Lisbon School of Economics & Management
Universidade de Lisboa

MESTRADO EM

CIÊNCIAS EMPRESARIAIS

TRABALHO FINAL DE MESTRADO

DISSERTAÇÃO

AVALIAÇÃO DE IMPLEMENTAÇÃO DE CIBERSEGURANÇA EM EMPRESAS PORTUGUESAS: ANÁLISE DOS PRINCIPAIS DESAFIOS E MELHORES PRÁTICAS

SOFIA MARIA CÂMARA CORREIA

JUNHO 2025

Agradecimentos

Em primeiro lugar gostaria de agradecer ao meu orientador, o Professor Doutor Paulo Almeida Gonçalves, pelo seu apoio e conselhos precisos. Sem a sua experiência e perspetiva seria muito difícil guiar esta dissertação, assim agradeço a sua paciência e dedicação.

Agradecer ainda à minha família o seu contínuo apoio em todas as minhas Odisseias, sobretudo quando parece já não haver porto em Ítaca. Obrigada por incutirem em mim desde cedo o gosto pela aprendizagem, e a descoberta do desconhecido.

Estender ainda um especial agradecimento ao meu amigo Francisco, que ao longo de duas décadas de amizade não só foi companheiro académico (qual Sartre para o meu Camus), como tem sido sempre o meu fiel escudeiro filosófico. A ti, um grande *salvé*.

Resumo

No presente contexto empresarial e tecnológico, temos vindo a verificar uma contínua digitalização das organizações. Uma consequência deste fenómeno é o aumento do número de incidentes cibernéticos. O presente Trabalho Final de Mestrado incide sobre o tema da cibersegurança no contexto empresarial português, com particular destaque para as Pequenas e Médias Empresas (PMEs), dada a sua relevância económica e maior vulnerabilidade a ataques informáticos.

Este trabalho apresenta uma reflexão das dificuldades que as PMEs enfrentam na implementação de práticas eficazes de cibersegurança. Estas dificuldades estão frequentemente associadas à escassez de recursos financeiros, à ausência de pessoal qualificado e à fraca cultura de segurança digital das organizações.

Para levar a cabo esta investigação foram seleccionadas duas questões de investigação: (1) *Quais são as medidas de cibersegurança mais adotadas pelas empresas portuguesas?* e (2) *Quais são as ameaças de cibersegurança mais comuns nestas organizações?* Considerando estas questões, este estudo tem como objectivos identificar as práticas de cibersegurança atualmente em vigor, compreender os principais riscos enfrentados pelas organizações e analisar o grau de maturidade cibernética das empresas portuguesas, assim como o envolvimento dos seus quadros superiores na gestão da segurança digital.

O presente projecto utiliza um método qualitativo, baseado na realização de entrevistas a sete profissionais de variados setores de atividade. A análise temática dos dados foi feita com o apoio do software MaxQDA. Posteriormente, o resultado obtido nas entrevistas foi cruzado com a informação apresentada na Revisão de Literatura.

Alguns do resultados esperados nesta investigação incluem a identificação de práticas comuns de cibersegurança, como a utilização de firewalls, antivírus e políticas de backup, bem como a elevada frequência de tentativas de ataques de phishing. A análise revelou ainda disparidades significativas entre as empresas no que toca à maturidade cibernética, ao conhecimento dos colaboradores e ao envolvimento dos gestores de topo. Verificou-se também um conhecimento limitado sobre as diretivas legais aplicadas, e a ausência ou precariedade de formação estruturada em cibersegurança.

Por último, a investigação aponta para a necessidade de sensibilização e capacitação contínua das organizações, reforço da liderança na área da segurança digital, e adoção de normativas adaptadas à realidade das PMEs. A longo prazo, estas ações poderão contribuir para o fortalecimento da resiliência cibernética do tecido empresarial português.

Palavras-chave: Cibersegurança, PMEs, Empresas Portuguesas, Maturidade Cibernética, Ataques Cibernéticos, Formação de Colaboradores.

Abstract

In the current business and technological landscape, we have been witnessing a continuous digital transformation of organizations. One consequence of this phenomenon is the increase in the number of cyber incidents. This Master's dissertation focuses on the subject of cybersecurity in the Portuguese business context, with particular emphasis on Small and Medium-sized Enterprises (SMEs), given their significant economic impact and increased vulnerability to cyberattacks.

This paper examines the challenges faced by SMEs in implementing effective cybersecurity measures. These difficulties are often associated with a lack of financial resources, the absence of qualified personnel, and the organization's weak digital security culture.

To carry out this research, two research questions were selected: (1) What are the cybersecurity measures most adopted by Portuguese companies? and (2) What are the most common cybersecurity threats in these organizations? Considering these questions, this study aims to identify the cybersecurity practices currently in place, understand the main risks faced by organizations, and analyze the degree of cyber maturity of Portuguese companies, as well as the involvement of their senior management in digital security management.

This project employs a qualitative method based on interviews with seven professionals from diverse sectors. The data analysis was conducted using MaxQDA software. The results obtained in the interviews were then cross-referenced with the information presented in the Literature Review.

Some of the expected results include the identification of standard cybersecurity practices, such as the use of firewalls, antivirus, and backup policies, as well as the high

frequency of attempted phishing attacks. The analysis also revealed significant disparities between companies in terms of cyber maturity, employee knowledge, and the involvement of senior managers. There was also limited knowledge of the legal directives applied, as well as the absence of structured cybersecurity training.

Ultimately, the research underscores the importance of raising awareness and continually training organizations, enhancing leadership in digital security, and implementing regulations tailored to the specific realities of SMEs. In the long term, these actions could boost the cyber resilience of the Portuguese business community.

Keywords: Cybersecurity, SMEs, Portuguese Companies, Cybersecurity Maturity, Cyberattacks, Staff Training.

Índice

Capítulo I – Introdução

1.1 Contexto do estudo

A área de investigação desta dissertação insere-se no campo da cibersegurança aplicada às empresas portuguesas. Trata-se de uma pesquisa às práticas de cibersegurança utilizadas por empresas portuguesas, de variadas dimensões, identificando quais são os desafios mais comuns enfrentados por estas organizações.

Nos últimos anos, e com a contínua digitalização das empresas a nível mundial, temos verificado um aumento no número de ciberataques tanto a organizações públicas como no sector privado (Arroyable, 2024). Estes ataques representam uma crescente ameaça à cibersegurança das organizações mundiais, sendo que em 2023 o país europeu mais atacado foi o Reino Unido, contabilizando 23% dos casos, em segundo lugar a Alemanha, com 15% dos casos, seguido da Dinamarca, com 14% dos casos, em quarto lugar encontra-se Portugal, com 11% dos casos, e a Itália e a França ocupam o quinto lugar com 8% dos casos. (IBM, 2024)

De acordo com o relatório da (Allianz, 2023) os ciberataques eram maior risco para as empresas mundiais em 2024. O relatório afirma que 36% das respostas dadas pelos inquiridos lista os ataques de cibersegurança como um dos maiores riscos globais, pelo terceiro ano consecutivo. Um dos aspetos mencionados neste estudo, que se relaciona com o tema proposto, conecta-se às diferenças experienciadas pelas pequenas e médias empresas (PMEs) e grandes empresas. Visto que as grandes empresas possuem mais recursos financeiros, conseguem investir mais na sua cibersegurança do que as

PMEs. Portanto, as PMEs representam um alvo fácil pois estão mais vulneráveis a ciberataques. Posto isto, é igualmente importante mencionar que os colaboradores representam uma das maiores vulnerabilidades de uma empresa, e que apostar na sua contínua formação, bem como adotar medidas quantitativas e qualitativas de proteção, contribuem para o aumento de resiliência cibernética de uma organização (Deloitte, 2024).

1.2 Perguntas de investigação

Apesar da consciencialização para a pertinência deste tópico, algumas empresas continuam a encontrar desafios no que toca à implementação de práticas de segurança digital. Alguns dos problemas que parecem surgir prendem-se com questões de falta de visão e planeamento para a cibersegurança, como tal é necessário avaliar como é que as empresas portuguesas enfrentam estes obstáculos. Com isto em mente foram identificadas as seguintes questões de pesquisa: (1) Quais são as medidas de cibersegurança mais adotadas pelas empresas portuguesas? (2) Quais são as ameaças de cibersegurança mais comuns dentro destas organizações?

1.3 Estrutura

A escolha deste tema resulta da necessidade de compreender de que forma é realizada a gestão da cibersegurança no tecido empresarial português. Devido à limitação de estudos focados especificamente nas PMEs portuguesas, esta investigação procura contribuir para a comunidade académica através dos resultados obtidos, promovendo um

maior entendimento sobre a cultura organizacional portuguesa no que diz respeito à cibersegurança.

Para que as questões de investigação fossem respondidas de forma eficaz, comecei por pesquisar informação para o capítulo da "Revisão de Literatura". Este capítulo apresenta os principais conceitos para o tema estudado, através de uma explicação extensiva das ideias-chave. Este estudo conta com uma abordagem qualitativa, em que o processo de recolha de dados é feito através de entrevistas. Esta informação consta do capítulo da "Metodologia" do estudo, onde estão ainda incluídos os métodos de recolha e análise de dados utilizados, bem como um resumo dos resultados obtidos. O capítulo seguinte, intitulado "Apresentação dos resultados", apresenta os resultados do estudo de forma organizada e pormenorizada. Segue-se um capítulo intitulado "Resultados Análise e Discussão", que apresenta uma análise desses resultados, integrando-os com a literatura existente. No capítulo final, "Conclusões, Limitações e Futuras Investigações", são resumidos os resultados gerais do estudo, discutindo a sua significância bem como quais as limitações encontradas. Além disso, este capítulo sugere possíveis caminhos para investigação futura, salientando como a investigação subsequente pode basear-se no trabalho apresentado neste capítulo.

Capítulo II – Revisão de Literatura

2.1 Importância da cibersegurança nas PMEs

As PMEs são as maiores contribuidoras para a economia, sendo que aproximadamente 400 milhões destas empresas podem ser consideradas como o esqueleto da economia mundial (Pawar, 2022). Estas formam o principal tecido económico da Europa, constituindo 99,8% de todos os negócios europeus, e em 2024 empregaram cerca de 90 milhões de pessoas (Espinosa, 2024).

No entanto, apesar desta relevância, as pequenas e médias empresas apresentam uma grande vulnerabilidade aos ataques cibernéticos (Pawar, 2022). Visto que as ameaças cibernéticas continuam a aumentar, tornou-se crítica a necessidade em proteger os ativos digitais e aparelhos em rede (Department, Cybersecurity in Europe - statistics and facts, 2024).

Cada vez mais, a cibersegurança ocupa um lugar vital no panorama empresarial atual, pois esta define não só as práticas mais relevantes da área, bem como as tecnologias e medidas utilizadas para salvaguardar os sistemas de informação, as redes e os dados de possíveis ataques, danos, acesso não autorizado, ou roubo de informação (Arroyable, 2024). Por este motivo, e visto que os dados de informação são o recurso mais precioso de uma organização, a segurança de informação ocupa um lugar relevante na gestão empresarial, pois lida com a confidencialidade, privacidade e integridade destes mesmos recursos (Antunes, 2021).

Em 2024 a maioria dos estados-membros da União Europeia revelou que a cibersegurança era uma das preocupações de alta prioridade para as empresas (Department, Cybersecurity in Europe - statistics and facts, 2024). Por exemplo, desde

Janeiro desse ano que 1/3 das empresas no Reino Unido colocaram em prática políticas de cibersegurança, sendo que as PMEs foram as que mais medidas implementaram (Borgeaud, 2024). O mesmo autor revela ainda que em 2023 as empresas britâncias reportaram que quase ¼ do seu orçamento é dedicado à cibersegurança com o objetivo de proteger dados sensíveis, prevenir perda financeira e garantir a continuidade empresarial no mundo digital.

Não obstante, as PMEs enfrentam diferentes tipos de desafios no que toca à implementação de medidas de cibersegurança nas empresas (ENISA, 2021). Efectivamente, um estudo conduzido por Pawar (2022) revela que existe uma falta de controlos de cibersegurança nas PMEs, pois muitas não adotam normas ou padrões de segurança, e mesmo quando estes padrões são adotados, são implementados de uma forma superficial.

Apesar do crescente número de ataques cibernéticos dirigidos às PMEs, muitas destas empresas continuam a subestimar o risco, ou não implementam medidas eficazes de prevenção (Erdogan et al., 2023). Um inquérito a 141 PMEs britânicas, demonstra que embora cerca de 60% dos participantes expressem preocupação com a possibilidade de um ciberataque, 30% admite nunca discutir o tema internamente. É referido ainda que muitas PMEs desconhecem se foram atacadas, revelando falhas nos sistemas de monitorização (Erdogan et al., 2023).

