa. Os utilizadores têm um entendimento claro dos procedimentos para identificar, armazenar, transferir, arquivar e destruir dados sensíveis de maneira segura. As práticas recomendadas de mesa e ecrã limpos são comunicadas e amplamente seguidas por todos os utilizadores. | 3 | 14.29% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de formação dos utilizadores sobre exposição não intencional de dados?



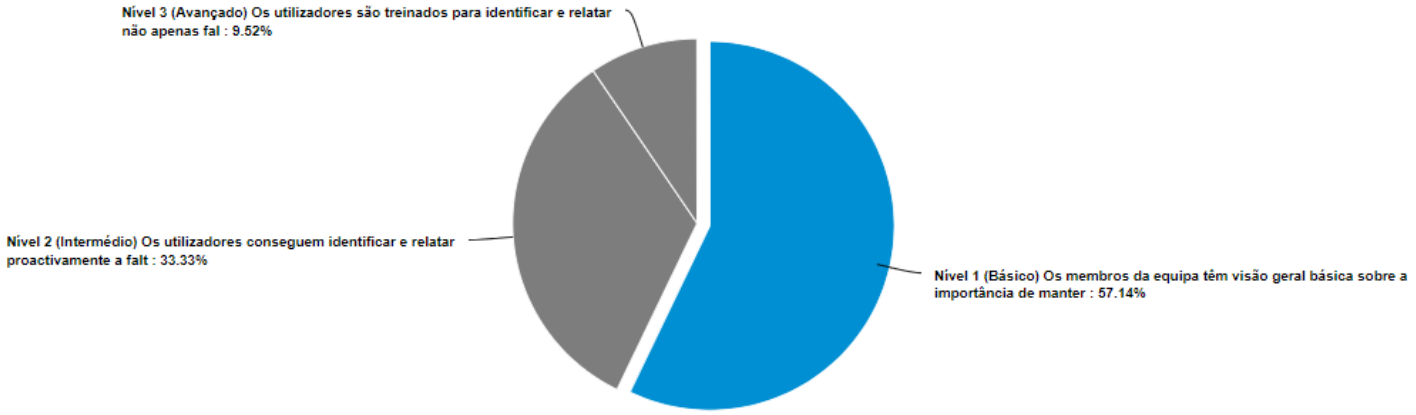

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Os membros da equipa não receberam formação a possíveis causas da exposição não intencional de dados. | 6 | 28.57% | | | | | |
| Nível 2 (Intermédio) Os utilizadores têm uma compreensão razoável das diferentes maneiras pelas quais os dados sensíveis podem ser expostos inadvertidamente, como a perda de dispositivos e divulgação não autorizada. | 13 | 61.9% | | | | | |
| Nível 3 (Avançado) A formação é detalhada e inclui uma exploração das causas da exposição não intencional de dados. Os utilizadores têm um entendimento completo das diferentes maneiras pelas quais os dados sensíveis podem ser expostos inadvertidamente, desde os cenários mais comuns até os mais complexos. São fornecidos casos de estuado e simulações de cenários para capacitar os utilizadores a reconhecer, prevenir e responder efetivamente a incidentes de exposição não intencional de dados. | 2 | 9.52% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de formação dos utilizadores sobre reconhecimento e comunicação de incidentes de segurança?



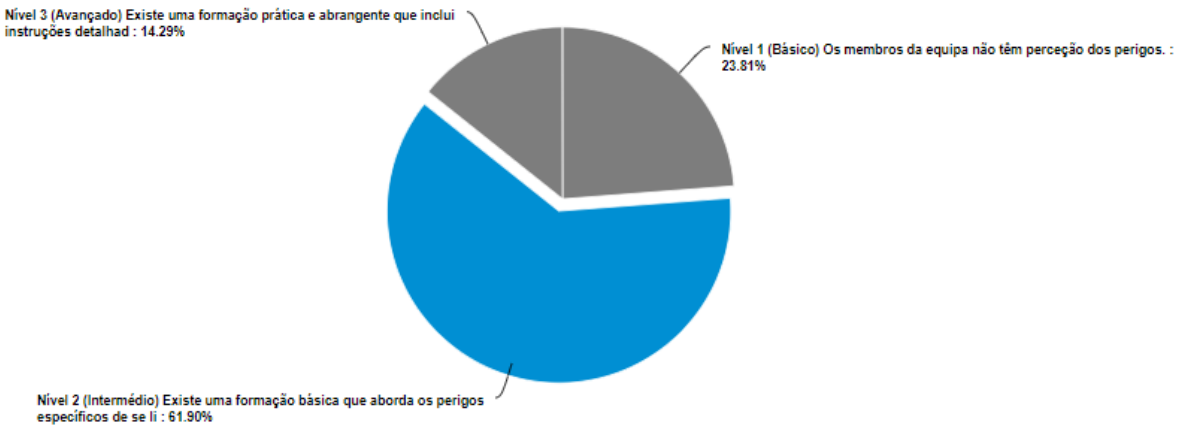

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Os membros da equipa não receberam formação sobre os sinais comuns de um potencial incidente de segurança. | 4 | 19.05% | | | | | |
| Nível 2 (Intermédio) Os utilizadores têm uma compreensão dos sinais de alerta que podem indicar a presença de um incidente de segurança. A formação aborda aspetos básicos sobre indicadores de incidentes em potencial e como reconhecê-los. | 14 | 66.67% | | | | | |
| Nível 3 (Avançado) Os utilizadores são treinados para reconhecer até mesmo os sinais mais subtis de atividade maliciosa ou anómala nos sistemas e redes da empresa. A formação pode incluir simulações de incidentes para fornecer aos utilizadores uma experiência prática no reconhecimento e resposta a incidentes. | 3 | 14.29% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de formação dos utilizadores sobre como identificar e comunicar se os seus ativos têm falta de atualizações de segurança?



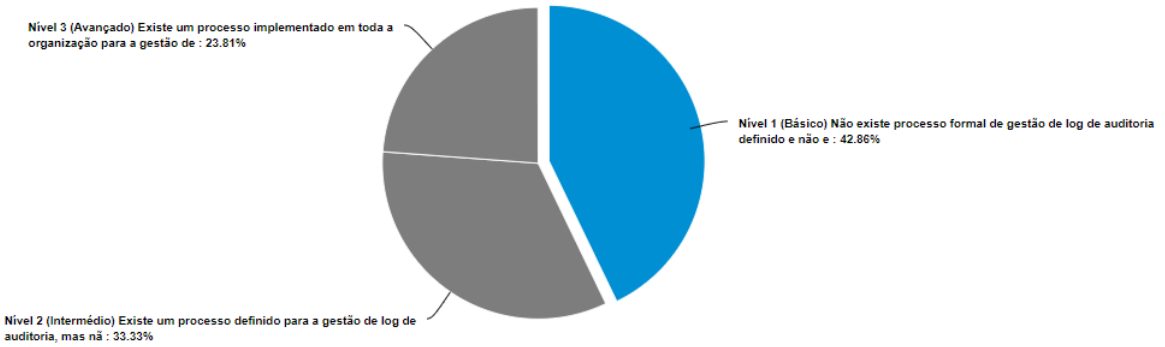

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Os membros da equipa têm visão geral básica sobre a importância de manter o software atualizado. | 12 | 57.14% | | | | | |
| Nível 2 (Intermédio) Os utilizadores conseguem identificar e relatar proactivamente a falta de atualizações de segurança, comunicando com a equipa de TI para a sua aplicação. | 7 | 33.33% | | | | | |
| Nível 3 (Avançado) Os utilizadores são treinados para identificar e relatar não apenas falhas óbvias, mas também possíveis vulnerabilidades ou áreas de melhoria nos processos e ferramentas. | 2 | 9.52% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de formação dos utilizadores sobre os perigos de se ligarem e transmitirem dados corporativos em redes inseguras?



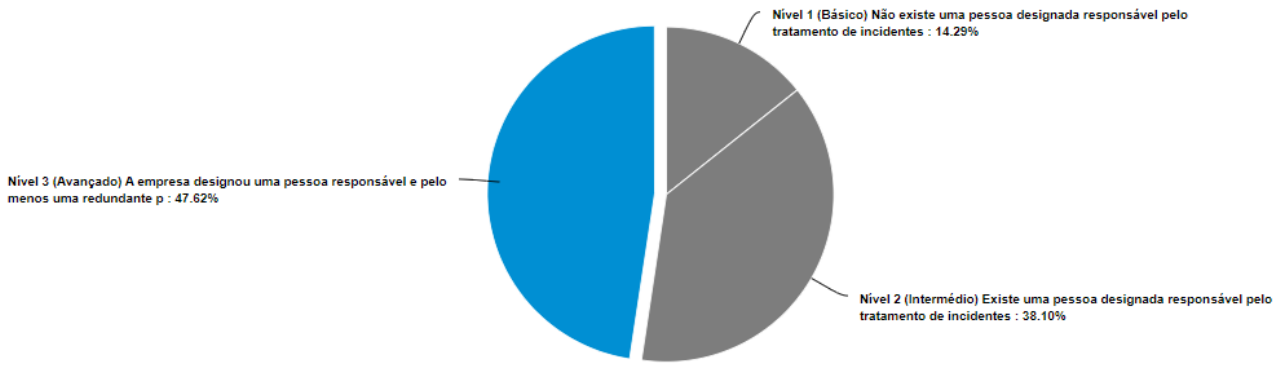

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Os membros da equipa não têm perceção dos perigos. | 5 | 23.81% | | | | | |
| Nível 2 (Intermédio) Existe uma formação básica que aborda os perigos específicos de se ligarem a redes Wi-Fi não seguras e os métodos comuns pelos quais os invasores podem comprometer os dados transmitidos nessas redes. | 13 | 61.9% | | | | | |
| Nível 3 (Avançado) Existe uma formação prática e abrangente que inclui instruções detalhadas sobre como utilizar e configurar redes Wi-Fi seguras, usando métodos seguros de cifragem e autenticação. Estes aprendem a utilizar Redes Virtuais Privadas (VPNs), para proteger os dados transmitidos quando trabalham remotamente. | 3 | 14.29% | | | | | |
| Total | 21 | 100 % | | | | | |

Na sua organização existe um processo de gestão de logs?



