INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Cibercrime nas Empresas Portuguesas: Perfis de Ataques Cibernéticos e as Denúncias de Incidentes às Autoridades

Maria Beatriz Martins Coelho

Mestrado em Gestão

Orientadora:
Professora Doutora Paula Alexandra Barbosa da Conceição Vicente Duarte, Professora Associada com Agregação,

Iscte – Instituto Universitário de Lisboa

Setembro, 2025

BUSINESS
SCHOOL

Departamento de Marketing, Operações e Gestão Geral

Cibercrime nas Empresas Portuguesas: Perfis de Ataques Cibernéticos e as Denúncias de Incidentes às Autoridades

Maria Beatriz Martins Coelho

Mestrado em Gestão

Orientadora:
Professora Doutora Paula Alexandra Barbosa da Conceição Vicente Duarte, Professora Associada com Agregação,

Iscte – Instituto Universitário de Lisboa

Setembro, 2025

Agradecimentos

A conclusão desta dissertação não seria possível sem o apoio incondicional da minha família, a quem sou eternamente grata. Eles foram o meu suporte e ensinaram-me o valor da perseverança e da dedicação. Agradeço também aos meus amigos, que me animaram, ao longo desta trajetória e sempre me incentivaram a seguir em frente. Um obrigado também aos meus colegas de trabalho e aos meus superiores pela flexibilidade e apoio ao longo deste ano.

Por fim, gostaria de expressar a minha profunda gratidão à minha orientadora, a Professora Paula Vicente. A sua orientação foi crucial para o sucesso desta pesquisa. A constante disponibilidade para esclarecer as minhas dúvidas e orientar o processo de escrita fizeram toda a diferença. Agradeço sinceramente por toda a ajuda e pela confiança depositada em mim ao longo deste trabalho.

Resumo

Esta dissertação analisa o panorama do cibercrime em empresas portuguesas, e foca-se nos tipos de ataques cibernéticos e nos motivos que levaram à subnotificação destes incidentes às autoridades. O estudo baseou-se nos dados do inquérito *Flash Eurobarometer 496* da Comissão Europeia, complementado pela revisão de literatura.

A revisão de literatura mostra que engenharia social e *malware* são os ataques mais comuns no contexto empresarial nacional. Diversas infraestruturas críticas em Portugal evidenciaram o impacto significativo destes crimes, tanto ao nível financeiro como operacional e reputacional. O aumento expressivo do número de denúncias entre 2016 e 2023 revelam uma maior consciência e exposição, mas destacam também desafios na resposta institucional.

A análise de *clusters* identificou três grupos de empresas, diferenciados pela incidência de ataques: um *cluster* sem registo de incidentes, um com baixa incidência e outro altamente afetado. A caracterização dos 3 *clusters* revelou uma predominância do setor da construção, transportes e TIC. Verificou-se uma elevada taxa de intenção de não reporte no *Cluster* 1. Nos *Clusters* 1 e 3 foram identificados como fatores de subnotificação, a perceção de trivialidade dos ataques, a preferência por resolução interna, o desconhecimento do papel da polícia, e a inconveniência como o receio de danos reputacionais.

A subnotificação compromete a eficácia das políticas públicas e a compreensão real do fenómeno do cibercrime, o que perpetua as vulnerabilidades no tecido empresarial. O estudo conclui que é urgente reforçar a sensibilização das empresas, simplificar os processos de denúncia e promover uma maior confiança nas autoridades policiais. Recomenda-se ainda a adoção de medidas de prevenção e resposta, envolvendo tanto o setor público como privado.

Palavras-chave: Cibercrime, Ataques cibernéticos, Subnotificação de cibercrimes, Segurança da informação; Portugal.

Códigos JEL:

- K42 - Ilegalidade e sua aplicação: Crimes e comportamentos ilícitos
- O33 - Inovação tecnológica: Escolha e difusão; Impactos na sociedade (incluindo segurança cibernética)

Abstract

This dissertation analyzes the landscape of cybercrime in Portuguese companies, focusing on the types of cyberattacks and the reasons behind the underreporting of such incidents to the authorities. The study was based on data from the European Commission's Flash Eurobarometer 496 survey, complemented by a literature review.

The literature review shows that social engineering and malware are the most common attacks in the national business context. Several critical infrastructures in Portugal have demonstrated the significant impact of these crimes, both financially and in operational and reputational terms. The sharp increase in the number of reports between 2016 and 2023 reveals greater awareness and exposure, but also highlights challenges in the institutional response.

The cluster analysis identified three groups of companies, differentiated by the incidence of attacks: a cluster with no record of incidents, one with low incidence, and another highly affected. The characterization of the three clusters revealed a predominance of the construction, transport, and TIC sectors. A high rate of non-reporting was observed in Cluster 1. In Clusters 1 and 3, the factors identified as contributing to underreporting included the perception of attacks as trivial, a preference for internal resolution, a lack of knowledge about the role of the police, and inconveniences such as fears of reputational damage.

Underreporting undermines the effectiveness of public policies and the accurate understanding of the cybercrime phenomenon, thereby perpetuating vulnerabilities in the business sector. The study concludes that it is urgent to strengthen business awareness, simplify reporting processes, and promote greater trust in law enforcement authorities. It also recommends the adoption of prevention and response measures involving both the public and private sectors.

Keywords: Cybercrime**,** Cyber attacks**,** Underreporting of cybercrimes**,** Information security and Portugal.

JEL Codes:

- K42 - Illegality and its application: Crimes and illegal behaviors
- O33 - Technological innovation: Choice and diffusion; Impacts on society (including cybersecurity)

Índice

Índice de Quadros

Índice de Figuras

Índice de Anexos

Índice de Apêndices

Capítulo 1 | Introdução

1.1 Contextualização

A segurança digital tornou-se uma questão central no mundo empresarial, especialmente com o aumento exponencial da digitalização e da dependência tecnológica. Empresas de todos os setores enfrentam um cenário desafiador, onde o cibercrime emerge como uma séria ameaça em constante evolução (Anderson *et al*., 2019).

De acordo com Sunil *et al*. (2021), o cibercrime compreende atividades criminosas que têm como alvo o ciberespaço, incluindo práticas como pirataria digital, fraudes online e acessos não autorizados a dados sensíveis. Estas práticas exploram as vulnerabilidades em redes e sistemas de informação, e causam impactos financeiros e operacionais, além de comprometerem a reputação e a confiança das organizações junto dos seus clientes.

No contexto português, a automatização de processos empresariais e a crescente utilização de sistemas de informação tornaram as empresas mais suscetíveis de serem alvo de ciberataques. Um exemplo notório é o ataque sofrido pelo Hospital Garcia da Orta, que foi alvo de um ataque de *ransomware* que paralisou os sistemas informáticos em 2022. O impacto foi significativo e consistiu no adiamento de consultas, obrigando ao uso de processos manuais, o que evidenciou a grave vulnerabilidade do setor da saúde face a este tipo de incidentes (CNN Portugal, 2022). Casos como este destacam a relevância de compreender as ameaças cibernéticas e o comportamento das empresas diante destes desafios.

Dada a crescente sofisticação dos ataques cibernéticos e as suas consequências devastadoras, torna-se essencial investigar os desafios enfrentados pelas empresas portuguesas neste domínio. Esta dissertação pretende contribuir para a compreensão dos tipos de ataques mais frequentes, se as empresas têm a intenção de reportar ou não às autoridades estas ocorrências, e quais as razões da eventual subnotificação, e quais as estratégias que podem ser desenvolvidas para mitigar estas ameaças, de forma a proteger os dados empresariais e fortalecer a segurança digital.

1.2. Definição do Problema

O objetivo central desta investigação é caracterizar a forma como as empresas portuguesas estão a lidar com o fenómeno do cibercrime, de que tipo de ataques cibernéticos estão a ser vítimas,

se têm intenção de reportar ou não os ataques às autoridades competentes e, em caso de não terem essa intenção, quais as razões para tal. Esta questão é de extrema relevância, pois a falta de denúncia dificulta a criação de políticas públicas e estratégias eficazes para a prevenção e mitigação do cibercrime, comprometendo a segurança digital em larga escala.