Argumenta-se que as características tradicionais de uma PME, como por exemplo, a sua dimensão, a sua estrutura tipicamente familiar, bem como o tipo de recursos financeiros utilizados, colocam estas empresas numa posição menos favorável no que toca à segurança de informação e conhecimento sobre cibersegurança (Antunes, 2021). Em 2024, 74% das organizações europeias revelaram não providenciar qualquer tipo de

formação em cibersegurança aos seus colaboradores. Inclusive, na França, esta percentagem atinge mesmo os 90% (Department, Cybersecurity in Europe - statistics and facts, 2024). Este resultado pode ser evitado através da adoção de uma perspetiva holística, conectando os objetivos gerais da empresa com as necessidades operacionais, fazendo com que a cibersegurança não seja apenas uma medida reativa, mas sim uma medida proativa, que é integral ao funcionamento da organização (Deloitte, 2024).

Apesar das dificuldades enfrentadas pelas PMEs, a realidade europeia demonstra que alguns setores — como as telecomunicações, eletricidade e finanças — já revelam níveis de maturidade cibernética significativamente superiores. Estas organizações implementam planos estratégicos e operacionais, monitorizam continuamente os riscos e desenvolvem políticas de resposta a incidentes. Embora a maturidade em cibersegurança não elimine a possibilidade de ataques, contribui decisivamente para a resiliência organizacional e para a continuidade do negócio (ENISA, 2024; Deloitte, 2024). Este contraste evidencia a importância de adaptar e transpor boas práticas dos setores mais avançados para o contexto das PMEs, tendo em conta as suas limitações e especificidades.

2.2 Legislação existente e recomendações de boas práticas

Nos últimos anos temos assistido à criação e implementação de novas legislações que visam a cibersegurança dentro do espaço europeu. (ENISA, Report on the State of Cybersecurity in the Union, 2024) Algumas destas legislações incluem as seguintes:

1. A Diretiva NIS, na sua versão mais atual a Diretiva NIS 2, que visa providenciar medidas legais que impulsionem o nível de cibersegurança na UE através da imposição de obrigações legais às organizações de diversos setores, incluindo o setor energético, de transportes, a banca, mercados financeiros e o sector da saúde.

A diretiva impõe ainda que os estados-membros aumentem a sua preparação para incidentes através de missões para *Computer Security Incident Response Teams* (CSIRT's). A NIS2 promove também maior cooperação estratégica entre os estados-membros, visando o fortalecimento cibernético contínuo dos países do bloco, facilitando assim as trocas de informação (ENISA, Report on the State of Cybersecurity in the Union, 2024). Estas obrigações incluem a cooperação entre estados-membros, bem como a comunicação de qualquer incidente às autoridades competentes (CNCS, 2024).

2. A CRA (*European Cyber Resilience Act*) foi proposta pela comissão europeia em 2022 e adotada em 2024 com o objetivo de tornar a legislação de cibersegurança, no espaço europeu, mais coerente, garantindo a segurança dos produtos desde a cadeia de abastecimento e durante a sua comercialização (Department, EU Cyber Resilience Act - Statistics and Facts, 2024). Esta diretiva apresenta requerimentos comuns para a cibersegurança em produtos digitais como hardware e software (ENISA, Report on the State of Cybersecurity in the Union, 2024).
3. A CSOA (*Cyber Solidarity Act*), é uma diretiva que entrou em vigor no início de 2025. Ela apresenta medidas para fortalecer a capacidade europeia em detetar, preparar e responder a incidentes e ameaças de cibersegurança (ENISA, Report on the State of Cybersecurity in the Union, 2024).
4. A CSA (*Cyber Security Act*), entrou em vigor no final de 2024 e propõe a adoção de certificações europeias para serviços de segurança. O objetivo é criar um mecanismo de emergência de cibersegurança para aumentar o nível de preparação e capacidade de resposta a incidentes (EU, 2024).

5. A DORA (*Digital Operational Resilience Act*), que visa a regulamentação operacional e resiliência no setor financeiro, foi publicada 2023 e entra em vigor a partir de 17 de Janeiro de 2025 (DORA, s.d.).
6. No sector da saúde contamos com a EHDS (*European Health Data Space*), que se encontra na última fase do processo de adoção (ENISA, Report on the State of Cybersecurity in the Union, 2024). Esta directiva visa criar regras específicas dentro do sector da saúde, que ajudem os utentes a controlar a sua informação de saúde pessoal, tanto a nível nacional, como europeu (EHDS, s.d.).

Para garantir que uma organização está protegida, a (ENISA, 2021) disponibiliza um conjunto de boas práticas, especificamente delineadas para as PMEs. Estas práticas salientam:

a) A necessidade em desenvolver uma cultura de cibersegurança dentro de cada empresa.
b) Garantir que todos os contactos associados à organização, como por exemplo os fornecedores, possuem requerimentos de segurança digital.
c) Salvaguardar a segurança dos sistemas através da utilização de *passwords* fortes.
d) Utilizar medidas de segurança para os aparelhos, como anti-vírus e encriptação de dados.
e) Implementar medidas de segurança de redes, como uma *firewall.*
f) Melhorar a segurança física dos equipamentos portáteis da organização, como computadores ou telemóveis
g) Efectuar atualizações de segurança dos sistemas
h) Garantir a segurança dos ficheiros arquivados na *cloud*

i) Salvaguardar a segurança dos *websites* da organização

j) Monitorizar e partilhar informação

A nível internacional existem diferentes modelos de padrões como é o caso da ISO/IEC 27001 e 27002, que oferecem uma referência para a maturidade e conformidade em cibersegurança (Ludin, 2024). A norma ISO 27001 é o padrão para gestão de sistemas de informação mais conhecido no mundo, que indica que a empresa implementou uma série de medidas para proteger e gerir os seus dados e sistemas dos riscos associados ao mundo digital (ISO27001, 2022). Já a ISO 27002 é o detalhe de um conjunto de controlos indicados na 27001 (ISO27002, 2022).

Esta norma é amplamente reconhecida para a implementação e gestão de Sistemas de Gestão da Segurança da Informação (SGSI), fornecendo um conjunto estruturado de cláusulas e controlos agrupados em 14 domínios, como política de segurança, controlo de acessos e gestão de incidentes (Clarissa e Wang, 2023). Um caso de estudo a uma entidade pública na Indonésia demonstrou como a aplicação da norma ISO 27001 permite medir o grau de maturidade da organização em termos de segurança, detetando lacunas importantes entre os níveis de implementação técnica e a governança. Esta perspetiva é especialmente relevante para o contexto das PMEs, que frequentemente carecem de políticas formais estruturadas. (Clarissa e Wang, 2023).

Contudo, a implementação da ISO 27001 pode ser demasiado vasta para uma PME, visto ser muito exigente em termos de recursos, necessitando um investimento financeiro significativo, que muitas PMEs não conseguem cumprir devido à falta de orçamento (Ludin, 2024).

Os controlos CIS são um conjunto de boas práticas em cibersegurança que visam fortalecer a postura digital de uma organização, auxiliando-a a proteger-se das principais

ameaças cibernéticas (CIS, 2025). De forma similar ao destacado anteriormente, estes controlos podem representar um desafio na sua priorização e customização para as PMEs, pois o seu âmbito é muito alargado e pode necessitar ser alinhado com o âmbito operacional das PMEs (Ludin, 2024).

A NIST foi desenhada para ser implementada em organizações americanas, no entanto é um padrão que pode ser utilizado mundialmente (ITGovernance, s.d.). A sua implementação conta com cinco funções principais; identificar, proteger, detectar, responder, e recuperar. Estas acções fornecem uma visão geral da gestão do risco de uma organização (NIST, 2024). Outro benefício é o facto desta ferramenta ser flexível e fácil de ser reproduzida por organizações de tamanhos e sectores diferentes (Ludin, 2024).

A ASMA é um software de cibersegurança que foi desenhado para detectar quais são os activos presentes no sistema da organização (Barikat, 2025). Esta estrutura foi organizada consoante três pontos-chave que incluem componentes básicos, componentes estruturais e níveis de implementação. Foi especificamente desenhado para PMEs, oferecendo uma abordagem mais detalhada às suas necessidades (Ludin, 2024).

Para além das normas internacionais como o NIST e a ISO/IEC 27001, também existem esforços nacionais para adaptar boas práticas à realidade empresarial portuguesa (Azinheira et. al., 2023). Estas práticas propõem uma metodologia inovadora que estabelece uma correspondência entre o *Roadmap* para Capacidades Mínimas de Cibersegurança (RMCSC), publicado pelo Centro Nacional de Cibersegurança (CNCS), e os controlos do ISO/IEC 27001. Esta metodologia visa facilitar a compreensão e adoção das normas de cibersegurança por parte das PMEs portuguesas, traduzindo os requisitos técnicos em orientações de governança mais claras. O mapeamento sugerido permite que estas empresas realizem autoavaliações estruturadas, sem necessidade de conhecimentos

técnicos avançados, constituindo uma ferramenta prática de transição entre a teoria normativa e a realidade empresarial. (Azinheira et. al., 2023).

Apesar da existência de legislação e recomendações de boas práticas para a cibersegurança, a adoção de soluções tecnológicas eficazes de cibersegurança nas PMEs é frequentemente limitada por falta de conhecimento técnico e restrições orçamentais (Manzoor et al., 2024). Algumas destas opções apresentam barreiras à adoção, como complexidade na configuração, necessidade de personalização e ausência de suporte técnico. Este cenário confirma a importância de ferramentas adaptadas às capacidades reais das PMEs (Manzoor et al., 2024).

2.3 Principais riscos e ameaças

Existe a ideia de que devido à sua dimensão, as PMEs são menos suscetíveis a sofrer ataques informáticos, no entanto isto não é verdade, pois a realidade constata que à medida que as PMEs levam a cabo a sua digitalização ficam também mais expostas a incidentes de cibersegurança (Arroyable, 2024).

Estudos demonstram que 60% das PMEs, que foram vítimas de ciberataques, tendem a fechar o seu negócio seis meses após o mesmo, realçando o impacto e a gravidade que um ciberataque pode ter na sobrevivência de uma organização (Pawar, 2022).

Cerca de 43% dos ciberataques têm como alvo as PMEs**,** que se tornam presas fáceis pela ausência de medidas robustas de segurança, escassez de profissionais qualificados e restrições orçamentais. (Manzoor et al., 2024). Este problema agravou-se com o aumento do trabalho remoto desde a pandemia de COVID-19, criando novos vetores de ataque e expondo lacunas na proteção de dispositivos móveis e na prevenção

de ataques de *phishing*. Esta realidade evidencia a necessidade de soluções acessíveis e adaptadas às limitações técnicas e financeiras das PMEs (Manzoor et al., 2024).

Por exemplo, os ataques de *rasomware* têm muito potencial para causar problemas às operações de uma empresa, bem como danos financeiros e reputacionais, e por isso são uma das mais persistentes ameaças cibernéticas em todo o mundo (Petrosyan, Ransomware - statiscs and facts, 2024).

Em 2023 mais de 72% das empresas mundiais foram afetadas por ataques de *rasomware*, sendo que nos Estados Unidos da América, uma das indústrias mais afetadas por este tipo de ataque foi o setor da saúde (Petrosyan, Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023, 2024). Ainda nesse ano, a CISA, a agência americana para cibersegurança, reportou que as PMEs têm uma probabilidade cinco vezes maior para serem atacadas do que as grandes empresas (SONICWALL, 2024).

Já em 2024 os países aderentes da UE continuaram a ser alvo de cibercrimes, que visaram atacar governos, organizações em diversos setores e a sociedade civil em geral. Os dados representados na Figura 1 demonstram variadas categorias de ataques que ocorreram entre 2023 e 2024, sendo que os principais foram os ataques do tipo DoS/DDoS/RDoS e os ataques de *rasomware.* Os ataques de engenharia social, como o *phishing* merecem também particular destaque, visto que pretendem enganar as vítimas para obter as suas credenciais de acesso ao sistema da organização (ENISA, Report on the State of Cybersecurity in the Union, 2024).

Uma investigação elaborada por Ambreen et. al., (2023) revela que muitos destes ataques ocorrem por falta de políticas de proteção, erros humanos ou sistemas de segurança desatualizados. Apesar de as PMEs terem estruturas mais ágeis, muitas vezes

não investem em medidas básicas de proteção como *backups* regulares, encriptação ou planos de resposta a incidentes. Estas vulnerabilidades estruturais tornam os riscos ainda mais significativos num cenário digital cada vez mais complexo (Ambreen et al., 2023).