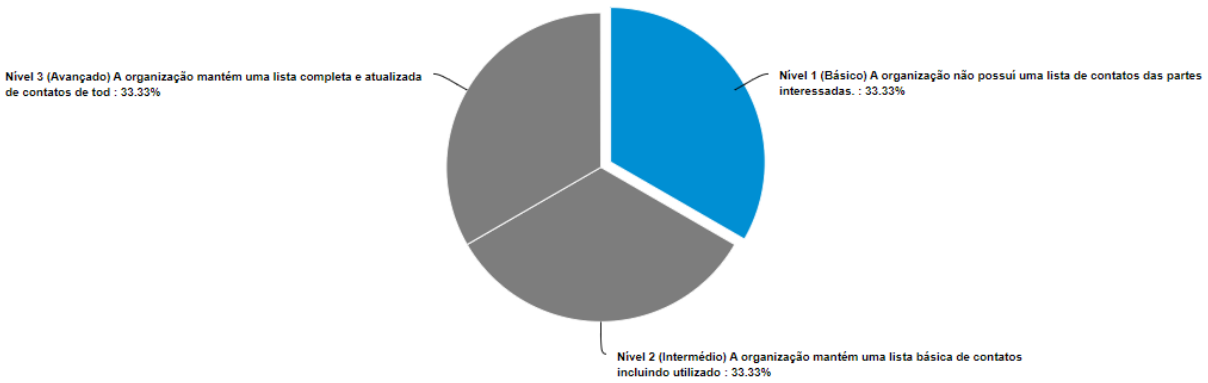

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe processo formal de gestão de log de auditoria definido e não existe informação dos requisitos de log da empresa. | 9 | 42.86% | | | | | |
| Nível 2 (Intermédio) Existe um processo definido para a gestão de log de auditoria, mas não é totalmente abrangente ou aplicado consistentemente em toda a organização. A recolha, revisão e retenção de logs são tratadas para alguns dos ativos corporativos. | 7 | 33.33% | | | | | |
| Nível 3 (Avançado) Existe um processo implementado em toda a organização para a gestão de log de auditoria. A recolha, revisão e retenção de logs são tratadas de forma abrangente e consistente para todos os ativos corporativos. Os requisitos de log da empresa são claramente definidos, documentados e revistos regularmente para garantir a conformidade contínua com as mudanças na empresa e nas regulamentações. | 5 | 23.81% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe a designação do responsável (interno ou externo) pelo tratamento e Gestão de Incidentes de Segurança?



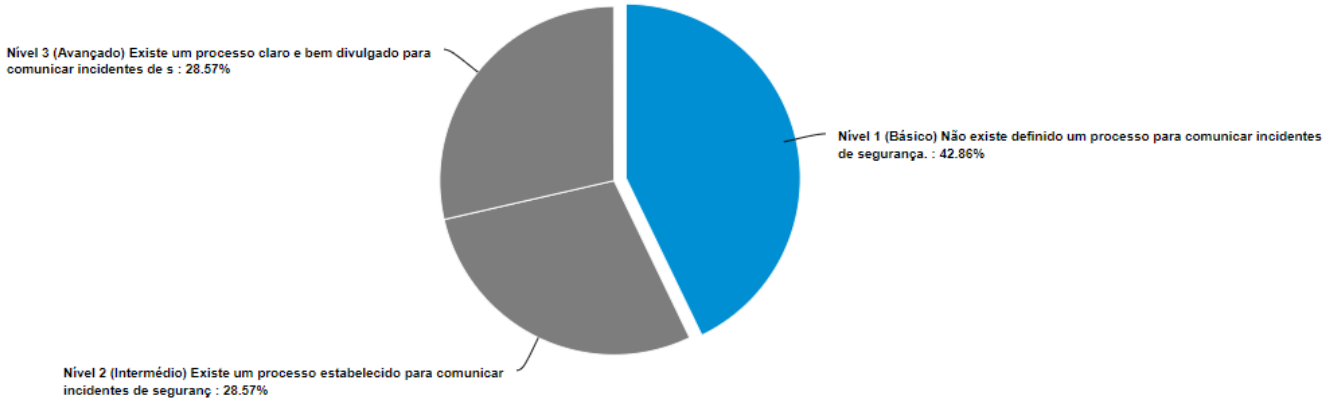

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe uma pessoa designada responsável pelo tratamento de incidentes. | 3 | 14.29% | | | | | |
| Nível 2 (Intermédio) Existe uma pessoa designada responsável pelo tratamento de incidentes. A análise do processo de tratamento de incidentes é realizada, mas não é feita regularmente ou de forma sistemática. | 8 | 38.1% | | | | | |
| Nível 3 (Avançado) A empresa designou uma pessoa responsável e pelo menos uma redundante para gerir o processo de tratamento de incidentes. A análise do processo de tratamento de incidentes é realizada regularmente e sempre que ocorrem mudanças significativas na empresa. | 10 | 47.62% | | | | | |
| Total | 21 | 100 % | | | | | |

Na sua organização existe uma lista de contatos para comunicação de Incidentes de Segurança?



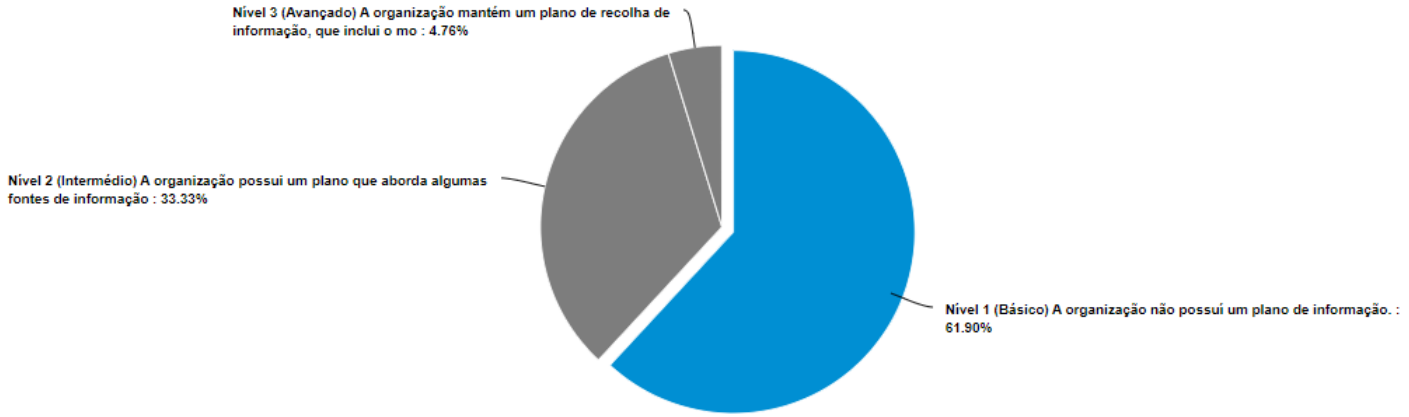

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) A organização não possuí uma lista de contatos das partes interessadas. | 7 | 33.33% | | | | | |
| Nível 2 (Intermédio) A organização mantém uma lista básica de contatos incluindo utilizadores internos, fornecedores externos, agências governamentais relevantes. | 7 | 33.33% | | | | | |
| Nível 3 (Avançado) A organização mantém uma lista completa e atualizada de contatos de todas as partes interessadas relevantes, incluindo utilizadores internos, fornecedores externos, agências governamentais e seguros de cibersegurança. Além de revisões anuais, há um processo contínuo de verificação e atualização das informações de contato sempre que ocorrerem mudanças relevantes nas partes interessadas. A organização realiza exercícios regulares de simulação de incidentes para testar a eficácia das informações de contato e os procedimentos de resposta. | 7 | 33.33% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um plano de comunicação de incidentes de segurança?



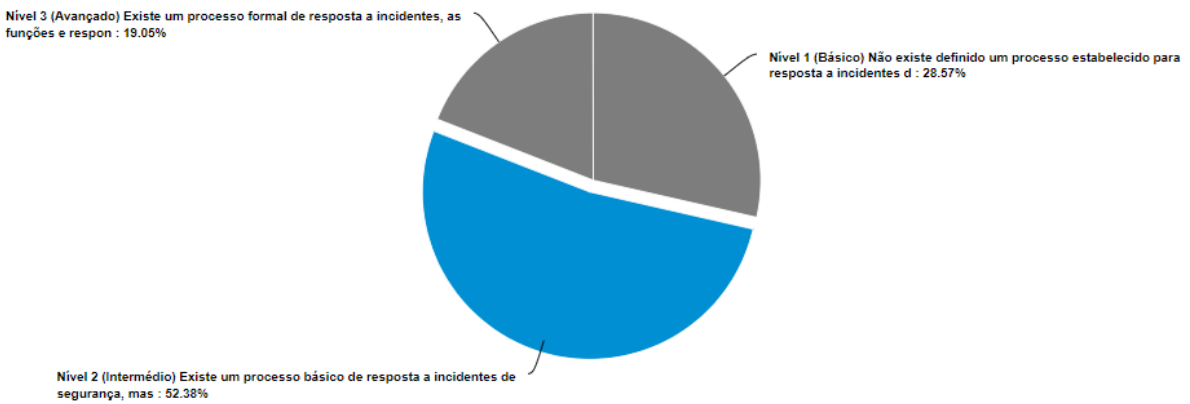

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe definido um processo para comunicar incidentes de segurança. | 9 | 42.86% | | | | | |
| Nível 2 (Intermédio) Existe um processo estabelecido para comunicar incidentes de segurança, mas pode não ser amplamente divulgado ou compreendido. | 6 | 28.57% | | | | | |
| Nível 3 (Avançado) Existe um processo claro e bem divulgado para comunicar incidentes de segurança. O processo inclui um cronograma definido para relatórios, procedimentos claros sobre quem deve comunicar, mecanismos para comunicar e informações mínimas necessárias para os relatórios. | 6 | 28.57% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um plano de recolha de informação sobre eventos de segurança de fontes fidedignas?