De forma mais específica, o problema divide-se em duas vertentes principais. A primeira relaciona-se com os tipos de ataques cibernéticos enfrentados pelas empresas em Portugal. É fundamental compreender as características das empresas que são vítimas, para que seja possível propor medidas de prevenção e mitigação. A segunda vertente foca-se na intenção de reporte destes incidentes e nos fatores explicativos da eventual subnotificação destes incidentes. Se as empresas optarem por não reportar estes ataques isso tem implicações graves, não apenas para as próprias empresas afetadas, mas também para o entendimento geral do fenómeno do cibercrime e para a criação de soluções eficazes.

Assim, compreender estas duas dimensões permitirá desenvolver estratégias de apoio e proteção às empresas, promovendo um ambiente empresarial mais seguro e resiliente.

1.3. Objetivos

Os principais três objetivos desta dissertação consistem em:

- Identificar perfis de ataques cibernéticos (nº de ataques) e avaliar a sua associação com características das empresas (p. ex. volume, setor de atividade).
- Analisar os tipos de ataques mais frequentes, o nível da intenção de reporte dos ciberataques às autoridades e as razões da eventual subnotificação dos ataques cibernéticos.
- Propor estratégias para fortalecer a segurança cibernética e incentivar a comunicação de incidentes.

1.4. Estrutura

A estrutura da dissertação foi organizada em 5 capítulos de forma a responder aos objetivos definidos anteriormente.

O Capítulo 1 apresenta uma introdução aprofundada sobre o cibercrime e a segurança digital, com foco nas ameaças que mais afetam as empresas em Portugal. Explica-se por que razão este tema é tão relevante atualmente, e destaca-se o crescimento e a complexidade dos

riscos digitais. Nesta parte, são também definidos os objetivos que orientam toda a investigação e explicada a forma como o trabalho está estruturado.

O Capítulo 2 é dedicado à revisão de literatura, onde começam por ser explorados as definições do conceito de cibercrime, segue-se uma breve explicação sobre a evolução deste fenómeno e quais são os diferentes tipos de ataques mais comuns. São apresentados exemplos reais de ciberataques ocorridos em Portugal. E no final aborda-se as razões para as empresas não reportarem os incidentes. Em suma neste capítulo são apresentados estudos anteriores e identificados os principais desafios que as organizações enfrentam.

O Capítulo 3 descreve a metodologia adotada. Nele são explicados o processo de recolha de dados, a origem e estrutura do questionário utilizado, bem como os critérios para seleção das variáveis consideradas nas análises. É explicado como será feito o tratamento aplicado aos dados e as técnicas estatísticas utilizadas, nomeadamente para a análise de clusters. Além disso, apresenta-se a segmentação das empresas consoante a incidência de ataques sofridos e procede-se à caracterização dos padrões de reporte e das motivações associadas à falta de comunicação de incidentes às autoridades.

O Capítulo 4 apresenta os resultados obtidos. A secção começa apresentar uma análise descritiva, relativamente às variáveis incluídas no estudo. Posteriormente identifica os diferentes clusters e relaciona-os com as características específicas das empresas. São examinados os tipos de ataques mais frequentes assim como as taxas de intenção de reporte de incidentes à polícia e ainda avaliados os fatores que mais contribuem para que muitos casos não sejam oficialmente comunicados. Esta análise permite compreender melhor a relação entre o perfil da empresa, a frequência de incidentes e o seu comportamento face ao reporte.

O Capítulo 5 reúne as conclusões e as recomendações resultantes do trabalho desenvolvido. As recomendações propostas incluem ações para reforçar a sensibilização das empresas, simplificar os processos de denúncia e aumentar a confiança nas forças de segurança. São também sugeridas medidas preventivas e de resposta que incentivem a colaboração entre entidades públicas e privadas. A primeira parte deste capítulo são as principais conclusões do estudo onde é analisado como os resultados podem ajudar a criar estratégias eficazes de cibersegurança e sobre o potencial destas medidas para tornar o ambiente empresarial mais seguro face às ameaças digitais.

Com esta estrutura, a dissertação procura oferecer uma visão ampla e detalhada do cibercrime no contexto português, de forma a combinar a teoria e os dados práticos para propor soluções realistas que ajudem a proteger melhor as empresas face às ameaças digitais.

Capítulo 2 | Revisão da literatura

2.1 Cibercrime

Com o avanço acelerado das tecnologias digitais, o conceito de Cibercrime tornou-se cada vez mais complexo e multifacetado, abarcando uma variedade de ações ilícitas que utilizam a tecnologia como ferramenta e exigem uma análise crítica e contínua para acompanhar as suas transformações e impactos.

O conceito de Cibercrime tem evoluído à medida que as tecnologias digitais se tornam mais integradas nas atividades humanas. Segundo Arora e Wadhwa (2017), o cibercrime consiste em ações que recorrem a computadores e à internet como instrumentos para a prática de atos ilícitos no espaço digital, sendo a tecnologia essencialmente um meio facilitador da ação criminosa. Esta definição remete para um entendimento mais técnico, em que os sistemas informáticos são utilizados como ferramentas para a realização de crimes, tais como ataques a redes, disseminação de *malware* ou roubo de identidade.

No entanto, Indra (2020) propõe uma abordagem mais abrangente, ao considerar o cibercrime não apenas como o uso da tecnologia para cometer crimes, mas também como a exploração estratégica das redes digitais para aceder a informações sensíveis e realizar fraudes complexas. Esta visão realça o carácter sofisticado das ameaças digitais atuais, que muitas vezes envolvem engenharia social, manipulação de dados e técnicas avançadas de intrusão.

Por sua vez, Junior *et al.* (2020) destacam um ponto adicional ao sublinhar que a tecnologia não é apenas um meio, mas também um alvo direto do cibercrime. Ou seja, as infraestruturas digitais, como servidores, bases de dados e redes de comunicação, tornam-se objeto de ataques com potencial de causar disrupções significativas em serviços essenciais e setores críticos. Assim, o cibercrime assume uma dupla dimensão: como uso instrumental da tecnologia e como ameaça à própria integridade das infraestruturas tecnológicas.

Estas perspectivas destacam a diversidade e complexidade do fenómeno, que ao expandir-se com novas tecnologias, desafia as fronteiras da legalidade digital e exige uma análise contínua e adaptável.

2.2 Evolução do Cibercrime

O Cibercrime é um fenómeno em constante transformação, que impõe crescentes desafios às autoridades e exige um esforço contínuo para atualização das estratégias de combate. Curtis e Oxburgh (2023) apresentam uma análise detalhada da evolução do Cibercrime e das dificuldades enfrentadas para identificar e mitigar ameaças, como *phishing* e *ransomware*, que se têm tornado cada vez mais sofisticadas.

Segundo Alam (2022), as primeiras manifestações de um software malicioso surgiram ainda nos primórdios da era digital. O primeiro vírus conhecido, denominado Creeper, foi desenvolvido em 1971, apesar de inofensivo, destacava-se pela sua capacidade de se propagar entre computadores locais, exibindo a mensagem: "*I'M THE CREEPER: CATCH ME IF YOU CAN*." Posteriormente, em 1986, foi criado o Brain, o primeiro vírus para computadores, com o objetivo de proteger um software numa disquete contra cópias ilegais. Ambos os exemplos iniciais não causavam danos, mas introduziram o conceito de autorreplicação maliciosa.

A evolução crítica deu-se em 1988 quando Morris explorou uma vulnerabilidade de *buffer overflow*, que se traduz num programa que escreve dados fora da memória alocada, infetando 10% da Internet nessa altura. Ocorreu ainda a criação do AIDS Trojan em 1989, considerado o primeiro *ransomware*, pois bloqueava o acesso aos ficheiros do utilizador e exigia pagamento para a sua recuperação. Este incidente foi um dos primeiros a expor a gravidade das falhas de segurança digital e a impulsionar a conscientização sobre a necessidade de defesa contra crimes cibernéticos (Alam, 2022).