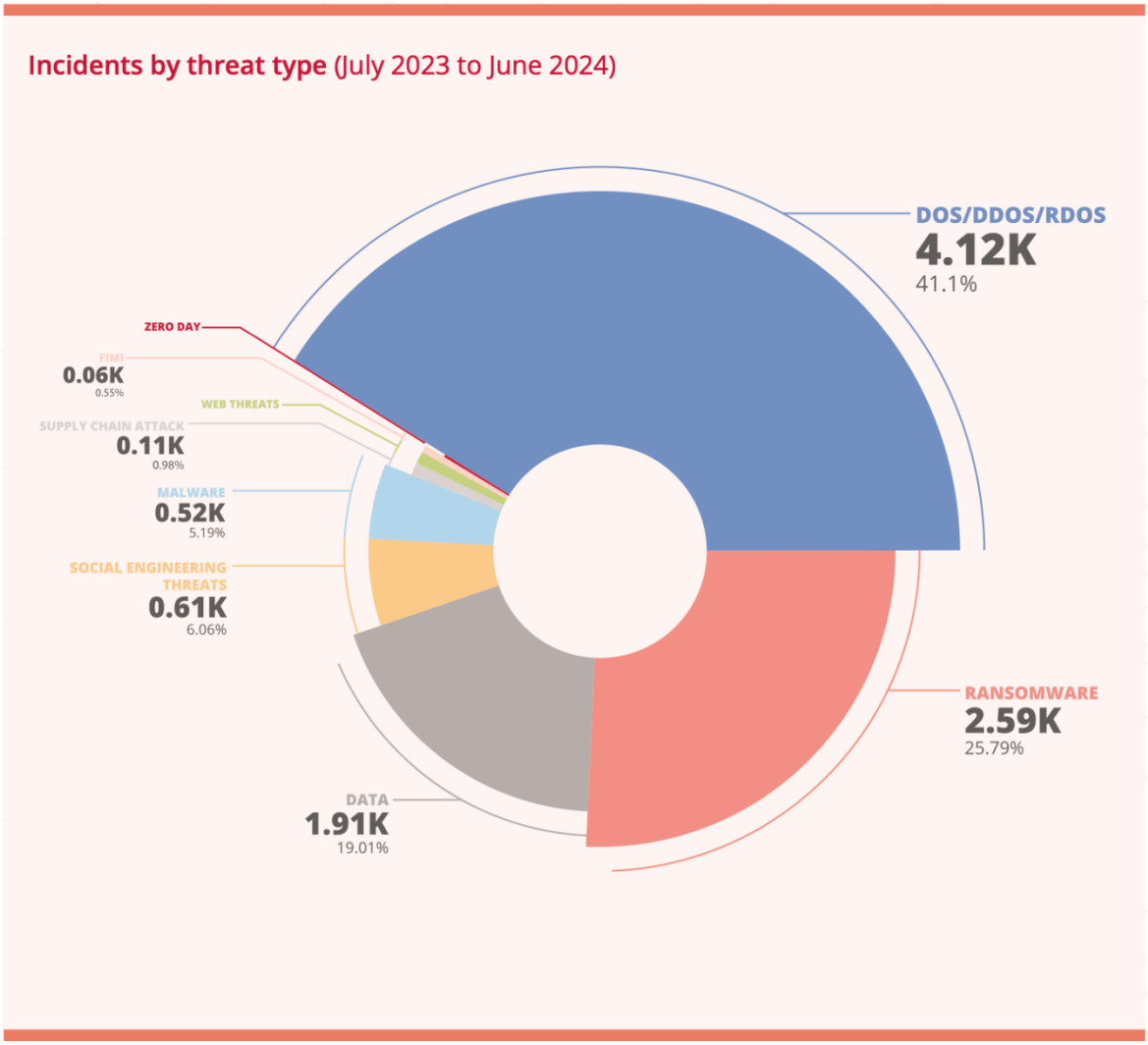


Figura 1- Incidentes de acordo com o tipo de ameaça Fonte: (ENISA, Report on the State of Cybersecurity in the Union, 2024)

Dentro destas ameaças, os setores mais afetados em 2024 no continente europeu foram o setor de administração pública e o setor dos transportes, como representado na Figura 2. Outros setores substancialmente afetados incluem a banca e o setor financeiro. (ENISA, Report on the State of Cybersecurity in the Union, 2024).

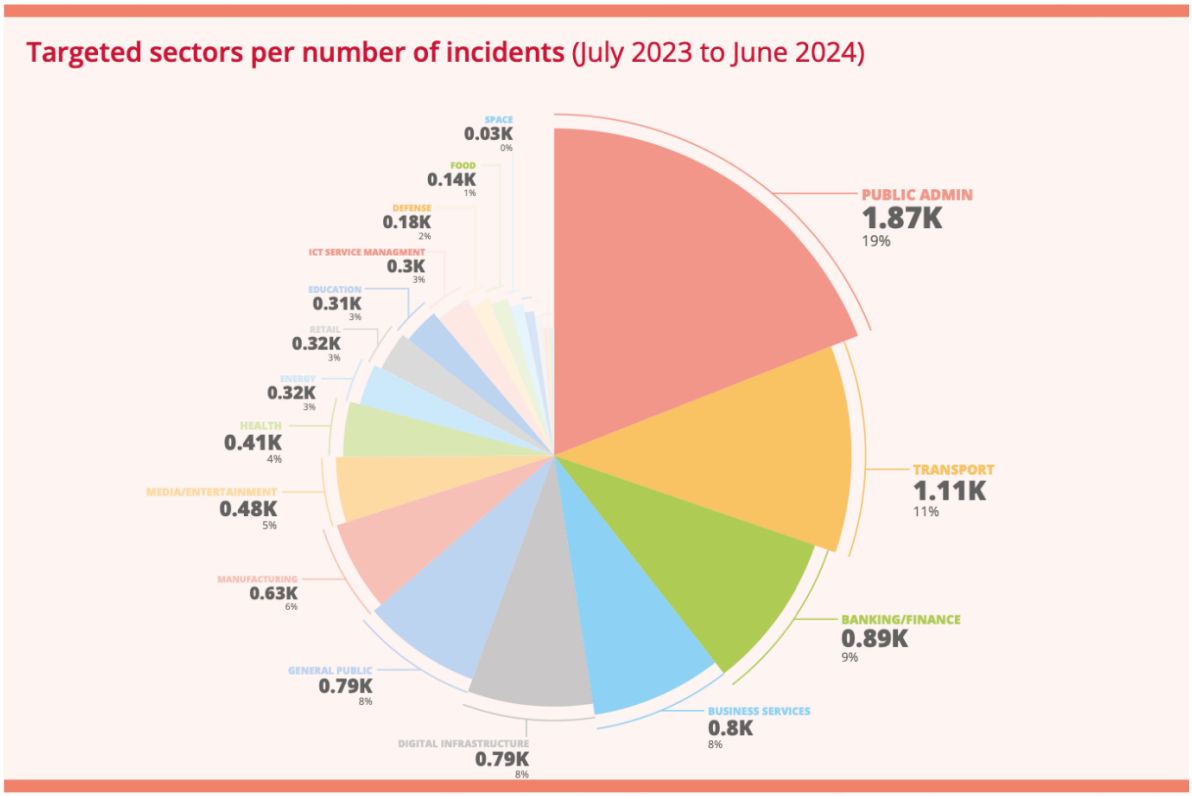


Figura 2 – Setores afetados por número de incidentes Fonte: (ENISA, Report on the State of Cybersecurity in the Union, 2024)

Além deas ameaças comuns já destacadas, o panorama atual da cibersegurança tem evidenciado uma sofisticação crescente dos ataques. Zaid e Garai (2024) identificam técnicas emergentes como ataques à cadeia de fornecimento, ameaças persistentes avançadas (APT), exploração de dispositivos IoT e *deepfakes* como desafios cada vez mais recorrentes. O caso SolarWinds, por exemplo, demonstrou como uma falha num fornecedor de software pode comprometer milhares de redes empresariais. Estas novas modalidades de ataque exploram a confiança entre entidades, bem como a engenharia social avançada, representando riscos sérios também para as PMEs. Estes autores defendem que o aumento da complexidade dos ataques exige uma reavaliação das estratégias tradicionais e o reforço da formação em cibersegurança dentro das organizações (Zaid & Garai, 2024).

Embora o foco tradicional da cibersegurança recaia sobre ameaças tecnológicas como *malware* ou ataques DDoS, é amplamente reconhecido que o comportamento dos colaboradores representa uma das principais vulnerabilidades organizacionais. De acordo com Sutton e Tompson (2025), muitos incidentes de segurança resultam da ausência de uma cultura organizacional sólida em cibersegurança. O risco aumenta quando há conflitos entre as exigências de produtividade e as práticas seguras, levando os colaboradores a contornar procedimentos para cumprirem metas operacionais. (Sutton & Tompson, 2025).

Verificamos então que os fatores comportamentais e cognitivos desempenham um papel fundamental na exposição das PMEs ao risco cibernético. Boletsis et al. (2024) identificaram que a perceção individual do risco**,** a familiaridade com o vocabulário técnico e até mesmo o nível de confiança digital dos gestores influenciam diretamente a propensão à adoção de medidas de cibersegurança. Um estudo conduzido pelos autores, baseado em entrevistas com 20 pequenas empresas no Reino Unido, demonstra que o desinteresse ou cansaço digital pode levar à rejeição ativa de soluções de segurança, mesmo quando o risco é reconhecido. Este desfasamento entre ameaça percebida e ação real contribui para a vulnerabilidade das organizações e mostra que os riscos não são apenas técnicos, mas também psicológicos e culturais (Boletsis et al., 2024).

2.4 Maturidade das PMEs e pessoal qualificado

A maturidade organizacional em cibersegurança não depende exclusivamente da existência de recursos técnicos ou humanos especializados, mas sim da integração da cibersegurança na cultura da organização. Sutton e Tompson (2025) propõem um modelo

composto por três dimensões interligadas: os valores culturais da organização, o vínculo entre esses valores e os comportamentos dos colaboradores, e os próprios comportamentos em contexto de trabalho. Através de uma revisão sistemática de 59 estudos, os autores concluem que fatores como a monitorização eficaz, o envolvimento ativo da gestão de topo, a existência de políticas realistas e o incentivo à partilha de conhecimento entre pares são essenciais para uma cultura de cibersegurança funcional. Estas práticas, contudo, são frequentemente ausentes nas PMEs, onde a informalidade organizacional e a escassez de recursos limitam a implementação sistemática de estratégias culturais de segurança (Sutton & Tompson, 2025).

De acordo com (ENISA, 2021) os maiores desafios para as PMEs são:

1. Baixo nível de conhecimento dos colaboradores
2. Falta de proteção de dados e informação sensível
3. Falta de orçamento
4. Falta de especialistas em cibersegurança nas PMEs
5. Falta de um guia para cibersegurança destinado às PMEs
6. TI sombra, ou seja, sistemas de tecnologia utilizados pelos funcionários sem a aprovação do departamento TI da PME
7. Falta de apoio por parte dos quadros superiores

Sabemos que as organizações de maior maturidade em cibersegurança estão mais bem preparadas e são mais resilientes (Deloitte, 2024). Assim, é cada vez mais importante incentivar uma cultura de cibersegurança dentro das organizações, investir em especialistas e reter talento. No entanto, as organizações têm muita dificuldade em encontrar candidatos apropriados às posições existentes (ENISA, Report on the State of Cybersecurity in the Union, 2024).

Um dos obstáculos que as PMEs enfrentam é a competição existente entre as empresas para contratar profissionais experientes em cibersegurança. Associada a esta questão está o problema dos salários destes profissionais, que são elevados e que as empresas não conseguem cobrir devido à falta de orçamento (Borgeaud, 2024).

Uma pesquisa efetuada recentemente pela *Eurobarometer*, revela que as lacunas existentes dentro da UE relativamente a postos de trabalho em cibersegurança estão a aumentar cada vez mais (ENISA&Gartner, 2024). Alguns dos principais obstáculos em contratar pessoal estão ilustrados na Figura 3.

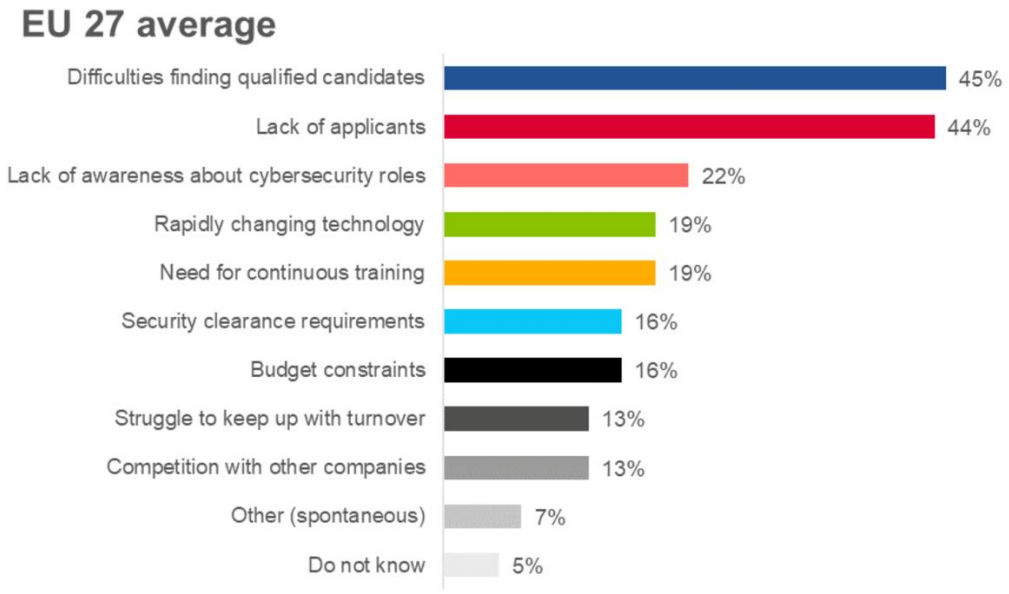


Figura 3 – Principais obstáculos em recrutar profissionais em cibersegurança Fonte: (ENISA&Gartner, 2024)

Assim, a maturidade cibernética das PMEs continua a ser condicionada pela falta de investimento em pessoal qualificado e estratégias de gestão de risco. De acordo com Ambreen et al. (2023), fatores como orçamentos reduzidos**,** ausência de equipas dedicadas de cibersegurança, e falta de sensibilização dos gestores de topo comprometem seriamente a capacidade de resposta a incidentes.