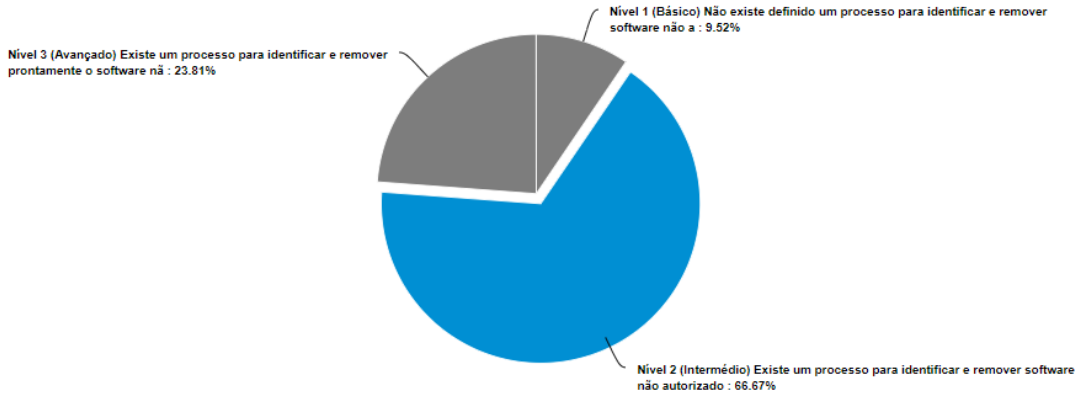

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) A organização não possui um plano de informação. | 13 | 61.9% | | | | | |
| Nível 2 (Intermédio) A organização possui um plano que aborda algumas fontes de informação, incluindo feeds RSS, alertas de segurança por e-mail e grupos de discussão da indústria. | 7 | 33.33% | | | | | |
| Nível 3 (Avançado) A organização mantém um plano de recolha de informação, que inclui o monitorização contínuo de fontes de externas, como feeds de inteligência de ameaças, grupos de segurança online e redes sociais. Existe uma abordagem proativa para disseminar informações sobre ameaças à segurança da informação. | 1 | 4.76% | | | | | |
| Total | 21 | 100 % | | | | | |

Na sua organização existe um processo de resposta a incidentes de segurança?



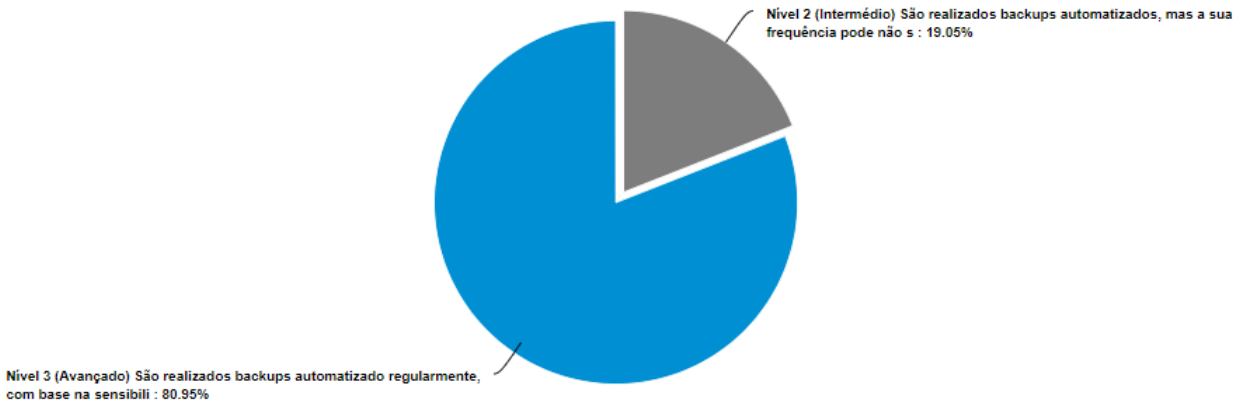

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe definido um processo estabelecido para resposta a incidentes de segurança. | 6 | 28.57% | | | | | |
| Nível 2 (Intermédio) Existe um processo básico de resposta a incidentes de segurança, mas pode ser inconsistente ou incompleto. As funções e responsabilidades estão vagamente definidas, e pode haver falta de requisitos de conformidade. | 11 | 52.38% | | | | | |
| Nível 3 (Avançado) Existe um processo formal de resposta a incidentes, as funções e responsabilidades durante um incidente são claramente definidas, juntamente com requisitos de conformidade e um plano de comunicação abrangente. O processo é revisto anualmente ou quando ocorrem mudanças significativas na empresa, garantindo que esteja sempre atualizado e eficaz na mitigação de incidentes de segurança. | 4 | 19.05% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de remoção de software não autorizado?



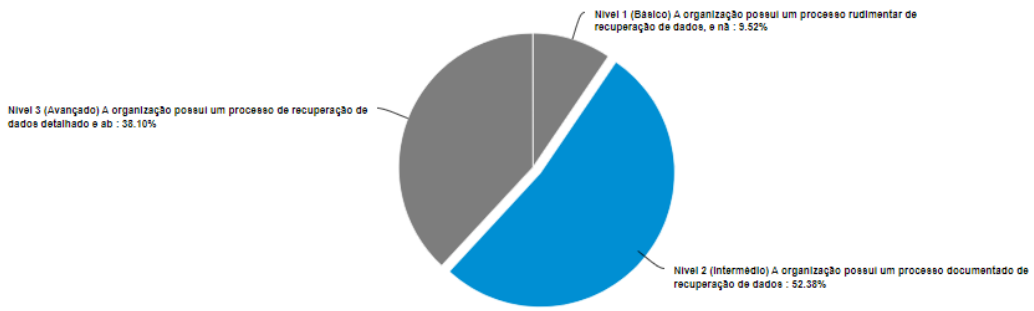

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe definido um processo para identificar e remover software não autorizado. | 2 | 9.52% | | | | | |
| Nível 2 (Intermédio) Existe um processo para identificar e remover software não autorizado, mas pode não ser implementado de forma consistente. O software não autorizado é identificado ocasionalmente, mas sua remoção nem sempre é realizada prontamente. | 14 | 66.67% | | | | | |
| Nível 3 (Avançado) Existe um processo para identificar e remover prontamente o software não autorizado, o processo é executado regularmente, com análises mensais ou até mesmo com maior frequência para garantir a conformidade contínua. O software não autorizado é removido prontamente dos ativos corporativos, a menos que uma exceção documentada seja concedida, incluindo uma justificativa e planos de mitigação para reduzir o risco associado. | 5 | 23.81% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de backups automatizados?



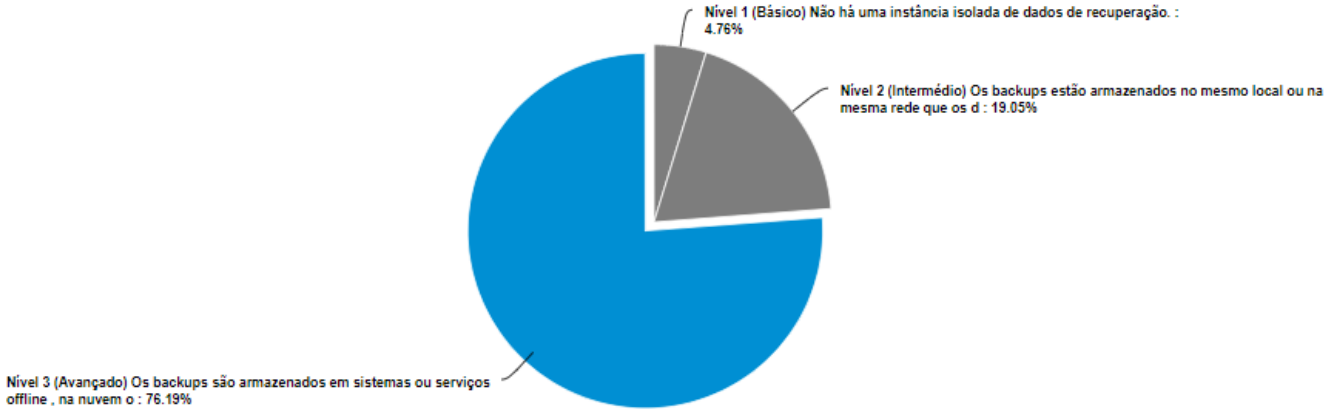

| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não existe uma solução de backup automatizada e não são realizados regularmente. | 0 | 0% | | | | | |
| Nível 2 (Intermédio) São realizados backups automatizados, mas a sua frequência pode não ser suficiente para garantir a proteção adequada dos dados. | 4 | 19.05% | | | | | |
| Nível 3 (Avançado) São realizados backups automatizado regularmente, com base na sensibilidade dos dados, a frequência de backup é ajustada conforme necessário para garantir a proteção adequada dos dados mais sensíveis. | 17 | 80.95% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe um processo de recuperação de dados?




| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) A organização possui um processo rudimentar de recuperação de dados, e não está documentado. | 2 | 9.52% | | | | | |
| Nível 2 (Intermédio) A organização possui um processo documentado de recuperação de dados que aborda o âmbito das atividades de recuperação, incluindo procedimentos para restauração de dados de backup. | 11 | 52.38% | | | | | |
| Nível 3 (Avançado) A organização possui um processo de recuperação de dados detalhado e abrangente, devidamente documentado e acessível a todos os membros relevantes da equipa. O âmbito das atividades de recuperação é claramente definido, com procedimentos específicos para diferentes tipos de incidentes e sistemas afetados. A priorização da recuperação é cuidadosamente planeada, com uma compreensão clara dos impactos nos negócios e requisitos de tempo de recuperação para diferentes tipos de dados. A segurança dos dados de backup é uma prioridade, com medidas robustas de proteção, como cifragem forte, controlo de acesso e armazenamento offsite seguro. A documentação é revista e atualizada regularmente, para garantir que permaneça relevante e eficaz diante de mudanças no ambiente de negócios ou nos requisitos regulamentares. | 8 | 38.1% | | | | | |
| **Total** | **21** | **100 %** | | | | | |

Na sua organização existe uma instância isolada com os dados de backup?




| Resposta | Contagem | Percentagem | 20% | 40% | 60% | 80% | 100% |
|---|---|---|---|---|---|---|---|
| Nível 1 (Básico) Não há uma instância isolada de dados de recuperação. | 1 | 4.76% | | | | | |
| Nível 2 (Intermédio) Os backups estão armazenados no mesmo local ou na mesma rede que os dados originais, existe uma tentativa de manter uma instância isolada de dados de recuperação, mas pode não ser totalmente eficaz. | 4 | 19.05% | | | | | |
| Nível 3 (Avançado) Os backups são armazenados em sistemas ou serviços offline , na nuvem ou offsite, garantindo a sua segurança e disponibilidade mesmo em caso de eventos adversos no local principal. | 16 | 76.19% | | | | | |
| Total | 21 | 100 % | | | | | |

# C Anexo C – Guia de Implementação de Melhorias

A cibersegurança é uma preocupação cada vez mais crítica para organizações de todos os tamanhos e setores. À medida que a dependência da tecnologia continua a crescer, também aumenta a sofisticação das ameaças.