Com a crescente digitalização das últimas décadas, o cibercrime evoluiu de simples atos de vandalismo digital para ataques sofisticados e altamente lucrativos. Na década de 1990, com a popularização da internet e do correio eletrónico, surgiram vírus como o *Melissa* (1999) e o *ILOVEYOU* (2000), que se propagavam por email e causaram prejuízos em mais de 8 biliões de dólares. Estes ataques evidenciaram a vulnerabilidade dos sistemas informáticos e impulsionaram o debate sobre a necessidade de regulamentação e proteção do espaço digital (Alam, 2022).

Este artigo de Alam (2022) revela ainda que os métodos de ataque estão a tornar-se ainda mais avançados, e incorporam redes neurais e inteligência artificial para prever padrões e identificar vulnerabilidades em sistemas de segurança. Além disso, destaca-se a crescente ameaça a infraestruturas críticas, como redes elétricas e sistemas de saúde, o que representa

riscos não apenas ecónomicos mas também à segurança nacional. Por exemplo, em 2010, a evolução do *malware* deu um grande salto, pois foi descoberto o *Stuxnet*, que consiste num malware autorreplicante criado para atacar instalações nucleares ou outras infraestruturas sensíveis de um país. Com isto, é possível verificar que as infraestruturas importantes de um país podem estar constantemente em risco.

Atualmente, o cibercrime é facilitado pelo recurso à *dark web*, que proporciona um ambiente anónimo para a comercialização de dados roubados, software malicioso e outros bens ilegais. Este mercado clandestino é alimentado pelo uso de criptomoedas como o Bitcoin, que oferecem anonimato nas transações, o que dificulta o rastreamento e a responsabilização criminal (Alam, 2022).

Em suma, desde os vírus inocentes como *Creeper* e *Brain*, até ao uso de Inteligência Artificial (IA) para efetuar ataques, é possível verificar que o cibercrime evoluiu de uma simples curiosidade técnica para um problema global com implicações económicas, políticas e de segurança nacional. Por isso é necessário que as medidas de defesa acompanhem esta evolução, o Cibercrime exige respostas cada vez mais complexas e coordenadas com leis, tecnologia e cooperação internacional (Alam, 2022).

No âmbito legal, Ruddin e Zein (2024) discutem a evolução das legislações relacionadas como Cibercrime, e destacam a importância da cooperação internacional para lidar com estas ameaças globais. A Convenção de Budapeste, por exemplo, estabeleceu diretrizes importantes na aplicação da lei contra crimes cibernéticos e o Regulamento Geral sobre a Proteção de Dados (RGPD) introduziu novas salvaguardas para proteger dados pessoais. Estas iniciativas demonstram como a legislação evolui em resposta aos avanços tecnológicos, embora ainda enfrente desafios para acompanhar o ritmo das inovações e das ameaças emergentes no ambiente digital (Ruddin e Zein, 2024).

2.3 Ataques Cibernéticos

Suayyid *et al.* (2023) afirmam que a cibersegurança é uma preocupação crescente para empresas em todo o mundo, uma vez que os criminosos exploram vulnerabilidades em sistemas digitais para atingir diferentes objetivos.

Estes ataques cibernéticos consistem em ações com má intenção destinadas a obter acesso não autorizado, comprometer a integridade de dados, causar interrupções operacionais

ou até mesmo roubar informações sensíveis, como dados privados. Com a crescente sofisticação das técnicas, até mesmo organizações com estruturas de cibersegurança robustas e formalizadas encontram desafios para prevenir ou mitigar tais ameaças, o que torna essencial o desenvolvimento contínuo de estratégias proativas e adaptáveis de defesa digital (Suayyid *et al*., 2023).

De acordo com o relatório da UNICRI (2014) , as ameaças e os ataques cibernéticos mais comuns são:

- *Malware*: De acordo com Ansori *et al*. (2023), o *malware* constitui uma ameaça significativa à integridade dos sistemas informáticos, sendo utilizado por cibercriminosos para explorar vulnerabilidades, roubar dados sensíveis ou causar danos operacionais. Um dos tipos mais perigosos de *malware* é o *ransomware*, que, ao infectar um dispositivo, criptografa os dados da vítima e exige o pagamento de um resgate, geralmente em criptomoedas, como condição para a recuperação do acesso.

- Engenharia Social: Gomes (2020) define a Engenharia Social como o conjunto de técnicas psicológicas e persuasivas usadas para manipular indivíduos afim de obter informações sensíveis ou aceder a sistemas restritos. Esta abordagem explora vulnerabilidades humanas como a confiança, o medo ou a curiosidade, em vez de explorar diretamente falhas técnicas. Por exemplo, os criminosos utilizam métodos como o *phishing* que é uma subcategoria de Engenharia Social, que consiste no envio de mensagens fraudulentas, geralmente por e-mail, que imitam comunicações legítimas de empresas, instituições bancárias ou serviços populares e costumam incluir links ou anexos maliciosos de forma a induzirem a vítima a fornecer dados pessoais, senhas ou informações bancárias. Uma variação mais recente e igualmente perigosa é o *smishing* (termo derivado de "*SMS phishing*"), no qual a tentativa de engano ocorre por meio de mensagens de texto no telemóvel. Estas mensagens podem conter links maliciosos ou instruções que levam a vítima a instalar aplicações falsas ou partilhar dados confidenciais. Ambos os métodos têm como base a confiança na comunicação recebida e exploram a tendência humana de responder rapidamente a alertas, promoções ou notificações aparentemente urgentes.

- Ameaças de *Zero-Day*: Segundo Guo (2023), as ameaças de *Zero-Day* referem-se a ataques cibernéticos que exploram vulnerabilidades, ainda desconhecidas dos criadores

do software ou hardware, para as quais não há qualquer correção ou atualização disponível. Estas vulnerabilidades são especialmente perigosas porque os métodos tradicionais de segurança digital, principalmente os que se baseiam em assinaturas pré-existentes, não conseguem detetá-las eficazmente, já que estas assinaturas simplesmente não existem no momento do ataque. Geralmente, estas falhas são exploradas em ataques direcionados, permitindo que os invasores utilizem técnicas inéditas para aceder de forma não autorizada a sistemas críticos. Isto possibilita aos criminosos permanecerem ocultos por períodos prolongados, até serem identificados. Aproximadamente 80% das violações de segurança têm origem em ataques *Zero-Day*, com custos significativos que chegam, em média, a 1,2 milhões de dólares por ataque. Estes ataques são frequentemente direcionados para sistemas corporativos, infraestruturas governamentais e setores essenciais como energia e saúde, podendo provocar danos consideráveis como o comprometimento de dados sensíveis, interrupções operacionais críticas e perdas significativas na reputação e confiança pública nas organizações afetadas (Guo, 2023).

- Ataques DDoS (*Distributed Denial of Service*): Sivakumar *et al.* (2023), referem que os ataques DDoS sobrecarregam um sistema-alvo com um volume massivo de tráfego. O excesso de solicitações impede o acesso de utilizadores legítimos, o que causa interrupções e torna os serviços ou *websites* inacessíveis por períodos prolongados. Estes ataques são particularmente prejudiciais para as empresas, pois podem resultar na paralisação de operações essenciais, o que acaba por afetar a experiência do cliente e causar prejuízos financeiros. Devido à sua gravidade e ao impacto potencial, proteger os sistemas contra DDoS é uma prioridade para as equipas de segurança, que utilizam métodos como filtros de tráfego e redes de distribuição de conteúdo para minimizar os efeitos desses ataques.

- Injeção de Structured Query Languag (SQL): Demilie e Deriba (2022) descrevem os ataques de injeção de SQL como uma forma de exploração de vulnerabilidades em aplicações *web*, onde códigos SQL maliciosos são inseridos em consultas ao banco de dados, alterando o seu funcionamento habitual. Esse tipo de ataque permite que os invasores tenham acesso a informações confidenciais sem autorização, manipulem dados ou até comprometam a integridade e segurança de todo o banco de dados. Em sistemas onde as entradas do utilizador não são devidamente filtradas ou validadas, os

invasores conseguem, por exemplo, visualizar informações privadas de utilizadores, modificar registos, e em casos extremos, obter o controlo administrativo do sistema. Ataques de injeção de SQL são particularmente perigosos porque exploram diretamente as camadas mais críticas de uma aplicação, o que obriga a que as empresas tomem medidas robustas de segurança, como filtragem de entradas, validação rigorosa e o uso de consultas parametrizadas para mitigar riscos e proteger dados sensíveis.