Em termos de postos de trabalho, uma das posições mais críticas em cibersegurança é a do CISO (*Chief Information Security Officer*). Este é um dos papéis mais importantes visto que os CISOs desenvolvem políticas de segurança, gerem o risco e respondem a incidentes cibernéticos. No entanto, verifica-se uma grande dificuldade por parte das empresas em colmatar esta posição (Department, Cybersecurity in Europe - statistics and facts, 2024).

Esta falta de talento é particularmente negativa nas PMEs, já que muitas admitem não ter um CISO, e que esta posição é normalmente atribuída a alguém dentro da organização que pode não possuir as competências necessárias (ENISA, Report on the State of Cybersecurity in the Union, 2024).

Para dificultar esta situação, antecipa-se que em 2025 os profissionais em cibersegurança deverão mudar de área de trabalho. Esta mudança é justificada pelos profissionais da área estarem stressados devido à falta de colegas para partilhar responsabilidade (Gartner, 2023).

Segundo um estudo elaborado por Erdogan et al. (2023), apenas 32% das PMEs inquiridas possuem cargos dedicados à cibersegurança e menos de 20% oferecem formação estruturada aos colaboradores**,** sendo esta, quando existente, geralmente limitada ao *onboarding*. Além disso, apenas 13% indicaram utilizar ferramentas para avaliação de risco, e um número ainda menor revelou identificar vulnerabilidades ou ataques de forma sistemática. Estes dados evidenciam uma maturidade organizacional reduzida, marcada pela ausência de rotinas e políticas eficazes, o que reforça a necessidade de investimento na cultura de cibersegurança e na capacitação interna das equipas**.**

A escassez de recursos humanos qualificados nas PMEs não é o único entrave à maturidade cibernética das empresas. Outra dificuldade inclui a integração de tecnologias mais avançadas. Zaid e Garai (2024) explicam que abordagens modernas como a *Zero Trust Architecture* (ZTA), o uso de inteligência artificial e *machine learning* para deteção de anomalias, e o *blockchain* para gestão de identidades exigem competências técnicas especializadas, formação contínua e uma liderança envolvida. (Zaid & Garai, 2024).

A maturidade cibernética das PMEs não pode ser avaliada apenas com base na existência de controlos técnicos ou normas implementadas, mas também na forma como os decisores se envolvem com o tema da cibersegurança (Boletsis et al., 2024). Estes autores propõem uma segmentação comportamental das pequenas empresas com base na sua disposição para agir, compreensão do risco e atitude face ao envolvimento com tecnologia.

Relativamente à liderança, sabemos que as organizações com uma liderança ativa em cibersegurança são duas vezes mais capazes de gerir o risco e responder a incidentes (ENISA, Report on the State of Cybersecurity in the Union, 2024). No entanto, verifica-se que os gerentes de topo não só têm um conhecimento limitado sobre este tema, como estão muito pouco envolvidos nas decisões de cibersegurança das suas organizações, fomentando a crença de que nunca serão alvos de um cibercrime (Arroyable, 2024).

Alguns dos problemas mais comuns estão conectados com o nível de conhecimento das equipas de gestão e o seu comprometimento em implementar padrões de segurança, que consequentemente relaciona-se com o nível de orçamento dedicado a esta área (ENISA, 2021).

Verificamos que existe um baixo nível de conhecimento nos funcionários das PMEs, representando um dos maiores desafios para estas empresas. De facto, apenas 54%

das PMEs reporta transmitir aos seus colaboradores informação acerca das suas responsabilidades perante as tecnologias de informação (ENISA, Report on the State of Cybersecurity in the Union, 2024).

De uma forma geral, o envolvimento da gestão de topo é fulcral para determinar o nível e o tipo de medidas de segurança que são implementadas na organização (ENISA, Report on the State of Cybersecurity in the Union, 2024).

Outro fator que torna o panorama ainda mais negativo é o facto de a maioria das PMEs não disporem de planos de contingência ou de recuperação e muitas não implementam sequer funções básicas do NIST *Cybersecurity Framework*, como monitorização contínua, deteção de anomalias ou avaliação de impacto. A gestão do risco cibernético nestas organizações é frequentemente intuitiva e reativa, em vez de ser sistemática e preventiva, o que perpetua a vulnerabilidade estrutural face a ameaças crescentes (Ambreen et al., 2023).

No que toca à realidade nacional, as empresas portuguesas enfrentam obstáculos em idealizar a sua maturidade cibernética pois, as limitações em recursos humanos e técnicos nas PMEs dificultam a implementação eficaz de sistemas de gestão da segurança da informação (Azinheira et. al., 2023). Verifica-se que subsiste uma lacuna significativa nesta área pois, a ausência de mecanismos de avaliação e a dificuldade em perceber quais os controlos mais relevantes acabam por limitar a maturidade organizacional em cibersegurança, perpetuando um ciclo de vulnerabilidade (Azinheira et. al., 2023).

Capítulo III – Metodologia

Esta investigação visa estudar as práticas de cibersegurança em algumas PMEs e grandes empresas portuguesas, com o objetivo de verificar quais são as semelhanças e diferenças entre estas organizações. O estudo é de carácter qualitativo para melhor compreender os comportamentos adotados pelas empresas aqui envolvidas, facilitando também alguma flexibilidade na informação recolhida durante o processo de investigação.

Para este estudo a recolha de dados foi elaborada da seguinte forma:

1. Fase 1: Análise de literatura existente sobre o tópico escolhido. Foram feitas várias pesquisas no portal SCOPUS, já que esta plataforma se evidencia pelas suas ferramentas de pesquisa avançada bem como pela facilidade em aceder a uma vasta coleção de artigos académicos. A pesquisa incluiu as seguintes combinações de palavras-chave em inglês:
    a. *Cybersecurity* + *Enterprises* + *SMEs*
    b. *Cybersecurity* + *staff awareness*
    c. *Cybersecurity* + *SMEs* + *Budgets*
    d. *Cybersecurity* + *Trends* + *SMEs*

Visto que este tema não só é extremamente recente, como está em constante mudança, a pesquisa foi limitada a artigos escritos entre 2021 e 2024. Atendendo ainda a esta característica, foram também escolhidos relatórios de cibersegurança elaborados por empresas internacionais e órgãos da União Europeia. Esta escolha prende-se pelo facto destes relatórios oferecerem uma melhor avaliação sobre as práticas de cibersegurança utilizadas em cada estado-membro. Relativamente aos artigos académicos utilizados,

estes foram escolhidos com base na sua relevância direta para o tema da cibersegurança em contexto organizacional, com ênfase nas PMEs. Outro motivo para esta escolha é a pertinência da informação face aos temas abordados nesta investigação, como as práticas de cibersegurança, as ameaças, a legislação, a maturidade organizacional e a formação dos colaboradores. Assim, ao conjugar os artigos académicos escolhidos com os relatórios pretende-se estabelecer uma comparação entre esta informação e as respostas obtidas nas entrevistas.

2. Fase 2: Entrevistas com diferentes membros de 7 PMEs e grandes empresas portuguesas. A escolha em efetuar entrevistas está ligada ao carácter qualitativo desta dissertação. Este método facilita o envolvimento do participante, garantindo acesso a *insights* mais pormenorizados e adaptados ao contexto do estudo. O guião para a elaboração das entrevistas foi construído com perguntas baseadas na informação recolhida na revisão de literatura, não obstante, os entrevistados foram encorajados a partilhar informação livremente, com a confiança de total sigilo e confidencialidade.
3. Fase 3: Análise da informação recolhida nas entrevistas estabelecendo uma comparação com a revisão de literatura.

3.2 Tratamento e análise dos dados

Durante o processo das entrevistas foram recolhidas gravações áudio que foram transcritas para texto através do Microsoft Word. Cada entrevista foi devidamente separada e catalogada. Perante a leitura das entrevistas foram salientados e recolhidos os principais tópicos. Através deste processo foi possível recolher e identificar padrões.

A análise dos dados recolhidos foi feita através do *software* MaxQDA visto que esta ferramenta é altamente reconhecida e eficaz na análise de dados qualitativos. Para facilitar a leitura dos dados recolhidos, estes foram categorizados em temas. De seguida, foram analisados de forma a delinear conclusões que contribuam para este estudo

Capítulo IV – Apresentação de Resultados

A recolha de informação para a elaboração deste estudo foi feita entre Fevereiro e Março de 2025. As questões focam-se sobretudo nas práticas de cibersegurança desenvolvidas pelas empresas. Foram entrevistadas sete pessoas com formações académicas variadas, e que desempenham diferentes funções em sete empresas portuguesas. Estas empresas atuam nos setores do retalho de luxo, engenharia e construção civil, consultoria, saúde, hotelaria, seguros e departamentos governamentais.

Os entrevistados aqui incluídos foram escolhidos tendo como base a informação identificada na Revisão de Literatura, especialmente no que toca ao *background* de cada entrevistado e como é que isso pode influenciar o seu nível de conhecimento em cibersegurança, e consequentemente a maturidade da empresa nesta área.

Os participantes foram contatados por telefone e por email, tendo recebido a devida informação acerca deste estudo, os seus objetivos e metodologia. Assim, foi pedida a participação de cada inquirido que, quando aceite, foi agendada de acordo com a disponibilidade de cada participante. Quando necessário, foram levadas a cabo mudanças de horário e designados contatos alternativos. O guião da entrevista foi providenciado atempadamente a cada participante, para que estes pudessem preparar as suas respostas antes da entrevista. As entrevistas foram feitas remotamente através do Microsoft Teams, e tiveram uma duração entre 25 e 50 minutos.

Cada entrevistado consentiu a sua participação antes da entrevista, e estas foram gravadas em formato áudio através do Microsoft Teams. Nas tabelas I e II é apresentada informação sobre cada entrevistado e sobre a respetiva entrevista.

Tabela I

Características dos entrevistados

Entrevistado	Tipo de entrevista	Duração
ENT1	Online – Microsoft Teams	52 min
ENT2	Online – Microsoft Teams	25 min
ENT3	Online – Microsoft Teams	43 min
ENT4	Online – Microsoft Teams	35 min
ENT5	Online – Microsoft Teams	50 min
ENT6	Online – Microsoft Teams	47 min
ENT7	Online – Microsoft Teams	30 min

Tabela elaborada pela autora

Tabela II

Informação sobre os entrevistados

ENT	Sexo	Formação Académica	Departamento	Cargo	Tempo exercido
ENT1	M	Licenciatura Gestão de Marketing	A	*Business Unit Manager*	5 anos
ENT2	M	Licenciatura Economia *Master in Finance*	B	Analista Financeiro	2 anos
ENT3	M	Licenciatura Eng. Multimédia	C	*OutSystems Developer*	1 ano e meio
ENT4	M	12º ano	D	Técnico Informático	19 anos
ENT5	M	12º ano	E	Técnico Informático	27 anos
ENT6	F	Mestrado em Sistemas de Informação	F	*Deputy Head of IT*	3 anos
ENT7	F	Licenciatura em Gestão Mestrado em Finanças	G	Analista de investimento	1 ano e meio

Tabela elaborada pela autora

No anexo III está incluída uma tabela que demonstra um resumo das declarações dos entrevistados em conjunto com a respetiva revisão de literatura organizada de acordo com os temas do guião da entrevista. No anexo IV está apresentado um sumário dos códigos utilizados durante o processo da análise de resultados, bem como um conjunto de explicações, a frequência com que cada participante mencionou o tópico nas entrevistas e citações dos entrevistados. O anexo V trata-se de uma visualização matrix dos códigos de cada entrevista.