Este guia foi elaborado com base nos recursos disponibilizados pelo *CIS Controls*, nomeadamente o *Implementation Guide for Small and Medium Sized Enterprises CIS Controls* IG1 [39], *Acceptable Use Policy Template for the CIS Controls* [76], sendo complementado com a perspetiva e experiência do autor. Pretende-se assim, fornecer orientações sobre os controlos necessário para responder aos SMD em Cibersegurança no nível Bronze e Prata. Neste, são apresentados exemplos práticos e sugestões de ferramentas que podem ser utilizadas para alcançar os objetivos de segurança propostos.

## C.1 Implementação da PUA

A Política de Uso Aceitável (PUA) é um componente crítico de qualquer programa de segurança da informação. Esta Secção descreve o processo de implementação de uma PUA, baseado no modelo *Acceptable Use Policy Template for the CIS Controls* [76].

A PUA tem como objetivo informar os utilizadores como eles podem utilizar os recursos de tecnologia da informação (TI) fornecidos pela empresa para realizar o seu trabalho. Essencialmente, é uma lista de "Fazer" e "Não Fazer", ou seja, "Uso Aceitável" e "Uso Proibido". O conteúdo de uma PUA pode variar, mas geralmente inclui as melhores práticas para os seguintes tópicos:

**Propósito**

A PUA define as diretrizes e expectativas para o uso adequado dos recursos tecnológicos fornecidos pela empresa. O objetivo é minimizar riscos, garantir a conformidade com regulamentações e promover boas práticas de segurança entre os colaboradores.

Esta Política de Uso Aceitável atua como um acordo entre a empresa e o utilizador que recebe ativos de Tecnologia da Informação (TI). Os ativos são definidos como qualquer coisa que tenha valor para uma organização, incluindo, entre outros, outra organização, pessoa, dispositivo de computação, sistema de TI, rede de TI, *software*, plataforma de computação virtual e *hardware* relacionado (por exemplo: fechaduras, teclados).

**Âmbito**

Esta política aplica-se a todos os utilizadores que utilizam os recursos tecnológicos da empresa, incluindo funcionários, terceiras partes, consultores e qualquer outra parte que tenha acesso aos ativos da organização.

**Exceções**

É provável que ocorram exceções a esta política, estas podem ocorrer por diversos motivos, onde os utilizadores podem necessitar de usar os ativos de TI da empresa de maneira inconsistente com a política. Todas as solicitações de exceção deverão ser feitas por escrito e deverão conter:

- O motivo da solicitação;
- Risco para a empresa de não seguir a política escrita;
- Mitigações específicas que não serão implementadas;
- Dificuldades técnicas e outras;
- Data da revisão.

Todas as exceções devem ser aprovadas pela pessoa responsável autorizado a aprovar a exceção.

**Ativos da Empresa**

Os ativos empresariais incluem todos os dispositivos e recursos tecnológicos que a empresa possuí e gere, como:

- Dispositivos de utilizadores: *desktops, laptops, tablets e smartphones*;
- Dispositivos de rede: pontos de acesso, *switches, firewalls, routers*;
- Dispositivos IoT: impressoras, sensores, sistemas de controlo industrial;
- Servidores: *web*, *e-mail*, aplicações e ficheiros.

**Responsabilidades do utilizador:**

- O utilizador deve usar apenas tecnologia e serviços aprovados;
- Todos os ativos da empresa são emprestados ao utilizador para que possam ser desempenhadas funções essenciais do trabalho;
- Após a separação da empresa ou rescisão do contrato, todos os ativos de TI fornecidos e os dados associados deverão ser devolvidos pelo utilizador;
- O utilizador deve proteger o ambiente físico em torno de sua estação de trabalho e bloquear seus computadores quando se afastarem;
- O utilizador deve garantir que as informações de identificação pessoal (PII), confidenciais e quaisquer dados confidenciais que possam ser cobertos por

regulamentação governamental ou outra regulamentação, não estejam prontamente disponíveis ou acessíveis em suas mesas ou em seu espaço de trabalho;

- O utilizador deve tomar os devidos cuidados para proteger as informações, os sistemas e os ativos relacionados sob sua custódia ou cuidado contra perdas, danos ou prejuízos;
    - Equipamentos perdidos ou danificados devem ser comunicados ao responsável de TI assim que possível;
- O utilizador deve armazenar as suas credenciais de forma segura;
    - O gestor de *passwords* aprovado deve ser utilizado para armazenar as credenciais digitalmente;
- As contas atribuídas ao utilizador devem aceder apenas ativos, sistemas operativos, aplicações, ficheiros e dados aos quais tenham acesso concedido. A capacidade de ler, executar, modificar, excluir ou copiar dados inadvertidamente não implica permissão para fazê-lo;
- Somente os utilizadores autorizados podem criar, publicar, expressando opiniões e declarações em nome da empresa em *websites* de redes sociais, *blogs* ou outros *websites* da *internet*;
- O utilizador deve manter confidencial o conhecimento sobre as informações e os sistemas de informação obtidos durante o emprego, e a confidencialidade deve ser mantida após o término do emprego.

**Uso Proibido**

Lista ações que o utilizador não deve realizar com os ativos empresariais.

- Somente os dispositivos aprovados e autorizados podem ser ligados a redes pertencentes ou geridas pela empresa. Isso inclui dispositivos portáteis de utilizador final, dispositivos removíveis (por exemplo: *pendrives*) e dispositivos de propriedade pessoal;
- O utilizador não deve partilhar suas credenciais com terceiros nem permitir o uso de sua conta por terceiros;
    - O utilizador é responsável por todas as atividades provenientes das suas credenciais;
- O utilizador não deve ludibriar os mecanismos de autenticação de utilizador ou a segurança de qualquer conta de utilizador ou ativo do sistema de informação;
- O utilizador não deve instalar *software*, *hardware* ou modificar definições de configuração do sistema em qualquer ativo corporativo, a menos que seja explicitamente permitido pela função e responsabilidade do utilizador;
- O utilizador não deve executar nenhuma atividade com a intenção de interromper o funcionamento de ativos ou redes empresariais;

    - O utilizador não devem realizar qualquer forma de monitorização de rede, pesquisa de portas ou pesquisas de segurança, a menos que esta atividade faça parte do trabalho normal do indivíduo e seja formalmente autorizada;
- O utilizador não deve aproveitar os ativos da empresa para obter ganhos económicos pessoais;
- O utilizador não devem utilizar a função "Lembrar-me" ou "Lembrar minha *password*" dentro de *browsers* de *internet*.

**Expectativas de Privacidade**

Esclarece o nível de privacidade que o utilizador pode esperar ao utilizar os ativos empresariais.

- Ao utilizar recursos empresariais, o utilizador não deve ter nenhuma expectativa de privacidade. O acesso e a utilização da *internet*, incluindo a comunicação por *e-mail* e mensagens instantâneas e o seu conteúdo, não são confidenciais, exceto nos casos reconhecidos por lei;
- A empresa reserva-se o direito de monitorizar, aceder e divulgar todas as informações geradas e ações realizadas utilizando os ativos de TI da empresa. Ficheiros, mensagens (incluindo anexos) e registos podem ser retidos e usados como prova em litígios, auditorias e investigações.

**Uso Pessoal**

Define as restrições para o uso pessoal dos ativos empresariais.

- É permitido ao utilizador o uso pessoal limitado dos ativos da empresa, como visitar *websites* e verificar contas de *e-mail* pessoais;
    - O utilizador pode aceder ao gestor de *passwords* pessoal baseados em *cloud* a partir dos ativos corporativos. A instalação local de um gestor de *passwords* deve ser aprovada pela TI;
    - O utilizador não deve armazenar credenciais corporativas em gestores de *passwords* pessoais;
    - O utilizador não deve realizar a sincronização do *browser* de *internet* ou perfis de navegação que sincronize o histórico de um dispositivo pessoal para um ativo empresarial (ou vice-versa).
- O utilizador não deve usar contas de propriedade pessoal (por exemplo, ID Apple, Conta do Google, Conta da Microsoft) em dispositivos empresariais, a menos que permitido pela empresa;
- O utilizador não deve usar chaves de licença corporativa em dispositivos pessoais, a menos que autorizados pela empresa;

- Os dados empresariais não devem ser armazenados em plataformas de fornecedores de *cloud* pessoais (por exemplo, Google Drive, Microsoft OneDrive, Dropbox).

**Identificação de Violações**

Métodos para relatar violações da PUA e outros incidentes de segurança.

- O utilizador que tiver conhecimento de qualquer evento que ameace a disponibilidade, integridade ou confidencialidade dos dados corporativos, ou que viole qualquer padrão, política, procedimento ou qualquer requisito associado, ou que seja contrário à lei, devem entrar em contato imediatamente com a TI ou seu responsável imediato.

**Trabalho Remoto**

Políticas para utilizadores que trabalham remotamente.

- Todo o trabalho empresarial deve ser executado em ativos aprovados pela empresa;
- Todos os dados empresariais devem ser armazenados em ativos empresariais aprovados;
- O utilizador não deve ligar ativos empresariais a redes WiFi abertas e não cifradas;
- O utilizador deve estar atento ao que está ao seu redor ao trabalhar remotamente para garantir que outras pessoas não estejam a visualizar informações confidenciais.

**Trazer Seu Próprio Dispositivo (BYOD)**

Declarações sobre o uso de dispositivos pessoais para atividades de trabalho.

- Os dispositivos pessoais não devem ser ligados à rede corporativa sem autorização formal;
- Os dados empresariais não devem ser armazenados em dispositivos pessoais sem autorização formal;
- O utilizador que utilizar os seus dispositivos pessoais para armazenar dados corporativos, podem ter seus dispositivos completamente apagados. Os motivos para a limpeza do dispositivo podem incluir:
    - Dispositivo perdido/roubado;
    - Rescisão do contrato de trabalho do utilizador;
    - Conta ou dispositivo comprometido/pirateado.

## C.2 Implementação do CIS Controls para PMEs IG1

Após a implementação da PUA, devem ser executadas as ações para proteger a organização, o *Implementation Guide for Small and Medium Sized Enterprises CIS Controls* IG1 [39], tem como objetivo acelerar a implementação do IG1 numa empresa e proporciona um conjunto de ações prioritárias para proteger as empresas contra os ataques mais comuns, fazendo uma abordagem da quase totalidade das *safeguards* do Grupo de Implementação 1.