- Ataques *Man-in-the-Middle* (MitM): Gangan (2015) define os ataques *Man-in-the-Middle* (MitM) como uma forma de interseção em que o invasor se insere entre duas partes em comunicação, e pode monitorizar e modificar os dados transmitidos sem que as partes percebam. Estes ataques exploram vulnerabilidades nos protocolos de autenticação utilizados pelas partes envolvidas na comunicação. Tipicamente, a autenticação é feita por entidades terceiras, responsáveis pela emissão de certificados digitais, e estas próprias entidades podem tornar-se pontos vulneráveis ao ataque.

- Ataques de *Brute Force*: Ataques de *Brute Force* ou Força Bruta são descritos por Hamza e Al-Janabi (2024) como tentativas repetidas de adivinhar senhas ou chaves de acesso, usando a força computacional para testar todas as combinações possíveis até que a correta seja encontrada. Estes ataques exploram a vulnerabilidade de senhas fracas ou de sistemas que não possuem proteção contra múltiplas tentativas de *login*.

- *Cross-Site Scripting* (XSS): *Cross-Site Scripting* (XSS) é um tipo de vulnerabilidade de segurança em aplicações *web*, na qual *scripts* maliciosos são incorporados e executados em páginas de *websites* confiáveis. Este ataque acontece quando as aplicações *web* não filtram adequadamente as entradas fornecidas pelos utilizadores antes de apresentarem essas páginas *web*. Uma vez que os scripts são executados no contexto de segurança do domínio alvo, o navegador interpreta o conteúdo malicioso como legítimo, permitindo que invasores redirecionem utilizadores para sites maliciosos, roubem dados de login ou sequestrem sessões inteiras. Dessa forma, os atacantes podem aceder a informações confidenciais como *cookies*, sessões de navegação e outros dados sensíveis armazenados pelo navegador (Abikoye *et al*. 2020).

2.4 Ataques Cibernéticos em Portugal

De acordo com os relatórios do Centro Nacional de Cibersegurança e do Mistério Público os ataques cibernéticos mais recorrentes em Portugal, em 2022 e 2023, foram o *ransonware,* o

phishing e as suas variantes *smishing e vishing* (Centro Nacional de Cibersegurança, 2024, 2023; Ministério Público, 2023).

Quadro 2.1- Evolução das denúncias recebidas e das denúncias remetidas para inquérito

Ano	Denúncias recebidas	Denúncias remetidas para inquérito
2016	108	25
2017	155	59
2018	160	50
2019	193	67
2020	544	138
2021	1160	195
2022	2124	359
2023	2916	563

Figura 2.1 - Evolução das denúncias recebidas e das denúncias remetidas para inquérito

De acordo com o Ministério Público (2023), e como é possível ver na Figura 2.1 e no Quadro 2.1, entre 2016 e 2023, observou-se um crescimento significativo nas denúncias recebidas. Em 2016, foram registadas 108 denúncias, tendo este número aumentado gradualmente até atingir um pico de 2.916 em 2023.

O aumento mais expressivo deu-se a partir de 2020, coincidindo possivelmente com a aceleração da transformação digital em resposta à pandemia de COVID-19. Em 2020, as denúncias subiram para 544, mais do dobro do ano anterior. Em 2021, esse número mais do

que duplicou, atingindo 1.160. Essa tendência ascendente manteve-se nos anos seguintes, com 2.124 denúncias em 2022 e 2.916 em 2023 (Ministério Público, 2023).

Paralelamente, o número de denúncias remetidas para inquérito também aumentou, passando de 25 em 2016 para 563 em 2023. Isto indica não apenas um maior volume de ocorrências, mas também um reforço na resposta institucional perante estes crimes. Embora este valor das denúncias remetidas para inquérito, quando comparado ao valor das denúncias recebidas, seja baixo pode indicar alguma ineficiência por parte das autoridades competentes (Ministério Público, 2023).

Em 2023 no conjunto das denúncias recebidas e efetivamente confirmadas (2060 das 2.916 denúncias recebidas), o *phishing* continua a destacar-se como uma das práticas mais recorrentes e preocupantes. Neste ano, foram recebidas 326 denúncias deste tipo, representando 16,09% do total de casos reportados. As campanhas de *phishing* caracterizam-se por mensagens fraudulentas enviadas massivamente com o objetivo de obter dados sensíveis, como informações de cartões de crédito e, em menor escala, acessos a contas bancárias (Ministério Público, 2023).

De facto, entre as denúncias de 2023, apenas 10 diziam respeito a tentativas de acesso direto a contas bancárias, enquanto a grande maioria visava dados de cartões de crédito. Além do *phishing*, os ataques de *ransomware* também merecem destaque, tendo afetado sobretudo pequenas e médias empresas. Foram ainda reportadas 45 denúncias relativas a mensagens de correio eletrónico contendo *malware* de diversa natureza (Ministério Público, 2023).

Segundo os relatórios do Centro Nacional de Cibersegurança (2023, 2024), Portugal enfrentou falhas críticas na segurança digital de organizações públicas e privadas. O ano de 2022 destacou-se por vários episódios muito mediáticos e com grande impacto na prestação de serviços essenciais. Em janeiro, o setor dos media foi abalado por um ataque ao grupo Impresa, que resultou na modificação das suas plataformas e no envio de mensagens fraudulentas aos utilizadores, o que gerou uma forte perceção de insegurança digital.

Já em fevereiro, a Vodafone foi alvo de um ataque grave que teve início a 7 de fevereiro de 2022. Este ataque de grande escala afetou a operadora de telecomunicações e causou falhas operacionais nos sistemas. Aproximadamente 4 milhões de clientes enfrentaram interrupções nos serviços. Além disso, a segurança de serviços essenciais, como os de emergência, prestados pelos bombeiros e hospitais, foi comprometida (Gonçalves, 2022).

Por exemplo a rede Multibanco, gerida pela SIBS, parceira da Vodafone, também foi afetada. Este ataque à Vodafone afetou quase metade da população em Portugal. A Polícia Judiciária não conseguiu identificar os responsáveis. A 10 de fevereiro, a Vodafone anunciou que a maioria dos seus serviços já estavam operacionais, embora ainda apresentasse algumas limitações e instabilidades (Gonçalves, 2022).

O ano de 2022 foi especialmente marcado por casos de ciberataque. Além dos já referidos, registaram-se, em fevereiro, ataques de *ransomware* ao Laboratório Germano de Sousa, que suspendeu os seus serviços laboratoriais, e à Sonae MC, que afetou diretamente os clientes através da indisponibilidade dos cartões de fidelização (Centro Nacional de Cibersegurança, 2023).

Seguiram-se outros incidentes deste tipo: em abril, o Hospital Garcia de Orta foi atingido, o que colocou em risco o normal funcionamento de um serviço de saúde; em maio, foi atingida a Eletricidade dos Açores, o que levantou sérias preocupações sobre a cibersegurança no setor energético e em agosto, a TAP sofreu um ataque que levou à exposição de dados sensíveis dos seus clientes (Centro Nacional de Cibersegurança, 2023).

Fora os ataques de *ransomware* houve em novembro, uma intrusão nos sistemas da Segurança Social, obtida através do acesso indevido a uma conta, que apesar de não ter comprometido dados pessoais, teve impacto significativo em termos de alarme social. O ano terminou com um total de 2.023 incidentes reportados, refletindo um aumento de 14% face a 2021. Este crescimento sustentado demonstra não só o aumento da atividade criminosa no ciberespaço, como também a maior capacidade de deteção e reporte das ameaças (Centro Nacional de Cibersegurança, 2023).