Capítulo V – Resultados, Análise e Discussão

Este capítulo será dividido em três partes. A primeira parte irá compreender os aspetos relacionados com as vulnerabilidades e práticas de cibersegurança. Este primeiro ponto incluirá informação sobre quais são as práticas de cibersegurança adotadas pelas organizações estudadas, qual a legislação em vigor, e que dificuldades estas organizações sentiram em implementar estes parâmetros. A segunda parte vai abordar qual a probabilidade das PME's sofrerem um ataque cibernético e quais as suas consequências para a organização. Por último, o terceiro ponto será dedicado à maturidade da empresa e abordará aspetos relacionados com a formação dos colaboradores, contratação de pessoal dedicado, e existência de um plano estratégico para cibersegurança.

5.1 Vulnerabilidades e práticas de segurança

Todos os entrevistados reconheceram que, nos dias que correm, qualquer empresa apresenta uma vulnerabilidade universal a ataques cibernéticos, reforçando a afirmação de Pawar, 2022 e do Department, Cybersecurity in Europe - statistics and facts, 2024 quando salientam que apesar das PMEs serem de extrema importância a nível económico, carecem de medidas robustas de proteção contra ataques cibernéticos. Os participantes admitem que as organizações onde trabalham atribuem uma importância elevada à proteção contra este tipo de ataques sendo que o ENT5 e o ENT6 reforçaram que a necessidade de proteção é extrema e contínua, como explica o ENT6:

> "A empresa reconhece a cibersegurança como uma prioridade estratégica e está atualmente a desenvolver uma jornada contínua de reforço da segurança cibernética".

De forma semelhante, todos os entrevistados demonstraram consciência da importância de controlar o acesso à informação, adotando medidas de proteção como firewalls, VPN's, antivírus, formação de colaboradores, políticas de backup, testes e auditorias de segurança. Estas práticas são importantes para o ENT1 que afirma ser crucial manter o sigilo e a confidencialidade das informações sobre os seus clientes, corroborando Antunes, 2021 que sublinha ser fulcral proteger os dados como recursos estratégicos das empresas, manifestando que esta prática é essencial à integridade da organização.

Contudo, verificamos também algum desfasamento no conhecimento dos controlos de cibersegurança implementados. Os entrevistados que revelaram melhor conhecimento foram o ENT4, o ENT5 e o ENT6, pois estão inseridos nos departamentos de informação nas suas respetivas organizações. Já os restantes entrevistados revelaram noções superficiais, indicando não haver comunicação entre os seus departamentos e o departamento de IT das suas empresas, como afirma o ENT1:

> "No que toca aos controlos, não tenho muito conhecimento, pois essas questões são tratadas pelo departamento de IT e não há comunicação entre departamentos sobre isso."

Isto indica um contrassenso pois como refere Department, Cybersecurity in Europe - statistics and facts, 2024, verificamos que na EU existe uma grande preocupação

com a cibersegurança, no entanto, de acordo com Pawar, 2022, algumas PME's revelam pouco conhecimento e adoção de medidas superficiais nesta área.

Inclusive, observamos o mesmo desconhecimento no que toca à legislação e normativas adotadas pelas organizações aqui estudadas. Apesar dos avanços legislativos criados pela EU e listados pela ENISA, Report on the State of Cybersecurity in the Union, 2024 o ENT1, o ENT2 e o ENT7 desconhecem totalmente que tipo de legislação foi adotada pela organização. O ENT5 afirma mesmo que a organização não cumpre qualquer tipo de legislação. O ENT6 declarou que a empresa está atualmente a estudar a aplicabilidade das principais normas de cibersegurança. O ENT3 revela apenas ter conhecimento da implementação do regulamento RGPD, e o ENT4 é o único que afirma que a organização adotou a normativa NIS1 e que posteriormente irão implementar a NIS2.

Ainda sobre a implementação de normativas, o ENT4 e o ENT6 são os que mais informação forneceram acerca dos benefícios e dificuldades enfrentados. Ambos afirmam que o maior benefício é o aumento da resiliência da organização. No que toca às dificuldades o ENT4 afirma que:

> "A maior dificuldade em implementar estas normativas deve-se ao facto destas alterações acontecerem no decorrer do período laboral da empresa, e isso causa alguns constrangimentos na operação, sendo que por vezes é necessários realizar alguns ajustes."

A literatura confirma estes obstáculos pois Ludin, 2024 afirma que algumas legislações não são apropriadas ao âmbito operacional da organização.

5.2 Probabilidade de sofrer um ataque e tipos de ataques mais comuns

A probabilidade de sofrer um ataque é avaliada de forma contraditória pelos entrevistados. Apesar de todos acreditarem que qualquer empresa pode sofrer um ataque cibernético, apenas o ENT4, o ENT5, e o ENT6 afirmam que essa possibilidade é elevada, sendo que o ENT4 e o ENT5 revelaram sofrer tentativas diárias de *phishing*. O ENT1 declarou que no último ano a empresa sofreu um ataque de *phishing*, mas que este não causou danos significativos na estrutura da empresa, desvalorizando o acontecimento. Já o ENT2, o ENT3 e o ENT7 afirmam acreditar que a probabilidade das suas organizações sofrerem um ataque é muito reduzida. Citando o ENT2:

> "Penso que a probabilidade de isso acontecer nesta organização é muito reduzida e não acredito mesmo que alguém queira atacar-nos."

Esta afirmação corrobora Arroyable, 2024 que explica a existência da falsa ideia de que as PME's não representam um alvo a ataques informáticos.

No que toca aos tipos de ataques sofridos, o ENT6 refere que essa informação é restrita e classificada. O ENT1, como já foi mencionado, declarou que a sua organização sofreu um ataque de *phishing* no último ano. O ENT4 e o ENT5 afirmaram que apesar de não terem sofrido um ataque, são diariamente alvos de tentativas de ataques de *phishing* através do envio de links maliciosos via email. O ENT7 declarou que apesar de não ter conhecimento da sua empresa ter sofrido um ataque concreto, que recebe diariamente muitas chamadas e mensagens fraudulentas e emails de *phishing* no telefone da empresa. Estes relatos estão em conformidade com o relatório da ENISA, 2021, que salienta o uso

regular de técnicas de engenharia social, como *phishing*, para aceder a dados confidencias das organizações.

5.3 Maturidade da empresa

Um elemento revelador da maturidade cibernética de uma organização é a presença de um CISO. Quando questionados se nas suas organizações existia um CISO apenas o ENT4 e o ENT6 responderam afirmativamente, sendo que os outros participantes admitem não existir um CISO, sendo que o ENT1 e o ENT2 desconheciam totalmente essa posição. Nos casos em que não existe um CISO (ENT1, ENT2, ENT3, ENT5 e ENT7), esta posição é desempenhada pelo departamento de informática ou por algum elemento sénior do departamento de IT. Isto reflete uma realidade comum apontada na literatura, onde esta função é frequentemente inexistente ou absorvida por outros profissionais da organização (ENISA, Report on the State of Cybersecurity in the Union, 2024).

A este ponto conecta-se o fraco envolvimento dos gestores de topo nas decisões de cibersegurança. Apenas o ENT4 e o ENT6 afirmaram que os gestores de topo estão presentes nas reuniões que visam decidir as medidas de segurança da empresa. Os restantes entrevistados afirmaram não ter conhecimento, sendo que o ENT1, o ENT2 e o ENT3 revelaram não haver muita comunicação entre os seus departamentos e os departamentos de informática. Esta ausência generalizada de comunicação reflete as preocupações de Arroyable, 2024, que aponta para uma fraca participação dos líderes em decisões de cibersegurança. Outra questão evidenciada na literatura por ENISA, Report on the State of Cybersecurity in the Union, 2024 refere que apenas 54% das PME's admite providenciar informação aos seus colaboradores sobre o uso das tecnologias de

informação, o que contribui para o baixo nível de conhecimento e envolvimentos também dos colaboradores.

Outra característica da maturidade cibernética é a existência de um plano estratégico, tal como evidenciado por Deloitte, 2024, que afirma que a existência de um plano estratégico indica que a organização apresenta mais resiliência cibernética. Neste ponto, apenas o ENT4 e o ENT6 afirmaram que a sua organização possui um plano estratégico. O ENT6 referiu que esta informação é confidencial, no entanto admitiu existirem medidas corretivas e procedimentos de resposta para mitigar e minimizar os impactos de eventuais ataques. O ENT1, o ENT2, o ENT3 e o ENT7 revelaram não ter qualquer conhecimento da existência de um plano estratégico, mas acreditam que ele existe, como explica o ENT3:

> "Não posso precisar com certeza se a organização tem um plano atualmente, mas lembro-me que já foi mencionado. Existem algumas questões relacionadas com a segurança que não foram comunicadas. Por exemplo, apenas disseram-me para informar o meu superior caso aconteça algo."

Já o ENT5 afirmou categoricamente que a organização não possui qualquer tipo de plano estratégico.

Por fim, o último indicador de maturidade a abordar é a formação dos colaboradores. O ENT1 afirmou que a empresa não fornece formação em cibersegurança aos seus colaboradores, e o ENT5 transmitiu que em 10 anos recebeu apenas uma formação em *Blueteam*. Estes dados confirmam o Department, Cybersecurity in Europe - statistics and facts, 2024 que informa que, no ano passado, 74% das empresas europeias

não forneceram qualquer tipo de formação aos seus colaboradores. Todos os outros entrevistados declararam receber formações na área, que são efetuadas de forma *online,* nas plataformas internas de cada organização, e que esta consiste em vídeos explicativos e questionários. Sobre a frequência com que esta formação é dada, o ENT2, o ENT3, o ENT4 e o ENT7 afirmaram que ela acontece entre uma a duas vezes por ano, e o ENT6 admitiu ter formações todas as semanas, afirmando que:

> "Estas formações acontecem todas as semanas para garantir que os colaboradores são continuamente atualizados. No entanto, admito que há dificuldade em aumentar a maturidade organizacional, pois isto envolve a criação de uma cultura de segurança digital em **todos** os colaboradores."

Capítulo VI – Conclusões, Limitações e Futuras Investigações

A presente investigação permitiu aprofundar a compreensão sobre o estado atual da cibersegurança nas empresas portuguesas, com ênfase nas Pequenas e Médias Empresas (PMEs). Através da análise qualitativa de entrevistas realizadas a profissionais de diferentes setores, foi possível responder às perguntas de investigação propostas para esta dissertação. Em resposta à pergunta "Quais são as medidas de cibersegurança mais adotadas pelas empresas portuguesas" constatou-se que estas são as seguintes:

- Utilização de *firewalls*, antivírus e VPNs;
- Políticas de *backup* e recuperação de dados;
- Controlo de acessos e senhas encriptadas;
- Filtragem de emails e restrição de acessos Web;
- Auditorias de segurança e testes de engenharia social (como simulações de phishing);
- Formação (em alguns casos) dos colaboradores.

Estas medidas demonstram um esforço crescente por parte das empresas para proteger os seus ativos digitais, embora seja possível notar uma disparidade entre empresas com maior maturidade cibernética e outras com práticas ainda muito básicas.

Já para a pergunta "Quais são as ameaças de cibersegurança mais comuns dentro destas organizações?" estas incluem:

- Ataques *phishing*, através de emails e chamadas fraudulentas, sendo relatado como tentativa quase diária por algumas organizações;
- Tentativas de acesso não autorizado e links maliciosos;
- Referências indiretas a outras ameaças como *ransomware* e DoS/DDoS, com base na literatura, embora menos reconhecidas diretamente pelos entrevistados.

No entanto, a percepção do risco variou significativamente entre os participantes — algumas empresas demonstraram subvalorização clara da ameaça.

Apesar dos resultados relevantes, este estudo apresenta algumas limitações. A primeira limitação a salientar é o tamanho reduzido da amostra. Foram realizadas apenas sete entrevistas, o que pode limitar a representatividade dos dados. A segunda limitação é a utilização do método qualitativo. Embora este método seja adequado ao tema, impede generalizações estatísticas. Outra limitação é a desigualdade no conhecimento dos entrevistados. Apesar do propósito ser entrevistar pessoas de diferentes departamentos e com variados *backgrounds,* esta característica do estudo pode representar uma limitação visto que alguns participantes demonstraram pouca ou nenhuma familiaridade com a política de cibersegurança da sua empresa, o que pode enviesar as respostas. Por último, o facto do estudo focar-se exclusivamente no contexto português, não permite comparações diretas com outras realidades internacionais.

Como forma de expandir os resultados e conhecimento adquirido com esta pesquisa, e dada a relevância crescente da cibersegurança, sugerem-se diferentes linhas de investigação. Para começar propõe-se estudos quantitativos com amostras alargadas para generalizar resultados. Também é possível efectuar análises comparativas entre diferentes setores de atividade, como por exemplo, saúde, finanças, ou instituições governamentais. É igualmente admissivel investigar a cultura organizacional da empresa e o papel da liderança na adoção de boas práticas de cibersegurança. Outro tópico de pesquisa é a avaliação do impacto económico de ciberataques nas PMEs. Por último, propõe-se que se elaborem estudos que acompanhem a evolução da maturidade cibernética das empresas ao longo do tempo.