### C.2.1 Inventário de Ativos

A primeira fase da implementação envolve a criação de inventários detalhados dos ativos da empresa, estes inventários ajudam a compreender e gerir melhor os dispositivos, *softwares*, dados e contas usados na organização, facilitando a proteção contra acessos não autorizados e ameaças externas.

- **Inventário de Ativos Corporativos**
  - Ações:
    - Realizar uma auditoria física e digital para listar todos os dispositivos ligados à rede da empresa;
    - Verificar (através do serviço de DHCP) os endereços IP e nome dos equipamentos ligados á rede (cabo e sem fios);
    - Podem ser utilizadas ferramentas como o NMAP[20], para fazer uma pesquisa na rede;
    - Para redes maiores, podem ser utilizadas ferramentas de análise de rede para identificar todos os dispositivos como Spiceworks[21] ou Lansweeper[22], onde permitem ainda identificar softwares instalados nos dispositivos.
  - Consultar o *CIS Controls Enterprise Asset Management Policy Template* [23];
  - Para o registo da informação pode ser utilizada o exemplo disponibilizado na Tabela 17.

[20] https://nmap.org/
[21] https://www.spiceworks.com/
[22] https://www.lansweeper.com/
[23] https://www.cisecurity.org/insights/blog/cis-controls-enterprise-asset-management-policy-template

**Tabela 17 – Inventário de Ativos Corporativos**

| Inventário de Ativos Corporativos | | | | | | |
|---|---|---|---|---|---|---|
| Listar todos os computadores da empresa. Incluir o tipo de ativo: desktops, laptops, telefones, routers, switchs, firewall, dispositivos IoT e servidores. | | | | | | Revisão: Trimestral |
| **Nome** | **Tipo** | **Modelo** | **Número de Série** | **Localização Física** | **Descrição** | **Notas** |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Nome:**
**Data de Revisão:**

- **Inventário de Softwares**
  - Ações:
    - Catalogar todos os *softwares* utilizados, especificando as versões e licenças;
    - Criar um inventário de aplicações em execução nos computadores através de ferramentas automatizadas, como o Spiceworks ou Lansweeper, ou manualmente, e registar todos programas instalados no sistema operativo;
    - Verificar periodicamente quais as aplicações de *software* estão em execução nos dispositivos.
  - Consultar o *Software Asset Management Policy Template for CIS Control* 2[24];
  - Para o registo da informação pode ser utilizada o exemplo disponibilizado na Tabela 18.

**Tabela 18 – Inventário de Software**

| Inventário de Sofware | | | | | | |
|---|---|---|---|---|---|---|
| Listar todos os softwares que são utilizados regularmente. Incluir o nome da aplicação, descrever como ele usado e informações de licenciamento relevantes, se aplicável. Considerar o software para laptops, servidores, sistemas de PoS e até mesmo aplicações móveis. | | | | | | Revisão: Trimestral |
| **Nome do Software** | **Tipo** | **Descrição** | **Versão** | **Produtor** | **Tipo de Licença** | **Chave de Licenciamento** |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |
| | | | | | | |

**Nome:**
**Data de Revisão:**

[24] https://www.cisecurity.org/insights/white-papers/software-asset-management-policy-template-for-cis-control-2

- **Inventário de Dados**
  - Ações:
    - Identificar e documentar os dados críticos armazenados na empresa, como informações financeiras e pessoais;
    - Garantir que todos os dados abrangidos por um quadro regulamentar sejam adequadamente protegidos de acordo com essa estrutura (exemplo RGPD).
  - Consultar o *Data Management Policy Template for CIS Control* 3[25] e *Audit Log Management Policy Template for CIS Control* 8 [26];
  - Para o registo da informação pode ser utilizada o exemplo disponibilizado na Tabela 19.

**Tabela 19 – Inventário de Dados**

| Inventário de Dados | | | | |
|---|---|---|---|---|
| Listar todas as informações confidenciais da empresa (por exemplo: PII, registos financeiros). Considerar todos os dados armazenados nos dispositivos nos inventários da sua empresa, software e fornecedores de serviços. Incluir o nome do ficheiro, onde ele está armazenado e as pessoas com acesso. | | | | Revisão<br>Trimestral |
| **Nome do Ficheiro** | **Localização** | **Tipo de Media** | **Razões da Sensibilidade\Tipo de dados** | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| **Nome:**<br>**Data de Revisão:** | | | | |

- **Inventário de Fornecedores de Serviços:**
  - Ações
    - Criar um inventário de serviços *web* ou soluções *cloud* como Google Workspace, Microsoft 365, SalesForce, incluindo a finalidade de uso e os responsáveis pela gestão de cada serviço;
    - Verificar junto dos utilizadores quais os serviços *online*, como como plataformas de partilha de ficheiros e colaboração *online* são utilizadas como parte de seu trabalho;
    - Desenvolver uma estratégia empresarial para permitir que os utilizadores utilizem serviços *online* novos e aprovados de que necessitam.

[25] https://www.cisecurity.org/insights/white-papers/data-management-policy-template-for-cis-control-3
[26] https://www.cisecurity.org/insights/white-papers/audit-log-management-policy-template-for-cis-control-8

- Consultar *o Service Provider Management Policy Template for CIS Control 15*[27]
- Para o registo da informação pode ser utilizada o exemplo disponibilizado na Tabela 20.

**Tabela 20 – Inventário de Fornecedores de Serviços**

| Inventário de Fornecedores de Serviços | | | | |
|---|---|---|---|---|
| Listar todos os fornecedores de serviços que são utilizados regularmente e descrever para que o serviço é usado. Incluir o nome do utilizador principal para o fornecedor de serviços. Considerar fornecedores de serviços para aplicações web (como por exemplo, Gmail, M365), fornecedores de comunicações e serviços móveis. | | | | Revisão: Trimestral |
| **Nome do Produto** | **Descrição** | **Utilizador Principal** | **Dados Sensíveis Armazenados na Plataforma** | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| **Nome:** | | | | |
| **Data de Revisão:** | | | | |

- **Inventário de Contas**
  - Ações:
    - Criar uma lista de todas as contas de utilizadores, serviço e de administração, documentando as permissões e os níveis de acesso;
    - Verificar junto dos utilizadores a identificação dos *websites* e serviços que são utilizados para o negócio da empresa;
    - Desenvolver uma estratégia para criar e documentar os novos recursos da empresa.
  - Consultar *Account and Credential Management Policy Template for CIS Control* 5 e 6[28];
  - Para o registo da informação pode ser utilizada o exemplo disponibilizado na Tabela 21.

[27] https://www.cisecurity.org/insights/white-papers/service-provider-management-policy-template-for-cis-control-15

[28] https://www.cisecurity.org/insights/white-papers/account-and-credential-management-policy-template-for-cis-controls-5-and-6

**Tabela 21 – Inventário de Contas**

| Inventário de Contas | | | | |
|---|---|---|---|---|
| Listar todas as contas que existem para toda a sua empresa. Utilizar os inventários de ativos corporativos, software e fornecedores de serviços como guia para documentar contas. Incluir o nome de utilizador, para que serve a conta e se essa conta é usada por vários pessoas. | | | | Revisão: Trimestral |
| **Fornecedor do Produto ou Serviço** | **Dono da Conta** | **Utilizador** | **Conta Partilhada? (Sim/Não)** | **Outras Notas** |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| | | | | |
| **Nome:** | | | | |
| **Data de Revisão:** | | | | |

### C.2.2 Proteção de Ativos

A segunda fase envolve a configuração segura dos dispositivos inscritos no inventário de ativos. Esta etapa inclui a implementação de políticas de configuração, defesa contra *malware* e gestão de vulnerabilidades.

- **Atualização *Browsers* e *Plugins*** - Garantir que todos os *browsers* e clientes de *e-mail* se encontram atualizados e que os mesmos se atualizam automaticamente;
- **Proteção contra *Malware*** - Instalar e manter softwares anti-*malware* atualizados em todos os dispositivos. Pode ser utilizado o *Malware Defense Policy Template for CIS Control 10* [29];
- **Uso de DNS Seguro** - Configurar serviços de DNS seguros para navegação *web*;
- **Limitação de Mídias Removíveis** - Restringir o uso de dispositivos de armazenamento removíveis para minimizar riscos de infeção e perda de dados;
- **Criptografia de Dados** - Usar criptografia para proteger dados sensíveis armazenados em dispositivos móveis e *laptops*, assim como para transmissão de informações confidenciais;
- **Configuração Segura de Dispositivos** - Garantir que todos os sistemas operativos e aplicações se encontram configurados com as melhores práticas de segurança, no

[29] https://www.cisecurity.org/insights/white-papers/malware-defense-policy-template-for-cis-control-10

*Secure Configuration Management for CIS Control* 4[30] e *Vulnerability Management Policy Template for CIS Control* 7[31].

Para o cumprimento de algumas destas ações podem ser utilizadas algumas ferramentas como:

- Uso de ferramenta como o *Qualys Browser Check*[32] para validar se o mesmo se encontram atualizados;
- Uso do *Microsoft Defender* Antivírus para proteção em sistemas Windows e *Malwarebytes*[33] para proteção adicional;
- Implementação do Quad9[34] como serviço de DNS padrão em todos os dispositivos da empresa;
- Configurar políticas de grupo na *Active Directory* para desativar a execução automática de mídias removíveis;
- Ativar o *BitLocker* em dispositivos *Windows* e *FileVault* em dispositivos Mac para cifragem dos discos rígidos;
- Utilizar a ferramenta OpenVas[35] para fazer verificações de segurança e criação de *baseline;*
- Para o registo da informação pode ser utilizada o exemplo disponibilizado na Tabela 22.