Já em 2023, os ciberataques mais comuns continuaram a ser os de *ransomware*, mas com um novo padrão de distribuição: a maioria dos incidentes teve efeitos localizados, incidindo sobretudo sobre a Administração Pública Local. Diversas Câmaras Municipais e uma entidade ligada ao setor das águas foram comprometidas, o que causou perturbações operacionais significativas, ainda que com alcance geográfico limitado (Centro Nacional de Cibersegurança, 2024).

No entanto, também se registaram alguns episódios com impacto nacional, como a falha tecnológica numa infraestrutura crítica, que causou uma interrupção generalizada de serviços digitais. A este cenário juntaram-se ações de ciberataques com motivações ideológicas. Um

exemplo foi a alteração não autorizada de conteúdos num site de comunicação social e um ataque de negação de serviço distribuída (DDoS) contra uma instituição da Administração Pública Central, ambos com efeitos disruptivos relevantes (Centro Nacional de Cibersegurança, 2024).

Em termos quantitativos, o último trimestre de 2023 destacou-se como o período mais ativo em número de incidentes registados. Organismos como o CERT.PT, a RNCSIRT e a APAV confirmaram que essa fase final do ano concentrou o maior volume de atividade maliciosa, o que reforça a tendência de crescimento e sofisticação das ameaças digitais em território nacional (Centro Nacional de Cibersegurança, 2024).

Outros tipos de ataques como Man-in-the-Middle (MitM) também têm sido utilizados por grupos criminosos em Portugal, nomeadamente em esquemas de fraude empresarial conhecidos como "CEO fraud" ou "Business Email Compromise (BEC)". Em 2024, a Polícia Judiciária deteve em Lisboa um indivíduo suspeito de integrar uma rede transnacional que, através da interceção e manipulação de comunicações de correio eletrónico entre empresas, alterava dados bancários para desviar transferências de elevados montantes para contas em bancos portugueses, caracterizando assim um ataque de tipo MitM (Polícia Judiciária, 2024).

Cerca de 80% das entidades que notificaram violações de dados pessoais à Comissão Nacional de Proteção de Dados (CNPD) em 2022 eram privadas, enquanto 20% eram públicas. O *ransomware* foi responsável por 30% dos incidentes de violações de dados, seguido por falhas humanas (22%) e falhas aplicacionais como *phishing* (13%). O crescimento das denúncias relacionadas ao *ransomware* foi de 57% em comparação ao ano anterior (CNPD, 2023).

Além disso, conforme indicado no relatório da Rede de Bibliotecas Escolares (RBE, 2023), houve um aumento significativo de ataques de engenharia social em Portugal, impulsionado pela rápida digitalização durante e após a pandemia de 2019. A transição digital também permitiu uma maior exposição a ataques de ciberespionagem, especialmente envolvendo organizações governamentais, onde os criminosos procuram obter vantagens estratégicas sobre estas entidades.

No geral, as táticas mais comuns em Portugal incluem o *phishing*, como observado no relatório da ESET (2024), que é uma empresa de cibersegurança. E além disso, foi possível verificar que os ataques de *ransomware* têm impactado gravemente infraestruturas críticas,

enquanto as técnicas de Engenharia Social, como *smishing*, exploram a falta de conscienzialização sobre a cibersegurança (Centro Nacional de Cibersegurança, 2024).

2.5 Denúncias do Cibercrime

Em Portugal, a subnotificação de cibercrimes constitui um problema persistente, que compromete a compreensão real da dimensão deste fenómeno e, consequentemente, a eficácia das medidas de prevenção e combate.

O Relatório Anual de Segurança Interna (RASI, 2021) indica que em 2020 foram registados cerca de 1672 crimes informáticos, número que representa um crescimento face a anos anteriores.

Segundo o Centro Nacional de Cibersegurança (2023), o total de crimes informáticos não reflete a totalidade dos incidentes ocorridos. Esta diferença entre a criminalidade efetiva e os crimes denunciados demostra a existência de um elevado grau de não reporte.

As razões que explicam este fenómeno são muitas. Muitas empresas não reconhecem determinados incidentes como cibercrimes, sobretudo quando os impactos parecem superficiais ou quando não existe prejuízo financeiro imediato. Por exemplo, os ataques de *phishing* não concretizados, fraudes de baixo valor ou falhas técnicas facilmente confundidas com erros humanos acabam por não ser comunicados às autoridades (Sangari*, et al.* 2022).

A estes fatores acresce o desconhecimento sobre os canais de denúncia. Apesar da existência de mecanismos como a "Linha Internet Segura" e o "Gabinete de Cibercrime da Procuradoria Geral da República". A verdade é que muitos utilizadores não sabem como recorrer a estas entidades, ou consideram o processo demasiado complexo e demorado (Centro Nacional de Cibersegurança, 2023).

Outro elemento que contribui para o não reporte é o receio de danos reputacionais. Muitas empresas, ao serem alvo de ataques, optam por não denunciar para não expor fragilidades internas e evitar perder a confiança de clientes ou dos investidores. Esta atitude, embora compreensível do ponto de vista empresarial, tem como consequência a omissão de incidentes relevantes e a limitação da resposta coletiva (Sangari et al., 2022).

Também existe uma perceção geral de que as autoridades não têm os meios técnicos e humanos necessários para investigar de forma eficaz este tipo de crime, o que reforça a crença de que denunciar não compensa (RASI, 2021).

A ausência de um sistema de denúncia simples e acessível contribui ainda mais para o desincentivo, o que cria um ciclo de vítimas que optam por não reportar (Centro Nacional de Cibersegurança, 2023).

Ao não reportarem os incidentes, dificulta-se a monitorização e a análise realista do problema, o que conduz a políticas públicas pouco eficazes. Além disso, perde-se a oportunidade de identificar padrões de ataque e redes criminosas, o que enfraquece a capacidade de prevenção e investigação (Sangari *et al.,* 2022).

Este quadro continua a incentivar a invisibilidade do cibercrime e cria uma sensação de insegurança, em que tanto empresas como cidadãos ficam vulneráveis a novos ataques sem que o Estado disponha de dados fiáveis para agir (Centro Nacional de Cibersegurança, 2023).

Apesar de muitas organizações portuguesas terem vindo a adotar medidas de cibersegurança, como demonstram os dados da Eurostat (2022), segundo os quais 90% das empresas com mais de 10 funcionários já implementaram pelo menos uma política de proteção digital, estas práticas não se traduzem necessariamente em denúncias mais frequentes. De facto, mesmo entre as empresas que relatam possuir planos de segurança ou formação para colaboradores, uma parte significativa dos incidentes nunca chega às autoridades, revelando uma clara dissociação entre prevenção interna e reporte oficial (Eurostat, 2022).

Em suma, o problema da subnotificação de cibercrimes em Portugal não se prende apenas com a existência de limitações técnicas ou legais, mas com um conjunto mais vasto de fatores sociais, culturais e organizacionais. O desconhecimento dos canais de denúncia, o receio de danos à reputação e a perceção de ineficácia das autoridades contribuem para a invisibilidade do cibercrime (Sangari *et al.,* 2022; Centro Nacional de Cibersegurança, 2023).

Combater esta realidade exige a implementação de estratégias que incluam campanhas de sensibilização, simplificação dos mecanismos de denúncia e um reforço da capacidade institucional de resposta. Só através de uma abordagem clara e sistemática será possível reduzir a subnotificação, aumentar a confiança das vítimas no sistema e reforçar a segurança do país (RASI, 2021).

Capítulo 3 | Metodologia

Este capítulo apresenta a abordagem metodológica adotada para a realização do estudo, incluindo os procedimentos de recolha e análise de dados. A metodologia foi definida com base nos 3 objetivos da investigação. Descrevem-se, de forma sucinta, os métodos aplicados e os critérios que orientaram o processo de investigação.

3.1 Dados

Os dados usados nesta investigação, têm por base o inquérito *Flash Eurobarometer 496-SMEs and Cybercrime* (Comissão Europeia, 2021), sobre a segurança cibernética em empresas na União Europeia. Para esta dissertação, apenas se consideram os dados relativos às empresas portuguesas, num total de 473 observações.

Tendo em conta os objetivos definidos para esta dissertações foram selecionadas para análise as seguintes variáveis/questões do questionário *Flash Eurobarometer 496* (Apêndice A):

D1-What is the main activity of your company?