Em suma, esta dissertação evidencia que, embora se verifique uma crescente consciencialização sobre a importância da cibersegurança nas empresas portuguesas, ainda existem lacunas significativas tanto ao nível da formação dos colaboradores como na adoção de estratégias estruturadas e liderança dedicada. O principal desafio continua a ser a promoção de uma cultura de segurança digital transversal.

Referências

1. Allianz. (2023). Identifying the major business risks for 2024.

2. Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. Journal of Cybersecurity and Privacy, 1(2), 219–238. https://doi.org/10.3390/jcp1020012

3. Arroyabe, M. F., Arranz, C. F. A., Fernandez De Arroyabe, I., & Fernandez de Arroyabe, J. C. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. Technology in Society, 78, 102670. https://doi.org/10.1016/j.techsoc.2024.102670

4. Azinheira, B., Antunes, M., Maximiano, M., & Gomes, R. (2023). A methodology for mapping cybersecurity standards into governance guidelines for SME in Portugal. Procedia Computer Science, 219, 121–128. https://doi.org/10.1016/j.procs.2023.01.272Barikat. (2025).

5. Barikat Cybersecurity. Retrieved from ASMA know your assets: https://www.barikat.com.tr/en/rd/asma

6. Boletsis, C., Halvorsrud, R., Pickering, J. B., Phillips, S. C., & Surridge, M. (2024). One size does not fit all: Exploring the cybersecurity perspectives and engagement preferences of UK-based small businesses. Computers & Security, 133, 103531. https://doi.org/10.1016/j.cose.2024.103531

7. Borgeaud, A. (2024, Agosto 7). Business cybersecurity in the United Kingdom - Statistics and facts. Retrieved from Statista: https://www.statista.com/topics/8437/business-cyber-security-in-the-uk/#topicOverview

8. CIS. (2025). Center for Internet Security. Retrieved from CIS Critical Security Controls: https://www.cisecurity.org/controls

9. Clarissa, S., & Wang, G. (2023). Assessing information security management using ISO 27001:2013. Jurnal Indonesia Sosial Teknologi, 4(9), 1361–1371. https://doi.org/10.59141/jist.v4i9.739

10. CNCS. (2024, Outubro 4). Directiva NIS2. Retrieved from Centro Nacional de CIbersegurança em Portugal: https://www.cncs.gov.pt/pt/diretiva-sri-2-nis-2/#collapse1One

11. Deloitte. (2024). The Global Future of Cyber Survey, 4th Edition - The Promise of Cyber. Deloitte

12. Department, S. R. (2024, Novembro 27). Cybersecurity in Europe - statistics and facts. Retrieved from Statista: https://www.statista.com/topics/12924/cybersecurity-in-europe/#topicOverview

13. Department, S. R. (2024, Novembro 27). EU Cyber Resilience Act - Statistics and Facts. Retrieved from Statista: https://www.statista.com/topics/12973/eu-cyber-resilience-act/#topicOverview

14. DORA. (n.d.). The Digital Operational Resilience Act (DORA) - Regulation (EU) 2022/2554. Retrieved from Digital Operational Resilience Act: https://www.digital-operational-resilience-act.com/

15. EHDS. (n.d.). The European Health Data Space (EHDS). Retrieved from EHDS: https://www.european-health-data-space.com/

16. ENISA. (2021). ENISA.

17. ENISA. (2024). Report on the State of Cybersecurity in the Union.

18. ENISA&Gartner. (2024). NIS Investments 2024 Cybersecurity Policy Assessment

19. Erdogan, G., Halvorsrud, R., Boletsis, C., Tverdal, S., & Pickering, J. B. (2023). Cybersecurity awareness and capacities of SMEs. In Proceedings of the 9th International Conference on Information Systems Security and Privacy (ICISSP 2023) (pp. 296–304). https://doi.org/10.5220/0011609600003405

20. Espinosa, C. (2024, Setembro 18). Number of SMEs in the EU from 2008 to 2024. Retrieved from Statista: https://www.statista.com/topics/8231/smes-in-europe/#topicOverview

21. EU, C. o. (2024, Dezembro 2). Cybersecurity package: Council adopts new laws to strengthen cybersecurity capacities in the EU. Retrieved from European Council: https://www.consilium.europa.eu/en/press/press-releases/2024/12/02/cybersecurity-package-council-adopts-new-laws-to-strengthen-cybersecurity-capacities-in-the-eu/

22. Gartner. (2023). Gartner. Retrieved from Gartner Press Release: https://www.gartner.com/en/newsroom/press-releases/2023-03-28-gartner-unveils-top-8-cybersecurity-predictions-for-2023-2024

23. IBM. (2024). Threat Intelligence Index.

24. ISO27001. (2022). ISO. Retrieved from ISO/IEC 27001:2022: https://www.iso.org/standard/27001

25. ISO27002. (2022). ISO. Retrieved from What is ISO/IEC 27002?: https://www.iso.org/standard/75652.html

26. ITGovernance. (n.d.). ITGovernance. Retrieved from Guide to the NIST CSF (Cybersecurity Framework): https://www.itgovernanceusa.com/nist-cybersecurity-framework

27. Ludin, W. N. E. W. M., Mohd, M., & Paizi@Fauzi, W. F. (2024). Comparative analysis of small and medium-sized enterprises cybersecurity program assessment model. International Journal of Advanced Computer Science and Applications, 15(8), 796–804. https://doi.org/10.14569/IJACSA.2024.0150889

28. Manzoor, J., Waleed, A., Jamali, A. F., & Masood, A. (2024). Cybersecurity on a budget: Evaluating security and performance of open-source SIEM solutions for SMEs. PLoS ONE, 19(3), e0301183. https://doi.org/10.1371/journal.pone.0301183

29. NIST. (2024). The NIST Cybersecurity Framework.

30. Pawar, S., & Palivela, H. (2022). LCCI: A framework for least cybersecurity controls to be implemented for small and medium enterprises (SMEs). International Journal of Information Management Data Insights, 2(1), 100080. https://doi.org/10.1016/j.jjimei.2022.100080

31. Petrosyan, A. (2024, Abril 22). Annual number of malware attacks worldwide from 2015 to 2023 in billions. Retrieved from Statista: https://www.statista.com/statistics/873097/malware-attacks-per-year-worldwide/

32. Petrosyan, A. (2024, Abril 23). Annual number of ransomware attempts worldwide from 2017 to 2023 (in millions). Retrieved from Statista: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

33. Petrosyan, A. (2024, Novembro 19). Ransomware - statiscs and facts. Retrieved from Statista: https://www.statista.com/topics/4136/ransomware/#topicOverview

34. Petrosyan, A. (2024, Novembro 9). Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023. Retrieved from Statista: https://www.statista.com/statistics/204457/businesses-ransomware-attack-rate/

35. SONICWALL. (2024). Sonicwall 2024 Cyberthreat Report.

36. Sutton, A., & Tompson, L. (2025). Towards a cybersecurity culture-behaviour framework: A rapid evidence review, Computers & Security, 148, 104110. https://doi.org/10.1016/j.cose.2024.104110

37. Zaid, T., & Garai, S. (2024). Emerging trends in cybersecurity: A holistic view on current threats, assessing solutions, and pioneering new frontiers. Blockchain in Healthcare Today, 7, Article 302. https://doi.org/10.30953/bhty.v7.302

Anexos

Anexo I – Práticas de Cibersegurança

Tema	Revisão de Literatura	Autores	Questão
Vulnerabilidade das PMEs	As PMEs estão mais susceptíveis a sofrerem ataques cibernéticos.	Pawar (2022)	Qual a importância que a sua empresa atribui à protecção contra-ataques cibernéticos?
Protecção de dados e sistemas	A cibersegurança é uma ferramenta importante na protecção de dados e sistemas de informação de uma empresa.	Arroyable (2024), Antunes (2021)	Quais são as práticas de cibersegurança implementadas na sua empresa, para proteger os sistemas de informação?
Controlos de cibersegurança	Existe uma falta de controlos nas PMEs europeias, e quando estes são implementados, são implementados de forma superficial.	Pawar (2022)	Que tipo de controlos de cibersegurança foram adotados na sua empresa, e como é que foram implementados?
Diretivas e legislação	Verificamos no espaço europeu a recente criação e implemenrtação de legislação para cibersegurança.	ENISA, Report on the State of Cybersecurity in the Union (2024)	Que tipo de diretiva ou legislação para a cibersegurança foi adotada pela sua empresa?
Dificuldades associadas à implementação de legislação	Algumas PMEs demonstram dificuldade em implementar algumas diretivas, por variados motivos.	Ludin (2024)	Quais os benefícios e dificuldades verificados na implementação dessa diretiva?
Probabilidade de uma PME sofrer um ataque de cibersegurança	Mito de que as PMEs estão menos susceptíveis a sofrerem ataques de cibersegurança.	Arroyable (2024)	Acredita que a sua empresa pode ser alvo de um ataque cibernético? OU Na sua opinião qual a probabilidade da sua empresa sofrer um ataque cibernético?

Consequências dos ataques cibernéticos	As empresas que sofrem ataques cibernéticos tendem a fechar 6 meses após o ataque, bem como podem sofrer danos financeiros e reputacionais.	Pawar (2022), Petrosyan, Ransomware - statiscs and facts (2024)	No último ano a sua empresa sofreu algum ataque cibernético? Se sim, quais foram as principais consequências?
Tipos de ataques cibernéticos	Os principais tipos de ataques cibernéticos às empresas europeias incluem ataques DdoS e Rasomware.	ENISA, Report on the State of Cybersecurity in the Union (2024)	Caso a sua empresa tenha sofrido um ataque de cibersegurança, especifique esse ataque. OU Contra que tipo de ataques está a sua empresa protegida?
Dificuldade em implementar práticas de cibersegurança	As PMEs são as empresas que mais dificuldade reportam ter em implementar medidas de cibersegurança, sobretudo no que toca a contratar pessoal qualificado nesta área.	ENISA, Cybersecurity for SMEs - Challenges and Recommendations (2021)	No que toca à implementação de práticas de cibersegurança, quais são as maiores dificuldades para a sua empresa?
Contratação de um CISO	Uma das posições mais difíceis de recrutar nesta área é a do CISO.	Department, Cybersecurity in Europe - statistics and facts (2024), ENISA, Report on the State of Cybersecurity in the Union (2024)	Na sua empresa existe um CISO? Se não, quem é que desempenha ou assume esse papel?
Envolvimento dos gestores de topo	Quanto mais envolvidos estão os gestores de topo nas decisões de cibersegurança da empresa, melhor é o desempenho da mesma	ENISA, Report on the State of Cybersecurity in the Union (2024), Arroyable (2024)	Quão envolvidos estão os gestores de topo da sua empresa nas decisões de cibersegurança?
Maturidade da empresa	Empresas com maior maturidade em cibersegurança são capazes de monitorizar e gerir o risco associado	Deloitte (2024)	A sua empresa possui um plano estratégico para monitorizar e minimizar os danos associados aos ataques cibernéticos?
Formação de colaboradores	Para que uma empresa seja resiliente é necessário cultivar o conhecimento em cibersegurança dentro da empresa	Department, Cybersecurity in Europe - statistics and facts (2024),	A sua empresa fornece algum tipo de formação em cibersegurança? Se sim, que tipo de formação e com

			que frequência isso acontece? E a quais colaboradores?
Conhecimento dos colaboradores	Verifica-se que nas PMEs, os colaboradores têm um baixo nível de conhecimento em cibersegurança.	ENISA, Report on the State of Cybersecurity in the Union (2024)	De 0 a 5 como classifica o seu conhecimento em cibersegurança? 0 = Nenhum conhecimento 1 = Muito pouco conhecimento 2 = Pouco conhecimento 3 = Neutro 4 = Algum conhecimento 5 = Muito conhecimento

Anexo II – Guião da Entrevista

I. Apresentação

a. Apresentação pessoal
b. Informação sobre o propósito da entrevista
c. Estrutura da pesquisa
d. Consentimento do entrevistado em conceder a entrevista e em que esta seja gravada e utilizada
e. Garantia de confidencialidade

II. Questões básicas sobre o entrevistado

a. Sexo
b. Qual é a sua formação académica?
c. Que cargo ocupa neste momento na sua atual empresa?
d. Há quanto tempo ocupa esse cargo e há quanto tempo está na sua atual empresa?