**Tabela 22 – Ficha de Proteção de Ativos**

| Ficha de Proteção de Ativos | |
|---|---|
| **Executar as ações a seguir para cada ativo da empresa. Utilizar o inventário de ativos de hardware para garantir que cada ativo esteja representado. Preencher também a ficha de segurança da conta.** | **Revisão**<br>Trimestral |

| Sim/Não | Nome do Ativo: |
|---|---|
| | Verificar de que todos os softwares instalados no sistema se encontram atualizados. |
| | Verificar se o dispositivo se encontra cifrado. |
| | Garantir que o ecrã do dispositivo seja bloqueada automaticamente após 10 minutos (600 segundos). |
| | Ativar a firewall e a proteção de rede. |
| | Verificar que as atualizações automáticas estão ativadas para o sistema operativo, como Windows ou MacOS. |
| | Certifique-se de que as atualizações automáticas estejam ativadas em cada aplicação. |
| | Utilizar apenas browsers de internet atualizados e modernos. |
| | Utilizar apenas aplicações de e-mail atualizados e modernos. |
| | Utilizar serviços DNS seguros, como Quad9. |
| | Instalar e ativar um software antivírus e assinaturas se encontram atualizados automaticamente. |
| | Desativar a execução automática e a reprodução automática para sistemas Windows. |

**Nome:**
**Data de Revisão:**

[30] https://www.cisecurity.org/insights/white-papers/secure-configuration-management-for-cis-control-4
[31] https://www.cisecurity.org/insights/white-papers/vulnerability-management-policy-template-for-cis-control-7
[32] https://browsercheck.qualys.com
[33] https://pt.malwarebytes.com
[34] https://quad9.net/
[35] www.openvas.org

### C.2.3 Segurança de Contas

A terceira fase concentra-se na segurança das contas usadas na empresa. Esta etapa envolve a criação de palavras-passe seguras, uso de autenticação multifator (MFA) e a alteração de palavras-passe padrão de todos os dispositivos e serviços.

- **Política de Palavras-passe** - Garantir que todas as contas utilizem palavras-passe fortes (mínimo de 14 caracteres, caso não utiliza MFA);
- **Alteração de palavras-passe Padrão** - Modificar todas as palavras-passe padrão de aplicações, sistemas operativos, *routers* e outros dispositivos ao adicioná-los à rede;
- **Gestão de Contas de Administração** - Estabelecer palavras-passe fortes e únicas para contas de administração e restringir o seu uso;
- **Ativação do MFA** - Utilizar o MFA quando disponível, especialmente para acessos remotos á rede interna, ou serviço de *e-mail*;
- **Gestor de credenciais** - usar um gestor de credenciais para ajudar a lembrar palavras-passe longas, apoiar na criação de palavras-passe complexas e exclusivas.

Para o cumprimento de algumas destas ações podem ser utilizadas algumas ferramentas como:

  - Utilizar o guia *Account and Credential Management Policy Template for CIS Control* 5 *and* 6 [36];
  - Uso do KeePass[37] para gerar e armazenar palavras-passe fortes e únicas para todas as contas de utilizador;
  - Utilizar o *website Have I Been Pwned*[38], para verificar se seus endereços de *e-mail* estiveram envolvidos em uma violação de dados;
  - Para o registo da informação pode ser utilizada o exemplo disponibilizado na Tabela 23.

[36] https://www.cisecurity.org/insights/white-papers/account-and-credential-management-policy-template-for-cis-controls-5-and-6
[37] https://keepass.info
[38] https://haveibeenpwned.com

**Tabela 23 – Ficha de Proteção de Contas**

| Ficha de Proteção de Contas | |
|---|---|
| **Concluir as seguintes ações para cada conta na empresa. Deve utilizar o inventário de contas para garantir que cada conta esteja representada. Preencher também a ficha de Proteção de Ativos.** | **Revisão**<br>Trimestral |

| Sim/Não | Identificação da Conta: |
|---|---|
| | Garantir que a conta se encontra protegida de alguma forma através de password, PIN ou código. |
| | Garantir que a password desta conta não é utilizada usada em nenhuma outra, incluindo contas pessoais. |
| | Se a conta não já não for necessária, remova-a ou desative-a. |
| | Ativar a autenticação multifator para esta conta. |

**Nome:**
**Data de Revisão:**

### C.2.4 Backup e Recuperação

A quarta fase foca na criação e gestão de *backups* para garantir a recuperação de dados em caso de incidentes cibernéticos.

- **Criação de *Backups*** - Realizar *backups* regulares de dados críticos, armazenando cópias em locais seguros e *offline*. Garantir que pelo menos um dos backups não está acessível na rede, pois fornece proteção adicional contra o Ransomware. Proteger também dados em papel físico;
- **Testes de Recuperação** - Periodicamente testar os *backups* para assegurar que os dados podem ser restaurados corretamente;
- **Remoção de informação sensível** - Remover informação sensível dos computadores que já não necessitam.

Para o cumprimento de algumas destas ações podem ser utilizadas algumas ferramentas como:

  - Utilizar serviços de backup na nuvem, como o Microsoft OneDrive, e armazenar cópias *offline* em discos rígidos externos, garantir que a informação se encontra encriptada;
  - Utilizar ferramentas dos próprios Sistemas operativos como o *Microsoft Backup and Restore* e *Apple Time Machine*, para a realização de *backups*;
  - Realização de auditorias aos equipamentos dos utilizadores;
  - Consultar o *Data Recovery Policy Template for CIS Control* 11[39];
  - Para o registo da informação pode ser utilizada o exemplo disponibilizado na Tabela 24.

[39] https://www.cisecurity.org/insights/white-papers/data-recovery-policy-template-for-cis-control-11

**Tabela 24 – Ficha de Backups e Recuperação**

| Ficha Backup e Recuperação | |
|---|---|
| **Cada dispositivo da sua empresa pode conter informações importantes que valem a pena serem armazenadas e protegidas em caso de incidente de cibersegurança ou desastre natural. Deve executar as seguintes ações para cada ativo da empresa.** | **Revisão**<br>Trimestral |

| Sim/Não | Nome do Ativo: |
|---|---|
| | Decidir quanto tempo os dados deste dispositivo devem ser armazenados. |
| | Exclua dados desnecessários de forma segura. |
| | Automatizar backups através de uma ferramenta, ou copiar as informações para uma disco removível regularmente |
| | Manter uma cópia das informações importantes e confidenciais off-line. |
| | Verificar se nos serviços de backup utilizados os dados se encontram cifrados. |
| | Manter todas as cópias físicas de backups (por exemplo, papel, pen drives) protegidas contra roubo ou destruição. |
| | Manter uma cópia dos dados confidenciais e importantes noutro outro local físico. Podem ser utilizados serviços de armazenamento em cloud. |

**Nome:**
**Data de Revisão:**

### C.2.5 Resposta a Incidentes

A quinta fase envolve a preparação para responder a incidentes de cibersegurança de forma eficaz, minimizando danos e garantindo a continuidade dos negócios.

- **Preparação**
  - **Plano de Resposta a Incidentes** - Desenvolver e documentar um plano de resposta a incidentes, incluindo procedimentos para diferentes tipos de incidente. *Incident Response Policy Template for CIS Control* 17[40];
  - **Identificar de responsável** - Identificar a pessoa que irá liderar o processo em caso de incidente;
  - **Partilha de informação** - Aderir a comunidades de partilha de informações de Cibersegurança, como o CNCS[41];
  - **Lista de contatos** - Manter uma lista de contatos externos como parte do seu plano. Estes poderiam incluir consultores jurídicos, agentes de seguros, se você oferece cobertura contra riscos cibernéticos e consultores de segurança;
  - **Legislação** – Estar ao corrente com as leis de notificação de violação de dados do seu estado;
  - **Preparação das Equipa** - Treinar a equipa para reconhecer e responder a incidentes de cibersegurança conforme o plano estabelecido; Realizar *workshops* de simulação de incidentes para familiarizar a equipa com os procedimentos de resposta.
  - Para o registo da informação pode ser utilizada o exemplo disponibilizado na Tabela 25.

[40] https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17
[41] https://dyn.cncs.gov.pt/pt/alertas/

**Tabela 25 – Ficha de Resposta a Incidentes**

| Ficha de Resposta a Incidentes | |
|---|---|
| | **Revisão** |
| **Preencher as seguintes informações para garantir que se está preparado caso exista um incidente de cibersegurança.** | Trimestral |
| **Designar a pessoa líder no tratamento de incidentes de cibersegurança.** | |
| Nome: | |
| Telefone | |
| Email: | |
| **Lista de pessoas ou empresas a contatar em caso de incidente? Incluir informações de contato. Esta lista pode conter forças da autoridades, técnicos de TI ou outros funcionários.** | |
| Nome da pessoa ou entidade: | |
| Telefone | |
| Email: | |
| **Nota: se ocorrer um incidente, solicitar que qualquer pessoa técnica responsável pelo incidente armazene e mantenha os ficheiros de log dos sistemas comprometidos. Isso inclui logs de aplicação e logs do sistema operativo.** | |
| **Sim/Não** | |
| | Informar os utilizadores sobre quem deve contatado, caso ocorra um incidente de cibersegurança. |
| **Nome:**<br>**Data de Revisão:** | |

- **Se ocorrer um incidente**:
  - Em Portugal a notificação de incidentes de cibersegurança deve ser feita através do *website* da CNCS[42] ou através de *e-mail* cert@cert.pt, no caso de entidades reguladas a notificação é obrigatória;
  - Considerar entrar em contato com um consultor de TI ou de cibersegurança se a natureza e a extensão do incidente não forem claras;
  - Considerar entrar em contato com o departamento de conformidade ou com um advogado se existirem suspeitas que informações pessoais estiveram envolvidas no incidente;
  - Preparar-se para notificar quaisquer indivíduos afetados cujas informações pessoais tenham sido envolvidas em uma violação;
  - Informar as autoridades conforme necessário;

### C.2.6 Educação em Cibersegurança

A última fase assegura que todos os funcionários estejam cientes das práticas de cibersegurança e capacitados para identificar e prevenir incidentes.

- **Identificar dados Sensíveis** - Identificar pessoas da organização que lidam com dados sensíveis;
- **Política de Educação em Cibersegurança** - Implementar uma política de formação contínua em cibersegurança para todos os utilizadores;

[42] https://www.cncs.gov.pt/pt/notificacao-incidentes/#linhasobservacao

- **Verificação de Conhecimento** - Realizar avaliações periódicas para verificar a compreensão dos utilizadores sobre práticas de segurança;
- Consultar o *Security Awareness Skills Training Policy Template for CIS Control 14*[43].