D2-How many employees does your company currently have?

D3- How long has your company been in business?

D5-What was your company's total turnover in 2020?

Q1- Which of the following does tour company currently have or use?

Q2- Do employees in your company use personally-owned devices such as smartphones, tablets, laptops or desktop computers to carry out regular business-related activities?

Q3- How well informed do you feel about the risks of cybercrime?

Q4- How well informed do you feel your employees are about the risks of cybercrime?

Q5- In the last 12 months, has your company provided employees with any training or awareness raising about the risks of cybercrime?

Q6- When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?

Q7- Has your company experienced any of the following types of cybercrime in the last 12 months?

Q8- Thinking about the most serious incident, how was this attack carried out?

Q9- Still thinking about the most serious incident, how was your business impacted?

Q10a - Who, if anyone, did you report this incident to?

Q10b- If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to?

Q11 Why did you not report the incident (or incidents) to the police?

Os dados estão disponíveis para utilização pública gratuita em https://www.gesis.org/en/eurobarometer-data-service .

3.2 Preparação dos Dados para Análise

Para dar início ao tratamento dos dados, foi realizada uma revisão inicial do questionário, com o objetivo de selecionar as variáveis relevantes para a análise. Entre o total de questões incluídas no inquérito, apenas a questão 10a foi excluída, por apresentar conteúdo redundante em relação à questão 10b (Anexo 7.A). Todas as demais questões foram mantidas e contribuíram para a construção das variáveis que compõem a base de dados.

Na sequência, foram identificadas diversas variáveis cujas respostas estavam codificadas no formato "1 = sim" e "2 = não". Para uniformizar a codificação e facilitar as análises estatísticas, estas variáveis foram recodificadas em formato binário, assim passaram a adotar os valores 1 = "sim" e 0 = "não". Esta padronização foi essencial para garantir a coerência e a consistência dos dados ao longo de todo o processo analítico.

Além disso, a variável "*Atividade*", que originalmente apresentava 21 categorias distintas, foi agrupada em apenas 6 categorias principais, com base em critérios de similaridade entre os setores de atividade. Esta nova versão da variável passou a ser designada por

"*SetorGrupo*", permitindo uma análise mais clara e comparável entre os diferentes grupos empresariais, ao mesmo tempo em que se preserva a representatividade dos dados.

No Apêndice 8.A encontram-se todas as variáveis usadas neste estudo. É possível observar as descrições, as tipologias e as categorias de cada variável. As variáveis selecionadas para análise são as seguintes: *"SetorGrupo", "NColaboradores", "AnosAtiv", "Volume", "OcorreuMalware", "OcorreuServiçoNegado", "OcorreuContasOnline", "OcorreuPhising", "Ocorreuransomware", "OcorreuAcessoNãoAutorizado", "OcorreuEscuta", "MalwarePolícia", "ServiçoNegadoPolícia", "ContasOnlinePolícia", "PhishingPolícia", "RansomwarePolícia", "AcessoNãoAutorizadoPolícia", "EscutaPolícia", "OutrosAtaquesPolícia", "ReportadoOutraAutoridade", "PolíciaNãoPodiaFazerNada", "DesinteressePolícia", "Internamente", "NãoSabiaPolíciaLidava", "Inconveniente" e "Trivial"*. A maioria destas variáveis, são qualitativas nominais binárias, como por exemplo, a "*OcorreuMalware", e existem* 4 variáveis qualitativas ordinais, como por exemplo "*Volume"*.

3.3 Análise de Dados

A análise dos dados foi realizada no programa RStudio, um software que fornece ferramentas para programação em R, e contempla as seguintes etapas:

1) Caracterização da amostra de empresas, em termos de atividade e funcionamento, e em termos de cibercrime;

2) Criação de um Índice de Cibercrime, caracterizador da experiência da empresa com atos de cibercrime; Este índice é construído pela soma das variáveis/questões Q7_1 a Q7_8, refletindo o número total de incidentes vivenciados por cada empresa nos últimos 12 meses.

3) Segmentação das empresas pelo Índice de Cibercrime, mediante Análise de Clusters hierárquica, recorrendo ao método de Ward em combinação com a medida de Distância Euclidiana ao Quadrado. Esta metodologia permite agrupar as empresas de acordo com o seu perfil de exposição ao cibercrime, criando clusters/segmentos de empresas com características semelhantes entre si, ou seja, homogéneas dentro dos grupos e distintas em relação aos outros clusters.

4) Caracterização dos clusters/segmentos em termos de exposição das empresas ao cibercrime e de características de atividades e funcionamento, nomeadamente *"SetorGrupo", "NColaboradores", "Volume"* e *"AnosAtiv"*.

5) Caracterização dos clusters consoante os tipos de ataques mais frequentes, considerando as variáveis *"OcorreuMalware", "OcorreuServiçoNegado", "OcorreuContasOnline", "OcorreuPhising", "Ocorreuransomware", "OcorreuAcessoNãoAutorizado", "OcorreuEscuta"* .

6) Avaliação da associação entre os segmentos identificados e a intenção de reporte dos incidentes às autoridades considerando as variáveis *"MalwarePolicia", "ServicoNegadoPolicia", "ContasOnlinePolicia", "PhishingPolicia", "RansomwarePolicia", "AcessoNaoAutorizadoPolicia", "EscutaPolicia"* e *"OutrosAtaquesPolicia"*.

7) Avaliação das razões para as empresas não reportarem às autoridades as situações de cibercrime considerando as variáveis *"ReportadoOutraAutoridade", "PolíciaNãoPodiaFazerNada", "DesinteressePolícia", "Internamente", "NãoSabiaPolíciaLidava", "Inconveniente" e "Trivial"*.

Capítulo 4 | Resultados

4.1 Caracterização da Amostra

Primeiramente foram criadas tabelas de frequência para todas as variáveis. Foram apresentados os 4 gráficos (Figura 4.2, 4.3, 4.4 e 4.5) referentes às tabelas de frequência (Apêndice 8.B) das variáveis qualitativas ordinais, que são *"SetorGrupo"*, *"NColaboradores"*, *"AnosAtiv"* e *"Volume"*. Posteriormente, foram gerados os gráficos de barras referentes às tabelas de frequência (Apêndice 8.C) das variáveis qualitativas nominais binárias (Figura 4.6, 4.7 e 4.8). Em suma estes gráficos permitiram observar a distribuição dos valores e possíveis padrões no comportamento destas variáveis. Estas informações iniciais foram essenciais para compreender as características do banco de dados e orientar as próximas etapas da análise.

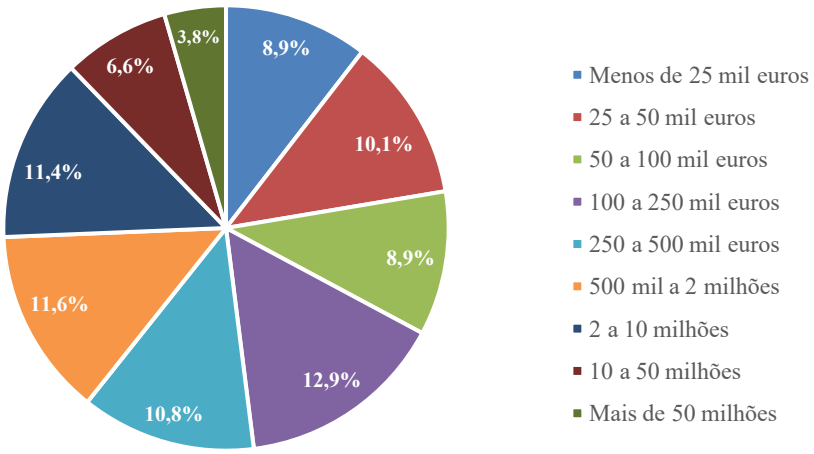

Figura 4.2 - Caracterização da amostra segundo o Volume de Negócios

Começando a análise das variáveis qualitativas ordinais pela variável "*Volume*", constatou-se que esta se encontrava estruturada em nove categorias de intervalos monetários, expressos em euros, que representam o volume de negócios das empresas analisadas, acrescidas de uma décima categoria correspondente aos valores omissos. De acordo com o Apêndice 8.B, a proporção de valores omissos nesta variável foi de 15%.