III. Cibersegurança

a. Qual a importância que a sua empresa atribui à proteção contra-ataques cibernéticos?
b. Quais são as práticas de cibersegurança implementadas na sua empresa, para proteger os sistemas de informação?
c. Que tipo de controlos de cibersegurança foram adotados na sua empresa, e como é que foram implementados?
d. Que tipo de diretiva ou legislação para a cibersegurança foi adotada pela sua empresa?
e. Quais os benefícios e dificuldades verificados na implementação dessa diretiva?
f. Acredita que a sua empresa pode ser alvo de um ataque cibernético? OU Na sua opinião qual a probabilidade da sua empresa sofrer um ataque cibernético?
g. No último ano a sua empresa sofreu algum ataque cibernético? Se sim, quais foram as principais consequências?

h. Caso a sua empresa tenha sofrido um ataque de cibersegurança, especifique esse ataque. OU Contra que tipo de ataques está a sua empresa protegida?
i. No que toca à implementação de práticas de cibersegurança, quais são as maiores dificuldades para a sua empresa?
j. Na sua empresa existe um CISO? Se não, quem é que desempenha ou assume esse papel?
k. Quão envolvidos estão os gestores de topo da sua empresa nas decisões de cibersegurança?
l. A sua empresa possui um plano estratégico para monitorizar e minimizar os danos associados aos ataques cibernéticos?
m. A sua empresa fornece algum tipo de formação em cibersegurança? Se sim, que tipo de formação e com que frequência isso acontece?
n. De 0 a 5 como classifica o seu conhecimento em cibersegurança?
   0 = Nenhum conhecimento
   1 = Muito pouco conhecimento
   2 = Pouco conhecimento
   3 = Neutro
   4 = Algum conhecimento
   5 = Muito conhecimento

IV. Conclusão

a. Considerações gerais sobre a entrevista
b. Agradecimento pelo tempo concedido e participação na entrevista

Anexo III – Sumário da entrevista

Guião	Declaração da entrevista	Revisão de Literatura
Vulnerabilidades das PME's	Todos os entrevistados reconheceram que no panorama atual qualquer empresa pode ser alvo de um ataque cibernético. Os participantes reforçaram que as empresas para as quais trabalham atribuem elevada importância à proteção contra este tipo de ataques.	Apesar das PME's serem as maiores contribuidoras para a economia mundial, estas são as que mais vulnerabilidades apresentam a ataques cibernéticos (Pawar, 2022). Desta forma, existe uma elevada necessidade em proteger os ativos digitais das organizações (Department, Cybersecurity in Europe - statistics and facts, 2024).
Proteção de dados e sistemas	Os participantes apontaram particular relevância ao controlo de informação, e ao tipo de informação a que cada colaborador da empresa tem acesso. Enumeraram ainda filtragem de emails, *firewalls*, restrição de acesso *Web*, bem como de aplicações nos computadores, antivírus, passwords alfanuméricas, VPN, gestão de incidentes, testes de auditoria e segurança, formação de colaboradores, gestão de incidentes, monitorização e deteção de ameaças, política de *backup* e recuperação.	Hoje em dia as empresas reconhecem que os dados de informação são um dos seus recursos mais importantes, e por esse motivo é essencial zelar pela integridade desses recursos através de práticas de segurança. (Antunes, 2021)
Controlos de cibersegurança	A maior parte dos entrevistados afirmou não ter conhecimento sobre o tipo de controlos adotados pelas suas respetivas empresas.	Apesar da maioria dos Estados-Membros da EU admitir que a preocupação com a cibersegurança é de alta prioridade

	Alguns chegam a afirmar que este tipo de informação mão é facultada pelos seus departamentos de IT. Não obstante, um dos participantes declarou que a sua empresa possui controlos preventivos, detetivos e corretivos.	(Department, Cybersecurity in Europe - statistics and facts, 2024) as PME's revelam ter uma falta de controlos de cibersegurança, ou apenas adotam controlos superficiais (Pawar, 2022).
Diretivas e Legislação	À semelhança do tópico anterior, muitos entrevistados desconhecem que tipo de legislação foi adotada pela empresa. Os entrevistados que afirmam ter esse conhecimento realçaram a legislação RGPD, e NIS 1, visando também implementar a NIS 2.	Para garantir práticas de cibersegurança dentro do continente europeu, surgiram nos últimos anos diferentes legislações que visam regular as PME's (ENISA, Report on the State of Cybersecurity in the Union, 2024). Existem ainda uma série de condutas de boas práticas para as PME's que visam salvaguardar a sua segurança digital (ENISA, 2021).
Dificuldades associadas em implementar legislação	Uma grande dificuldade salientada é o transtorno causado pela implementação de legislação, visto que essas mudanças ocorrem durante o período laboral normal, o que causa alguns constrangimentos na operação. Outra dificuldade passa por promover a mudança cultural da empresa em adotar novas perspetivas de cibersegurança. No entanto, o maior benefício é o aumento da capacidade e resiliência cibernética da organização.	As implementações de algumas normativas podem representar obstáculos às PME's, como por exemplo a exigência de investimento financeiro elevado, ou o facto de algumas normas não serem apropriadas ao âmbito operacional da organização, necessitando serem adaptadas à PME em questão (Ludin, 2024).
Probabilidade da PME sofrer um ataque	Todos os entrevistados admitem haver essa probabilidade, mas alguns acreditam que a probabilidade é baixa, sendo que um deles afirma não acreditar que algum organismo	Em 2023 a CISA reportou que as PME's estão cinco vezes mais suscetíveis de serem atacadas do que as grandes empresas (SONICWALL, 2024). Apesar desta

	queira atacar a empresa onde trabalha. Já noutros casos, os participantes declararam que as suas empresas sofrem tentativas de ataques diariamente.	suscetibilidade, muitas pessoas ainda acreditam que devido às características e dimensão da organização, esta não será atacada. (Arroyable, 2024)
Consequências dos ataques cibernéticos	A maioria dos entrevistados afirma que as suas empresas não sofreram ataques cibernéticos. Um deles declarou ter sofrido um ataque que não gerou grandes consequências. Outro participante afirmou que a informação sobre incidentes é classificada e restrita, não obstante, admite que os ataques cibernéticos são uma realidade constante para as empresas.	Um ciberataque pode representar grandes perdas para uma organização, incluindo a cessação do negócio (Pawar, 2022). Outras consequências incluem danos financeiros e reputacionais. (Petrosyan, Ransomware - statiscs and facts, 2024)
Tipos de ataques	Os exemplos mais regulares que foram fornecidos são os ataques de *phishing* via email. Um dos entrevistados declarou receber muitas chamadas e mensagens fraudulentas no telefone da empresa.	Em 2023, 72% das empresas mundiais foi vítima de ataques ransomware (Petrosyan, Annual share of organizations affected by ransomware attacks worldwide from 2018 to 2023, 2024). O relatório da (ENISA, Report on the State of Cybersecurity in the Union, 2024) destaca ainda um aumento nos ataques DoS/DDoS/RDoS, e o uso contínuo de ataques *phishing* via email, que visam obter informação confidencial das vítimas.
Dificuldades em implementar práticas de cibersegurança	Todos os entrevistados afirmam que a maior dificuldade é providenciar formação aos seus colaboradores e fazer com que os mesmos sigam os cuidados necessários, criando uma cultura de segurança digital.	Alguns dos maiores desafios que as PME's encontram incluem o baixo nível de conhecimento dos colaboradores, bem como a falta de especialistas em cibersegurança dentro das PME's (ENISA, 2021).
Contratação de um CISO	Das sete entrevistas efetuadas apenas dois responderam afirmativamente. Os restantes	Uma das posições mais difíceis de preencher nesta área, é a posição do CISO

	entrevistados declararam que essa posição é efetuada pelo departamento de IT, sendo que muitos desconhecem quem é a pessoa encarregue dessa função, uma vez que não interagem com o departamento de IT.	(Department, Cybersecurity in Europe - statistics and facts, 2024). Esta contratação é tão difícil, que muitas PME's admitem não ter um CISO, sendo que esta posição é absorvida por outra pessoa dentro da empresa (ENISA, Report on the State of Cybersecurity in the Union, 2024).
Envolvimentos dos gestores de topo	A maior parte dos entrevistados não sabe responder a esta pergunta, mas afirmam acreditar que existe envolvimento dos gestores de topo nas questões de cibersegurança. Dois dos participantes afirmaram que a gestão de topo está envolvida em todas as reuniões com os departamentos de segurança e informação.	As organizações que demonstram ter maior capacidade para gerir o risco e responder a incidentes são aquelas com uma liderança ativa (ENISA, Report on the State of Cybersecurity in the Union, 2024). No entanto, muitos gestores de topo estão pouco envolvidos nas decisões de cibersegurança das suas organizações (Arroyable, 2024).
Plano estratégico para cibersegurança	Muitos dos entrevistados acreditam que a empresa possui um plano estratégico, mas afirmam que essa informação não é transmitida aos seus departamentos. Um participante afirma que a organização não possui plano estratégico. Dois participantes afirmam que a empresa possui plano estratégico, sendo que uma delas informou que esse plano é restrito e confidencial.	Uma empresa que possui um plano estratégico em cibersegurança demonstra ter uma maturidade maior nesta área, o que representa mais resiliência e capacidade de monitorizar os riscos cibernéticos, bem como de mitigá-los (Deloitte, 2024).
Formação dos colaboradores	Um dos participantes afirmou que a empresa não faculta formação nesta área. Outro participante declarou que em 10 anos recebeu uma formação. Ainda noutro caso, o entrevistado afirmou que a empresa faculta formação semanal aos colaboradores. Os	Em 2024, 74% das empresas europeias declararam que não providenciam qualquer tipo de formação nesta área aos seus colaboradores (Department, Cybersecurity in Europe - statistics and facts, 2024).

	restantes quatros declararam que a formação é feita *online* na plataforma interna da empresa através de vídeos explicativos e questionários.	
Auto-avaliação	Classificação dos participantes: 0 – Nenhum participante 1 – Um participante 2 – Um participante 3 – Nenhum participante 4 – Quatro participantes 5 – Um participante	Apenas 54% das PME's admite providenciar aos seus colaboradores informação sobre as suas responsabilidades perante as tecnologias de informação, o que contribui para o baixo nível de conhecimentos dos colaboradores (ENISA, Report on the State of Cybersecurity in the Union, 2024).

Anexo IV – Códigos e Subcódigos derivados das entrevistas

Código	Notas	Frequência	Citações dos participantes
P1. Nível de importância atribuída à cibersegurança			
Muito importante	Perceber que nível de importância é que cada organização atribiu à cibersegurança e se isso se reflete nas ações de proteção contra ataques.	7	A empresa reconhece a cibersegurança como uma prioridade estratégica e está atualmente a desenvolver uma jornada contínua de reforço da segurança cibernética. (ENT6)
P2. Práticas de cibersegurança em vigor			
Filtragem de emails	Garantir que os emails recebidos não contêm links maliciosos	2	O departamento de informática faz filtragem de emails e é ativo em informar quando há recebimento de algum tipo de *malware*. (ENT1)
Cuidados na utilização dos computadores	Práticas seguras de utilização de computadores por parte dos funcionários	1	Tentamos instruir as pessoas de como devem utilizar o material para evitar acessos exteriores. (ENT4)
Formação de colaboradores	Informar todos os colaboradores das práticas de segurança e fazer com que estes cumpram com a regulamentação	1	Damos formação a todos os colaboradores para que saibam que cuidados devem ter no tratamento da informação. (ENT6)
Políticas de backup e recuperação	Armazenamento de dados para segurança e recuperação em caso de ataque informático	1	

Atualização de patches	Aplicação de correções de *software* para corrigir possíveis vulnerabilidades no sistema	1	
Deteção de ameaças	Medidas preventivas para detetar ameaças atempadamente	1	Fazemos monitorização contínua e auditorias de segurança para identificar atividades suspeitas. (ENT6)
Two Factor Authentication	Utilização de dois métodos de autenticação para aceder às contas dos funcionários e sistemas	2	
Passwords encriptadas	Garantir que os funcionários sabem como escolher uma password forte	3	Existe algum cuidado do departamento informático em educar as pessoas de como devem criar uma password forte, e tentar não repetir a mesma password para mais do que um acesso aos sistemas. (ENT3)
Proteção de dados	Utilização de sistemas de proteção de dados	1	Também tentamos segregar o acesso de cada funcionário aos sistemas para melhor proteger os dados. Ou seja, as pessoas só têm acesso aos dados que necessitam aceder para o desempenho da sua função. (ENT3)
Firewall	Instalação e uso de *firewalls* para proteção dos dados dos dados e sistemas	5	
Anti-vírus	Instalação e uso de anti-vírus dos dados e sistemas	3	