Para o cumprimento de algumas destas ações podem ser seguidas algumas boas práticas como:

- Certificar-se de que todos sabem que o bom senso é, em última análise, a sua melhor defesa. Se algo parecer estranho, suspeito ou bom demais para ser verdade, provavelmente é uma tentativa de ataque;
- Incentivar o uso de *passwords* fortes e exclusivas para cada conta e autenticação multifator sempre que possível;
- Exigir que todos usam o bloqueio de ecrã nos dispositivos móveis;
- Certificar-se de que todos os utilizadores entendam como manter os seus dispositivos e *softwares* atualizados;
- Realizar testes trimestrais de *phishing* para avaliar a capacidade da equipa de identificar e evitar ataques;
- Na Tabela 26 são apresentados alguns conteúdos de sensibilização de áreas mais críticas;
- Outras ferramentas como o Microsoft Defender for O365[44] e o KnowBe4[45], podem ser utilizadas para outros conteúdos em português, permitindo ainda a utilização de testes de p*hishing*;
- Consular os recursos de formação disponibilizados pela CNCS na plataforma NAU[46].

**Tabela 26 – Lista de Formações**

| Engenharia Social |
|---|
| Security Awareness: Phishing & Ransomware |
| Security Awareness: Vishing |
| (ISC)² U.S. Military Germany |
| SANS Security Awareness: Social Engineering |
| Social Engineering Webinar |
| Professor Messer |
| **Autenticação** |
| Security Awareness: Passwords |
| Professor Messer: Authentication Methods |
| Professor Messer: Password Attacks |
| **Manuseamento de dados** |
| Security Awareness on Data Handling |

[43] https://www.cisecurity.org/insights/white-papers/security-awareness-skills-training-policy-template-for-cis-control-14
[44] https://learn.microsoft.com/pt-pt/defender-office-365/attack-simulation-training-simulations
[45] https://www.knowbe4.com/products/security-awareness-training
[46] https://www.nau.edu.pt/pt/

| |
|---|
| DoD CyberExchange: Identifying & Safeguarding PII |
| SANS Data Security |
| **Exposição não intencional de dados** |
| Security Awareness: Removable Media |
| Security Awareness: Data Leakage |
| Physical Security Awareness |
| **Reporte de incidentes de segurança** |
| Security Awareness Training: Reporting an Incident |
| Incident Reporting |
| **Identificação falta de atualizações de segurança** |
| Software Updates |
| End User Browsing |
| **Ligação se redes inseguras** |
| Security Awareness: Wifi |

O CNCS desenvolveu a C-Academy[47], que é uma iniciativa de formação avançada em cibersegurança que tem como objetivo desenvolver competências específicas nessa área. Além disso, promove está a promover a C-Network[48], que é uma rede de centros de competências em cibersegurança que visa incentivar a cooperação e o desenvolvimento de capacidades entre diversas entidades.

## C.3 *Safeguards* do IG1 adicionais

O *Implementation Guide for Small and Medium Sized Enterprises CIS Controls* IG1 [39], utilizado na Secção anterior, responde a 49 das 56 *safeguards,* faltando assim a mitigação das seguinte 7 *safeguards*:

- 3.3 - Configurar listas de controlo de acesso a dados;
- 4.4 - Implementar e gerir uma *firewall* nos servidores;
- 4.6 - Gerir com Segurança os ativos e *Software* Corporativos ;
- 6.5 - Exigir MFA para acesso administrativo;
- 8.1 - Estabelecer e manter um processo de gestão de *log* de auditoria;
- 8.2 - Recolher l*ogs* de auditoria;
- 12.1 - Garantir que a infraestrutura de rede está atualizada.

Sendo que o 12.1 não foi mapeando com os requisitos do SMD em Cibersegurança, apresentam-se sugestões de implementação\mitigação das restantes 6 *safeguards*.

[47] https://www.cncs.gov.pt/pt/c-academy/
[48] https://www.cncs.gov.pt/pt/c-network/

### C.3.1 Configurar listas de controlo de acesso a dados

Para mitigar o *safeguard* 3.3 do *CIS Controls*, que envolve a configuração de listas de controlo de acesso a dados (ACLs), podem ser seguidas as seguintes fases:

- Identificar os dados Sensíveis – já realizado anteriormente, utilizando a Tabela 19;
- Definição de Políticas de Acesso - conceder acesso apenas às pessoas que realmente precisam desses dados para suas funções.

Para o cumprimento, podem ser tomadas as seguintes ações técnicas e utilizadas algumas das seguintes ferramentas como:

- Configuração de ACLs:
  - Sistemas de Ficheiros - em Windows para configurar as permissões, utilizar o *icacls*[49] ou através do explorador de ficheiros. Em Linux, utiliza comandos como *chmod*[50] e *setfacl*[51];
  - Nas aplicações - ajustar as configurações de segurança dentro das próprias;
  - *Active Directory* (AD) -ferramenta da Microsoft usada para gerir permissões e políticas de acesso em um ambiente Windows, permite a configuração de ACLs para ficheiros e pastas, o controlo de acesso é baseado em grupos, e políticas de segurança centralizadas;
  - *Netwrix Auditor*[52] – é uma ferramenta de auditoria e monitorização de segurança que permite identificar mudanças em permissões de acesso, geração de relatórios de conformidade, e análise de riscos.
- Revisão de acesso - regularmente avaliar e atualizar as listas de controlo de acesso conforme as necessidades dos utilizadores;

### C.3.2 Implementar e gerir uma *firewall* nos servidores

Para mitigar a *safeguard* 4.4 do *CIS Controls* que envolve a implementação e gestão de *firewall* nos servidores, podem ser seguidas as seguintes fases:

- Identificar os servidores relevantes que necessitam de *firewall*, devendo ser utilizada a lista de ativos da Tabela 17;
- Determine o tipo de *firewall* necessária: *firewalls* virtuais, *firewalls* de sistema operativo ou agentes de *firewall* de terceiros com base na infraestrutura e necessidades específicas.

[49] https://learn.microsoft.com/en-us/windows-server/administration/windows-commands/icacls
[50] https://www.geeksforgeeks.org/permissions-in-linux/
[51] https://www.geeksforgeeks.org/linux-setfacl-command-with-example/
[52] https://www.netwrix.com/

Para o cumprimento, podem ser tomadas as seguintes ações técnicas e utilizadas algumas das seguintes ferramentas como:

- Escolher a implementação de *firewall* necessária:
  - A *firewall* do sistema operativo no caso do Windows utilizar o Defender Firewall, ou as *iptables*[53] para Linux, através de linha de comandos;
  - *Firewall virtual* - para plataformas de *cloud* como AWS ou Azure;
  - *Firewall* de terceiros – através da instalação de agentes de *firewall* como Sophos[54], Watchguard[55], etc.
- Configuração de regras de *firewall*, definindo políticas de segurança:
  - Política de Negação: bloquear todo o tráfego por defeito e permitir apenas o tráfego necessário;
  - Permitir Tráfego Necessário: Especificar as portas e serviços que são permitidos, exemplo: HTTP (porta 80), HTTPS (porta 443), SSH (porta 22).
- Realização de testes e verificar:
  - Realizar testes para garantir que as regras de *firewall* estão a funcionar conforme o esperado, utilizar por exemplo o NMAP[56] para validar;
  - Verificar os *logs* da *firewall* regularmente para identificar e resolver qualquer tráfego indesejado ou bloqueios inesperados.

### C.3.3 Gerir com Segurança os ativos e *Software* Corporativos

Para mitigar a *safeguard* 4.6 do *CIS Controls* que envolve a gestão segura de ativos de rede e *software*, podem ser seguidas as seguintes fases:

- Acesso seguro a interfaces de administração:
  - *Secure Shell* (SSH) para acesso remoto seguro a servidores e dispositivos de rede;
  - *Hypertext Transfer Protocol Secure* (HTTPS), para aceder a interfaces *web*, assegurando que os dados transmitidos sejam cifrados;
  - *Remote Desktop Protocol* (RDP), para acesso remoto a *desktops*, com a opção de *Network Level Authentication* (NLA) e criptografia forte;
- Desativar protocolos inseguros:
  - Desativar Telnet e HTTP em todos os dispositivos e servidores, a menos que seja absolutamente necessário por razões operacionais, nesse caso devem ser tomadas medidas adicionais de segurança;

[53] https://www.geeksforgeeks.org/iptables-command-in-linux-with-examples/
[54] https://www.sophos.com
[55] https://www.watchguard.com
[56] https://nmap.org/

  - Se forem utilizadas ferramentas de acesso remoto como o VNC, verificar se a comunicação se encontra cifrada.
- Para validar uma a desativação de protocolos inseguros, pode ser utilizado o NMAP para pesquisar portas e identificar quais serviços e protocolos estão em uso. Exemplo: nmap -sV -p 1-65535 <endereço_IP>.

### C.3.4 Exigir MFA para acesso administrativo

Para mitigar a *safeguard* 6.5 do *CIS Controls*, que exige a implementação de autenticação multifator (MFA) para todas as contas de acesso administrativo, podem ser seguidas as seguintes fases:

- Listar todas as contas de administração que precisam de MFA, incluindo em servidores, aplicações, serviços em *cloud* e dispositivos de rede. Utilizar a Tabela 21;
- Verifique quais sistemas e aplicações já suportam MFA nativamente e identifique aqueles que podem precisar de soluções adicionais;
- Escolher uma da Solução de MFA de acordo com as necessidades como é o caso de: *Microsoft Authenticator*[57]*, Authpoint*[58];
- Integração com sistemas existentes:
  - Sistemas operativos, configurar o MFA para acesso ao sistema operativo, usando ferramentas como *Windows Hello for Business*[59] ou autenticação *Pluggable Authentication Module* (PAM)[60] em Linux;
  - Aplicações em *cloud*, ativar o MFA como AWS, Azure, Google Cloud, e SaaS *(Software as a Service)* como Office 365, Salesforce, etc.
- Gestão de exceções e soluções alternativas:
  - Definir um processo claro para gerir exceções onde a implementação de MFA não é possível, garantindo que qualquer exceção seja documentada e aprovada;
  - Em casos onde MFA não pode ser implementado diretamente, considere alternativas como VPNs seguras com MFA ou *gateways* de acesso seguro.