A distribuição das categorias, tal como ilustrada na Figura 4.2, revelou diferenças significativas entre os intervalos de volume de negócios. A categoria mais expressiva corresponde ao intervalo de 100 a 250 mil euros, que reúne 12,9% das organizações. Em seguida, destacaram-se as categorias de 500 mil a 2 milhões de euros com 11,6% e de 2 a 10

milhões de euros com uma percentagem de 11,4%, ambas apresentam uma presença relevante no conjunto das empresas analisadas.

Em contraste, observou-se que a categoria com menor expressão é a das organizações cujo volume de negócios ultrapassa 50 milhões de euros, o que representa apenas 3,8% do total. Este dado sugeriu que empresas de grande dimensão, em termos de faturação, são menos frequentes na amostra.

É possível concluir que perante o diverso intervalo de volume de negócios que esta distribuição evidenciou um predomínio de empresas situadas nos escalões intermédios de volume de negócios, o que refletiu uma realidade dominada por pequenas e médias empresas (PME).

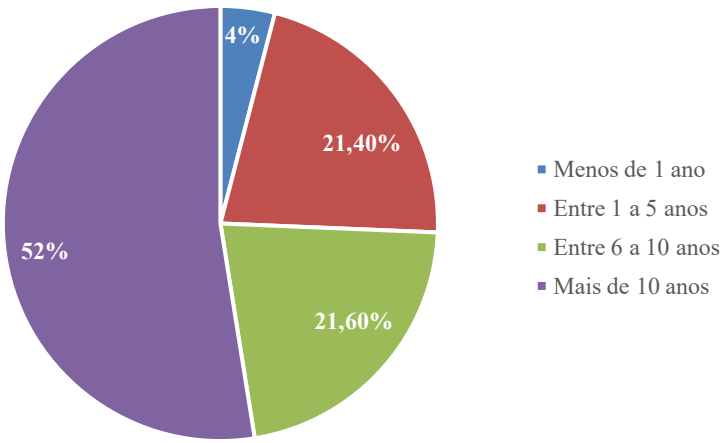

Figura 4.3 - Caracterização da amostra segundo os Anos de Atividade

Passando agora para a variável "*AnosAtiv*" foi observado segundo a Figura 4.3 que a categoria predominante corresponde às empresas com mais de 10 anos de atividade, representando 52% do total. Este resultado evidencia que mais de metade das empresas inquiridas possui experiência no mercado.

Verificou-se ainda que a categoria menos expressiva é a das empresas com menos de 1 ano de atividade, que reúne apenas 4% da amostra. Este resultado indica que as organizações em fase inicial ou de entrada no mercado têm uma presença pequena no conjunto analisado.

Entre estas duas extremidades, constatou-se que as categorias de 1 a 5 anos com 21,4% e de 6 a 10 anos com 21,6% apresentam percentagens semelhantes, o que demonstra que uma

parte considerável das empresas já ultrapassou os primeiros anos, embora ainda se encontre em fases recentes de consolidação.

Com estes resultados é possível concluir que as empresas que responderam ao questionário não se caracterizam por ser recentes, mas sim por organizações estáveis e maduras.

Outra informação importante é que nesta variável existiam 5 empresas que apresentavam como resposta o número 5 o que pode ter sido um erro quando preencheram o questionário, por isso estes valores foram transformados em valores omissos (NA).

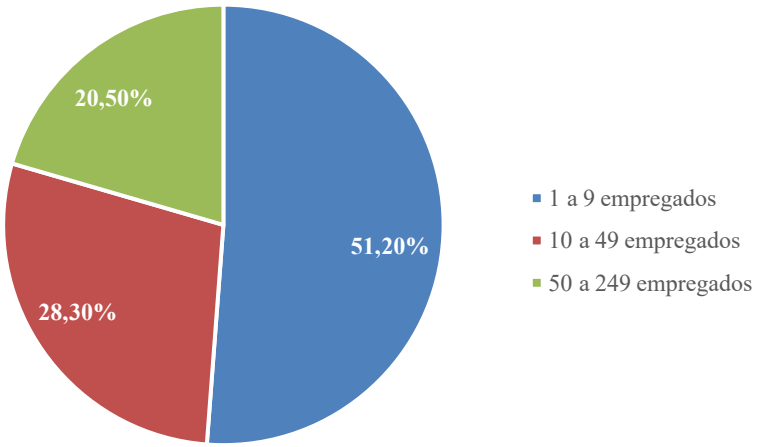

Figura 4.4 - Caracterização da amostra segundo o Número de Colaboradores

Seguidamente na variável "NColaboradores", que representa o número de colaboradores que cada empresa possui, observou-se que as empresas da amostra concentram-se apenas nas categorias de 1 a 9 empregados, de 10 a 49 empregados e de 50 a 249 empregados. Assim, verificou-se que não existem empresas sem colaboradores, ou seja, apenas com o empresário individual, nem empresas com mais de 250 trabalhadores.

Segundo a Figura 4.4, constatou-se que a categoria de 1 a 9 empregados é a mais representativa, porque abrange 51,2% das empresas analisadas. Em seguida, surge a categoria de 10 a 49 empregados, com 28,3%, e, por fim, a categoria de 50 a 249 empregados, que corresponde a 20,5% da amostra.

Estes resultados demonstram que mais de metade das empresas inquiridas possuem uma estrutura de recursos humanos bastante reduzida, caracterizando-se como microempresas. Contudo, uma parte significativa enquadra-se também nas categorias de pequenas com 10 a 49 empregados e médias empresas com 50 a 249 empregados, segundo a legislação portuguesa.

Em suma, é possível concluir que o perfil predominante são as micro, pequenas e médias empresas (PME) ao contrário das grandes organizações, inexistentes na amostra em estudo.

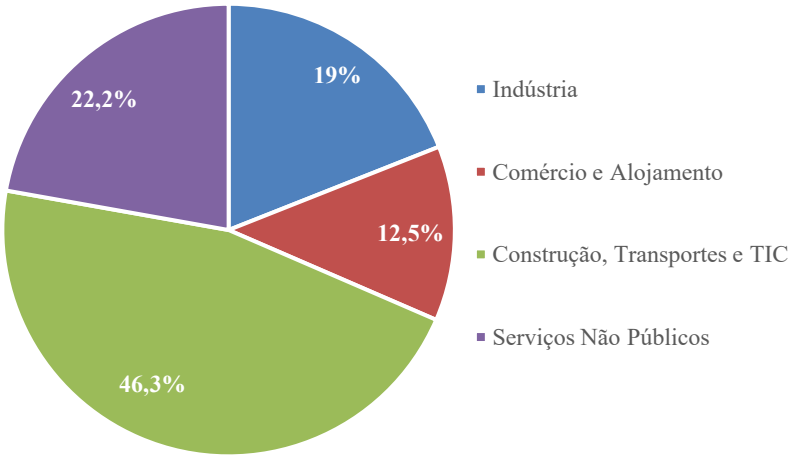

Figura 4.5 - Caracterização da amostra segundo o Setor de Atividade

Relativamente à variável "*SetorGrupo*", segundo a Figura 4.5, é possível observar que a maioria das empresas atua no setor da Construção, Transportes e TIC, que reúne 46,3%. Este resultado mostrou o peso significativo destes ramos de atividade no conjunto de empresas inquiridas.

Em contraste, verificou-se que o setor do Comércio e Alojamento apresenta uma pequena percentagem, com apenas 12,5% das empresas. Os setores da Indústria e dos Serviços Não Públicos registaram percentagens intermédias, de 19% e 22,2%, respetivamente, o que demostrou uma presença relevante, mas inferior à do setor predominante.

Os setores de Serviços Públicos e de Agricultura e Pesca não apresentam qualquer valor na base de dados, o que significa que nenhuma empresa da amostra pertence a estas áreas de atividade.

Assim, concluiu-se que a distribuição das empresas por setores de atividade apresenta uma forte predominância do setor da Construção, Transportes e TIC.