P.3 Controlos de cibersegurança			
Preventivos, Detetivos e Corretivos	Aplicação de controlos por etapas diferentes visando coesão na segurança	1	O objetivo foi adotar controlos de segurança em três frentes para garantir que a segurança é contínua. (ENT6)
Restrições WEB e de aplicações	Proibição no uso de alguns *websites*, ou instalação de aplicações nos computadores da organização	1	São feitas restrições específicas para garantir que os funcionários usam o material de forma correta e segura. (ENT5)
Auditorias	Avaliação dos sistemas de segurança da organização para identificar riscos	1	Monitorização contínua e auditorias de segurança para identificar atividades suspeitas. (ENT6)
Sem conhecimento	Não sabem especificar	1	
VPN	Utilização de uma rede virtual privada para encriptar dados e proteger os utilizadores	2	Tanto os funcionários da empresa como os nossos clientes utilizam uma VPN. (ENT3)
Testes de segurança	Conjunto de diferentes testes efetuados para averiguar quais são as vulnerabilidades do sistema	2	São enviados emails falsos que funcionam como uma armadilha para averiguar quem é que cai na mesma. Se algum funcionário falhar, é sugerido que faça uma formação. (ENT2)
P.4 Legislação e Diretivas			
Não adotámos	Sem qualquer tipo de diretiva em vigor	1	Não adotámos nenhuma legislação. (ENT5)
NIS 1	Diretiva europeia para a cibersegurança que visa aumentar a resiliências das organizações	1	Temos implementada a NIS1 e de futuro iremos também implementar a NIS2. (ENT4)

A preparar implementação		1	Estamos de momento a estudar a implementação de legislação. (ENT6)
GDPR	Lei de proteção de dados	1	
Não sabe	Falta de comunicação entre departamentos resulta em falta de informação geral	3	Não tenho qualquer tipo de conhecimento sobre a adoção de legislação, e essas questões raramente são comunicadas a outros departamentos. (ENT7)
P.5 Dificuldades em diretivas			
Constrangimentos na operação	A adoção de algumas diretivas pode causar constrangimentos no decorrer do dia de trabalho dos funcionários	1	Estas alterações causam diversos constrangimentos no decorrer da operação, pois as mudanças ocorrem durante o período laboral. (ENT4)
Não sei responder	Falta de comunicação entre departamentos manifesta falta de informação pelos funcionários	2	
Novas certificações para o pessoal	Com a adoção de novas diretivas, pode ser necessário providenciar novas formações na área aos colaboradores	1	Por vezes é difícil facultar novas formações, ou providenciar novas certificações aos colaboradores para que estejam aptos a entender as novas diretivas. (ENT3)
Dificuldade em contratar pessoal	Pode verificar-se alguma dificuldade em contratar pessoal apto para lidar com as novas diretivas adotadas	1	
Ações dos colaboradores	Problemas em fazer com que os funcionários retenham	2	Uma das maiores dificuldades é consciencializar os

	informação sobre as novas diretivas e consigam cumprir com novos parâmetros de segurança		colaboradores da importância da segurança cibernética. (ENT6)
P.6 Probabilidade de sofrer um ataque			
Elevada	Consideração de que a probabilidade é elevada	4	A probabilidade é elevada, e somos alvo de tentativas de ataque quase todos os dias. (ENT4)
Baixa	Consideração de que probabilidade é baixa	3	Creio que a probabilidade de sermos atacados é muito reduzida, diria que deve ser 20%. (ENT7)
Sim, há probabilidade	Reflexão sobre a existência de probabilidade de a empresa ser atacada	6	Hoje em dia qualquer empresa pode ser alvo de um ataque cibernético. (ENT2)
P.7 Sofreu algum ataque no último ano			
Informação restrita	Sigilo em informar se a organização foi atacada ou não	1	A informação sobre incidentes específicos é classificada e restrita. (ENT6)
Sim		1	Sofremos um ataque no último ano, mas não houve grandes consequências. (ENT1)
Não sei		1	Não tenho conhecimento dessa informação, visto que não informam os outros departamentos. (ENT7)

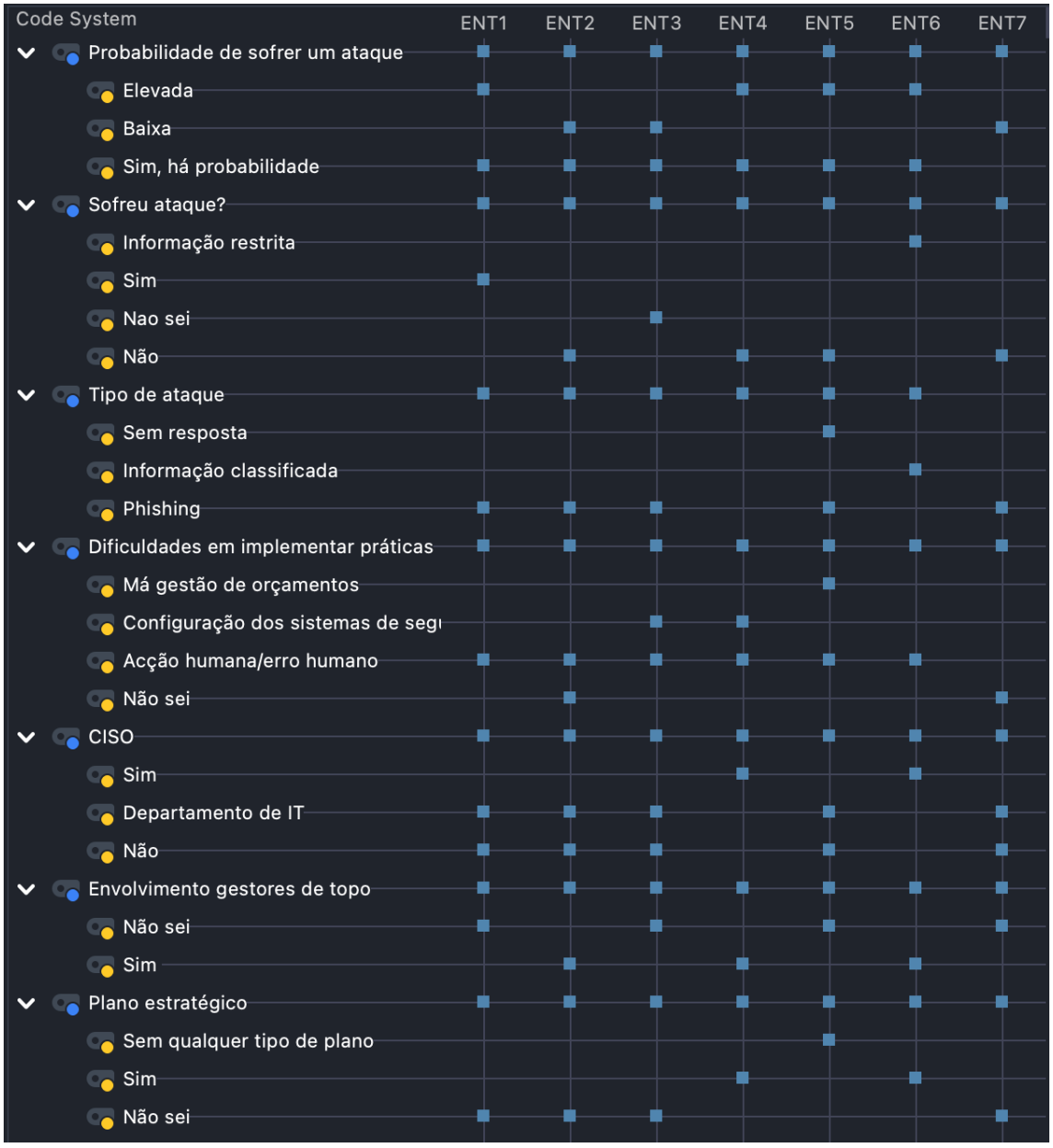
Não		4	No último ano não sofremos nenhum ataque, mas somos afetados diariamente por tentativas de ataque. No entanto, quando acontecer, creio que vamos andar atrás do prejuízo. (ENT5)
P.8 Tipo de ataque sofrido			
Sem resposta	Uma vez que não houve ataque informático, não há especificação do tipo de ataque	1	
Informação restrita	Sigilo em informar se a organização foi atacada ou não	1	A informação sobre incidentes específicos é classificada e restrita. (ENT6)
Phishing	Nas situações em que a organização não sofreu um ataque, verifica-se que as tentativas de ataque são todas de *phishing*	5	Recebemos quase todos os dias tentativas de ataques de phishing através de emails maliciosos. (ENT4)
P.9 Dificuldade em implementar práticas de cibersegurança			
Má gestão de orçamentos	A falta de orçamento dedicado à cibersegurança faz com que esta área da empresa seja mais menosprezada	1	Para além de outros problemas, vejo também situações de má gestão de orçamentos, em que esta área acaba por sofrer. (ENT5)
Configuração dos sistemas de segurança	Dificuldades em instalar sistemas de segurança de forma contínua, visto que estes podem	2	Por vezes existem alguns constrangimentos sentidos na operação ao aplicar novas regras

	causar problemas na operação diária da empresa		de proteção do antivírus que podem criar falsos positivos e isso obriga-nos a despistar e corrigir. (ENT4)
Acção humana/erro humano	O maior problema em implementar práticas de segurança são as próprias pessoas, visto que estas tendem sempre a cometer erros	6	Um dos maiores problemas é o entendimento dos utilizadores em julgar se é boa prática ou não. (ENT4) É difícil promover uma mudança cultural e aumentar a maturidade da empresa. (ENT6)
Não sei	Falta de informação no tema	2	Não sei especificar visto que não tenho conhecimento do tipo de obstáculos que os colegas do departamento de IT encontram. (ENT3)
P.10 Existência de um CISO na organização			
Sim	Existe um CISO	2	
Não	Não existe um CISO	5	
Departamento de IT	Nos casos em que não existe um CISO, a posição é preenchida pelo departamento de IT	5	Infelizmente falta pessoal na equipa, e é difícil contratar nesta área. As pessoas que aqui estão são autodidatas e fazem um pouco de tudo. (ENT5)
P.11 Envolvimento dos gestores de topo			
Não sei	Falta de informação entre departamentos faz com a	4	

	resiliência cibernética da organização seja menos eficaz		
Sim	O envolvimento dos gestores de topo nas operações de segurança da empresa, aumentam a maturidade cibernética da mesma	3	Os gestores de topo estão envolvidos em todas as reuniões e decisões sobre a segurança informática da organização. Há mesmo muito envolvimento. (ENT6)
P.12 Existência de um plano estratégico			
Sem qualquer tipo de plano	A inexistência de um plano estratégico para cibersegurança faz com que a organização esteja mais vulnerável, tornando-a ineficaz na presença de um ataque.	1	
Sim	Organizações com um plano estratégico em cibersegurança demonstram mais capacidade de resposta e maturidade cibernética.	2	
Não sei	Falta de informação entre departamentos	4	Não sei se a organização tem um plano estratégico nesta área. Apenas disseram-me para informar o meu superior caso alguma coisa acontecesse, mas o departamento de IT não fornece mais informações. (ENT3)
P.13 Formação dos colaboradores			

Não	Não oferece qualquer tipo de formação	1	Nunca recebemos qualquer tipo de formação nesta área. (ENT1)
Sim	Oferece formação	5	Sim, recebemos formação que é dada a todos os colaboradores da empresa na plataforma interna. (ENT2)
1 formação em 10 anos	Ofereceu apenas uma formação há uma década atrás	1	Recebi uma formação em Blueteam há 10 anos atrás, e nunca mais ofereceram formações. (ENT5)
Semanalmente	As formações são feitas semanalmente	1	As formações acontecem de semanalmente para garantir o contínuo envolvimento dos colaboradores. (ENT6)
Uma vez por ano	As formações são feitas uma vez por ano	2	
Duas vezes por ano	As formações são feitas duas vezes por ano	1	
Online+vídeos+questões	As formações são feitas online, no sistema da organização e consistem em vídeos e questões de avaliação	4	A formação é feita através de uma plataforma interna da empresa, dedicada às formações dos colaboradores, e também são partilhados *flyers* informativos via email. (ENT4)
P.14 Auto-avaliação			
2	Classificação de 0 a 5	2	
4	Classificação de 0 a 5	4	
5	Classificação de 0 a 5	1	

Anexo V – Matrix do código para cada entrevista no MAXQDA


Code System
ENT1
ENT2
ENT3
ENT4
ENT5
ENT6
ENT7
Probabilidade de sofrer um ataque
Elevada
Baixa
Sim, há probabilidade
Sofreu ataque?
Informação restrita
Sim
Nao sei
Não
Tipo de ataque
Sem resposta
Informação classificada
Phishing
Dificuldades em implementar práticas
Má gestão de orçamentos
Configuração dos sistemas de segı
Acção humana/erro humano
Não sei
CISO
Sim
Departamento de IT
Não
Envolvimento gestores de topo
Não sei
Sim
Plano estratégico
Sem qualquer tipo de plano
Sim
Não sei


Code System
ENT1
ENT2
ENT3
ENT4
ENT5
ENT6
ENT7
Nível de importância
Práticas de cibersegurança
Controlos
Legislação e Diretivas
Dificuldades em implementar diretivas
Probabilidade de sofrer um ataque
Sofreu ataque?
Tipo de ataque
Dificuldades em implementar práticas
CISO
Envolvimento gestores de topo
Plano estratégico
Formação
Não
Sim
1 formação em 10 anos
Semanalmente
Duas vezes por ano
Uma vez por ano
Online+Vídeos+Questões
Auto-avaliação
5
2
4