### C.3.5 Estabelecer e manter um processo de recolha e gestão de *log* de auditoria

Para mitigar as *safeguards* 8.1 e 8.2 do *CIS Controls,* que envolvem a gestão, retenção e revisão de *logs* de auditoria de forma eficaz, podem ser seguidas as seguintes fases:

[57] https://www.microsoft.com/pt-pt/security/mobile-authenticator-app
[58] https://www.watchguard.com/wgrd-products/authpoint/multi-factor-authentication
[59] https://learn.microsoft.com/en-us/windows/security/identity-protection/hello-for-business/
[60] https://www.geeksforgeeks.org/what-is-linux-pam-module-and-how-to-configure-it/

- Definir requisitos de *logging*:
    - Identificar dos ativos empresariais (servidores, dispositivos de rede, aplicações, serviços de *cloud*, etc.) que precisam de *logs*;
    - Definir quais os tipos de *logs* que devem ser recolhidos (eventos de segurança, acessos, alterações de configuração, falhas, etc.);
    - Alinhar os requisitos de *log* com normas de conformidade relevantes (por exemplo: GDPR, ISO/IEC 27001).
- Recolha de *logs*, nos ativos identificados:
    - Nos sistemas operativos, ativar o *log* de eventos no Windows (*Event Viewer*) e no Linux (*syslog*);
    - Nos dispositivos de rede, configure log em *routers*, *switches* e *firewalls*;
    - Nas aplicações, garantir que as aplicações críticas estão configuradas para gerar *logs* de atividades importantes;
    - Nos serviços de *cloud,* utilizar serviços de *log* oferecidos pelos fornecedores (exemplo: AWS *CloudTrail*, *Azure Monitor*).
- Centralização de *logs*, podem ser utilizadas soluções SIEM[61], como solução de gestão e análise de informações de segurança:
    - Splunk[62] - Plataforma de análise e monitorização de logs de acesso, auditoria de segurança, e geração de relatórios;
    - ELK Stack (Elasticsearch, Logstash, Kibana)[63] - Conjunto de ferramentas para pesquisa, análise e visualização de dados. Recolhe e analisa *logs* de acesso, visualização de dados de segurança, e geração de relatórios personalizados.
- Definir política de retenção de *logs*:
    - De curto prazo, definir períodos de retenção para *logs* de curto prazo (30 a 90 dias) para análise imediata;
    - De longo prazo, estabelecer períodos de retenção para *logs* de longo prazo (de vários anos) para conformidade regulatória.

## C.4 *Safeguards* do IG2

Como indicado no processo de mapeamento foram identificas 5 *safeguards* adicionais do IG2, pelo que também se apresentam algumas sugestões de implementação das mesmas.

[61] https://www.microsoft.com/pt-pt/security/business/security-101/what-is-siem
[62] https://www.splunk.com/
[63] https://www.elastic.co/

### C.4.1 Implementar o DMARC

Para mitigar a *safeguard* 9.5 relacionada à redução de e-*mails* falsificados ou modificados de domínios válidos, devem ser implementadas políticas e verificações DMARC, para isso podem ser seguidas as seguintes fases:

- Implementação de SPF[64]:
  - Definir os Endereços IP Autorizados;
    - Listar os servidores de *e-mail* que estão autorizados a enviar *e-mails* em nome do seu domínio;
  - Criar ou atualizar o registo SPF no DNS do seu domínio. O registo SPF especifica quais servidores de e-mail têm permissão para enviar e-mails:
    - Exemplo simples: v=spf1 ip4:192.168.0.1 include:_spf.example.com ~all.
- Implementação de DKIM[65]:
  - Geração de Chaves DKIM:
    - Gerar um par de chaves DKIM (pública e privada) para assinar os e-mails;
    - Configurar o servidor de e-mail para usar a chave privada para assinar os e-mails (nem todos os servidores de *e-mail* possuem esta capacidade).
  - Criar o registo de DKIM no DNS, para isso é necessário publicar a chave pública como um registo do tipo TXT;
    - Exemplo simples: default._domainkey.example.com IN TXT "v=DKIM1; k=rsa; p=<chave-pública>".
- Implementacão de DMARC[66]:
  - Definição da política, definir a política DMARC para o domínio. Pode ser *none* (nenhuma ação), *quarantine* (quarentena) ou *reject* (rejeitar);
  - Configuração do registo DMARC no DNS. O registo DMARC é um registo TXT no DNS que segue o formato: _dmarc.example.com IN TXT "v=DMARC1; p=none; rua=mailto:dmarc-reports@example.com; ruf=mailto:dmarc-reports@example.com; fo=1":
    - Exemplo Simples: v=DMARC1; p=none; rua=mailto:dmarc-reports@example.com.
- Ferramentas para apoio na implementação:

[64] https://mxtoolbox.com/dmarc/spf/setup/how-to-setup-or-modify-spf
[65] https://mxtoolbox.com/dmarc/dkim/setup/how-to-setup-dkim
[66] https://mxtoolbox.com/dmarc/details/how-to-setup-dmarc

  - SPF Record Generator: Ferramentas online como MXToolbox[67] ou SPF Wizard[68] para criar registos SPF;
  - DKIM Tools: Ferramentas como EasyDMARC[69] ou DKIM Core[70] para gerar e verificar chaves DKIM;
  - DMARC Analyzer: Serviços como EasyDMARC[71] ou MXToolbox[72] para analisar e gerenciar políticas DMARC.
- Para o processo de verificação pode ser utilizada a ferramenta sugerida nos SMD em Cibersegurança - https://webcheck.pt/pt/

### C.4.2 Estabelecer e manter uma arquitetura de rede segura

Para mitigar a *safeguard* 12.2 que exige o estabelecimento e a manutenção de uma arquitetura de rede segura, abordando segmentação, princípio do menor privilégio e disponibilidade, para isso podem ser seguidas as seguintes fases:

- Planear o *design* de arquitetura segura:
  - Identificação de segmentos: dividir a rede em segmentos distintos, como servidores, dispositivos de utilizadores, dispositivos IoT e sistemas críticos;
  - Sub-redes e VLANs: usar sub-redes e VLANs (*Virtual Local Area Networks*) para isolar diferentes tipos de tráfego e limitar a propagação de ameaças;
  - Zonas de segurança: criar zonas de segurança com base no nível de sensibilidade e importância dos ativos, como zonas de DMZ (*Demilitarized Zone*) para servidores expostos à *internet*, zonas internas para sistemas corporativos e zonas restritas para dados altamente sensíveis.
- Disponibilidade:
  - Implementar mecanismos de redundância e *failover*, como *routers* e *switches* redundantes, para garantir a continuidade do serviço em caso de falhas;
  - Utilizar balanceadores de carga para distribuir o tráfego de rede de maneira eficiente e evitar sobrecarga em um único ponto.
- Tecnologia e ferramentas:
  - Implementar *firewalls* de próxima geração (NGFW[73]) que oferecem recursos avançados de inspeção de pacotes e controlo de aplicações;
  - Utilizar IPS para detetar e bloquear atividades maliciosas na rede.

[67] https://mxtoolbox.com/
[68] https://www.spfwizard.net/
[69] https://easydmarc.com/tools/dkim-record-generator
[70] https://dkimcore.org/tools/
[71] https://easydmarc.com/tools/dmarc-record-generator
[72] https://mxtoolbox.com/DMARCRecordGenerator.aspx
[73] https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw

### C.4.3 Estabelecer e manter diagrama(s) de arquitetura

Para mitigar a *safeguard* 12,4 que exige a criação e manutenção de diagramas de arquitetura e/ou outra documentação do sistema de rede, para isso podem ser seguidas as seguintes fases:

- Criação de diagramas de arquitetura e documentação de rede
  - Utilizar a Tabela 17, onde foram identificados os ativos da rede, incluindo servidores, dispositivos de rede (*routers*, *switches*, *firewalls*), *endpoints* e serviços *cloud*;
  - Mapear as conexões entre os diferentes componentes da rede, identificando as rotas de comunicação, segmentações de rede e dependências entre sistemas.
- Ferramentas de desenho e documentação
  - Microsoft Visio[74] - ferramenta para criação de diagramas de rede e arquitetura;
  - Draw.io[75] - ferramenta gratuita em *cloud* para criação de diagramas.
- Manutenção Contínua da Documentação
  - Atualizar os diagramas de rede e a documentação de acordo com as mudanças ocorridas no último ano, ou sempre que existirem alterações significativas na rede.

### C.4.4 Estabelecer e manter um processo de resposta a incidentes

A *safeguard* 17.4 é sem dúvida a mais exigente de mitigar, pois exige o estabelecimento e manutenção de um processo de resposta a incidentes, abordando papéis e responsabilidades, requisitos de conformidade e um plano de comunicação. Na Secção C.2.5 – Resposta a Incidentes, este ponto já for abordado parcialmente, podendo também ser utilizado o *template Incident Response Policy Template for CIS Control 17* [76]. Seguem-se mais algumas recomendações:

- Definir Papéis e Responsabilidades
  - Equipa de Resposta a Incidentes (IRT), formalizar a equipa dedicada na resposta a incidentes composta por membros da segurança da informação, TI, *compliance* e outras partes interessadas;
  - Papéis Específicos: Defina papéis claros dentro da equipa, como líder do incidente, analista de segurança, comunicador de incidentes, etc.
- Implementação do Processo de Resposta a Incidentes

[74] https://www.microsoft.com/pt-pt/microsoft-365/visio/flowchart-software
[75] https://www.drawio.com
[76] https://www.cisecurity.org/insights/white-papers/incident-response-policy-template-for-cis-control-17

- Definir claramente as etapas a serem seguidas durante a resposta a um incidente (identificação, contenção, erradicação, recuperação e análise pós-incidente);
- Criar guias de ação detalhados para diferentes tipos de incidentes (por exemplo, ataque de *phishing*, *ransomware*, fuga de dados).

- Ferramentas e Tecnologias de Suporte
  - Implementar um sistema SIEM para recolha e análise de *logs* de segurança em tempo real, como referido na Secção C.3.5.

# DECLARAÇÃO

Declaro, sob compromisso de honra, que o trabalho apresentado neste projeto, com o título "Proteção de PMEs no Ciberespaço - Aplicação de CIS Controls para resposta ao Selo de Maturidade Digital em Cibersegurança", é original e foi realizado por Estudante Lúcio Miguel Brites dos Santos Crespo (2220279) sob orientação do Professor Ricardo Gomes (ricardo.p.gomes@ipleiria.pt) e da Professora Doutora Marisa Maximiano (marisa.maximiano@ipleiria.pt)

Leiria, julho de 2024

Assinado por: **Lúcio Miguel Brites dos Santos Crespo**
Num. de Identificação: 11908283
Data: 2024.07.27 15:49:26+01'00'
CHAVE MÓVEL

_____

Estudante Lúcio Miguel Brites dos Santos Crespo