Posteriormente foram também realizadas as tabelas de frequência das variáveis qualitativas nominais binárias e estas apresentam as contagens e as percentagens para todos os indicadores binários (Apêndice 8.C). Estas tabelas apresentam também os valores e as percentagens dos valores omissos.

Seguidamente, foi possível verificar que ataques cibernéticos ocorreram mais vezes, quais os ataques que as empresas denunciaram e quais as razões mais relevantes para que as empresas não reportem. Nas variáveis presentes na Figura 4.6 não há valores omissos por isso estamos perante uma escala percentual de 0% a 100%.

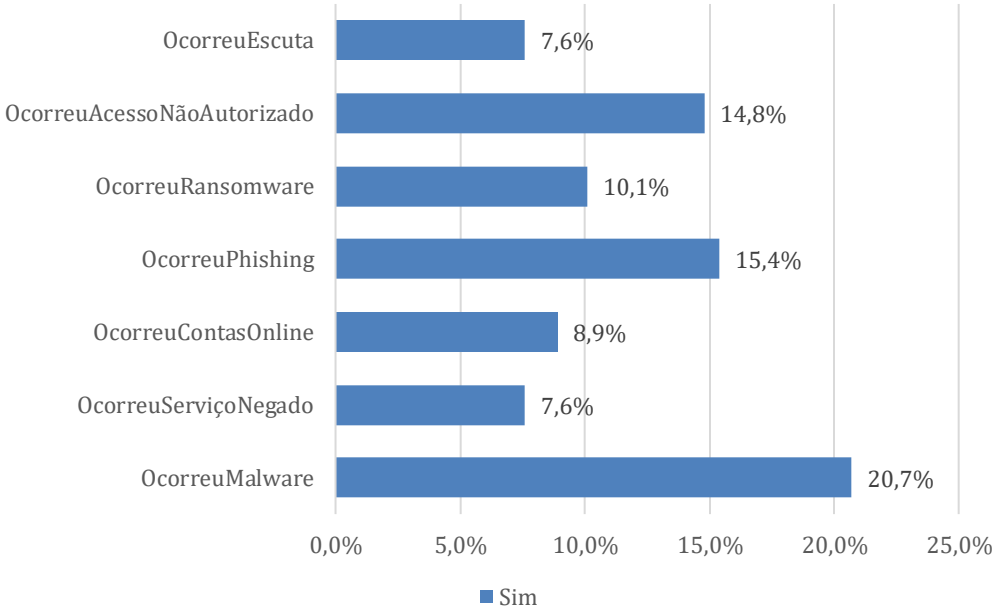

Figura 4.6 - Caracterização das variáveis referente aos Cibercrimes que ocorreram

A Figura 4.6 evidencia que uma pequena percentagem das empresas participantes declarou ter enfrentado incidentes de segurança cibernética. Este dado sugere que, em grande parte das organizações, as medidas de proteção implementadas parecem eficazes na prevenção deste tipo de ocorrência.

Ainda assim, algumas empresas relataram episódios relevantes. O incidente com maior expressão foi o de *malware*, "*OcorreuMalware*" apresentou uma percentagem de 20,7% das organizações. Seguiram-se as variáveis de "*OcorreuPhishing*", com 15,4% e a de "*OcorreuAcessoNãoAutorizado*" com 14,8%, que, apesar de não atingirem a mesma dimensão do *malware*, revelaram fragilidades significativas nos sistemas de defesa.

Em contraste, os episódios menos frequentes corresponderam às variáveis de "OcorreuServiçoNegado" e "OcorreuEscuta", ambas com uma percentagem de apenas 7,6% das empresas. Estes valores, relativamente reduzidos, podem refletir menor incidência destes tipos de ataques.

Assim, embora o panorama geral seja de baixa exposição a ciberataques, nota-se que riscos associados sobretudo ao *malware* e a práticas de engenharia social, como o *phishing*, continuam presentes e não podem ser ignorados.

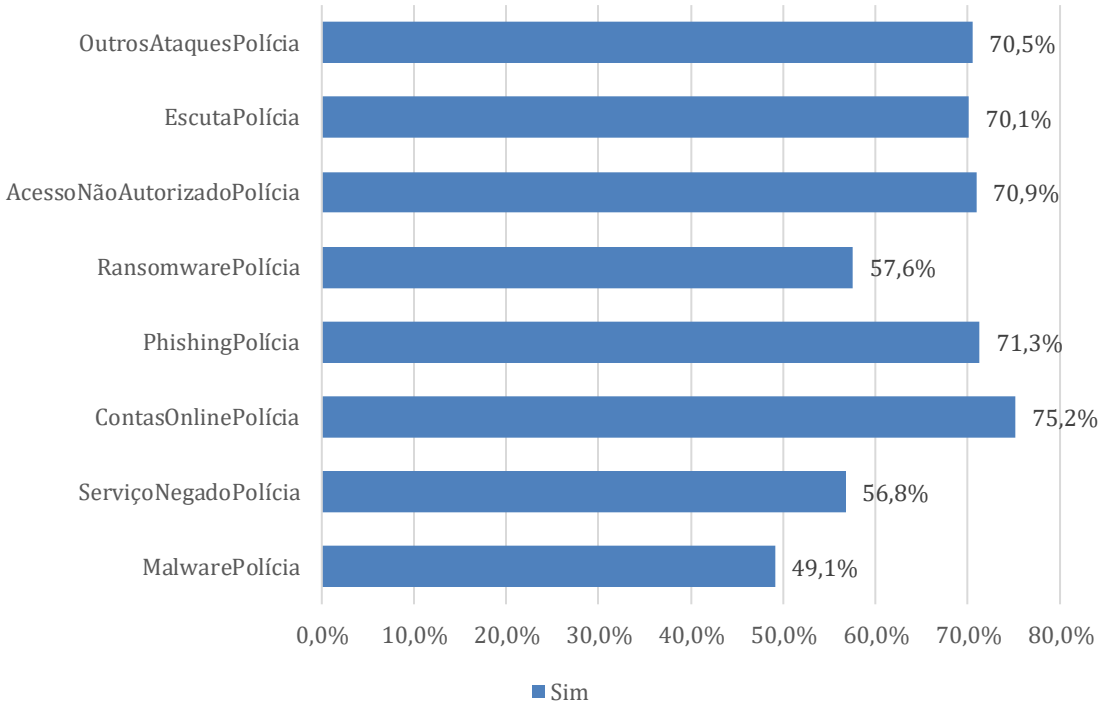

Figura 4.7 - Caracterização das variáveis referentes à Intenção de Reporte à Polícia

Relativamente às variáveis relacionadas à intenção de reporte de ciberataques à polícia, observou-se uma elevada taxa de omissão das respostas, o que representa 50,5% dos dados para cada uma das variáveis analisadas.

No entanto, a partir dos dados válidos disponíveis (49,5%), foi possível identificar quais os tipos de ataques apresentam as maiores percentagens de intenção de reporte à polícia,

Entre os incidentes, segundo a Figura 4.7, o ataque com uma maior percentagem de intenção de reporte à polícia é o que está associado às contas online hackeadas, representado pela variável *"ContasOnlinePolícia"*, com uma percentagem de intenção de reporte de 75,2%. Logo em seguida, destaca-se a variável *"PhishingPolícia",* onde 71,3% das empresas afirmaram

que tinham a intenção de comunicar esse tipo de incidente à polícia. A seguir seguiram-se as variáveis *"AcessoNãoAutorizadoPolícia", "OutrosAtaquesPolícia"* e *"EscutaPolícia"*. Quase no final da lista encontra-se *"RansomwarePolícia"* com 57,6%.

Por outro lado, o ataque com menor taxa de intenção de reporte é representado pela variável "*MalwarePolícia*", com apenas 49,1%.

No geral, os dados válidos sugeriram que mais da metade das empresas analisadas manisfestou intenção de reportar os ataques cibernéticos às autoridades competentes, caso estas fossem vítimas, o que refletiu uma tendência positiva em termos de conscientização e responsabilidade diante de crimes digitais.

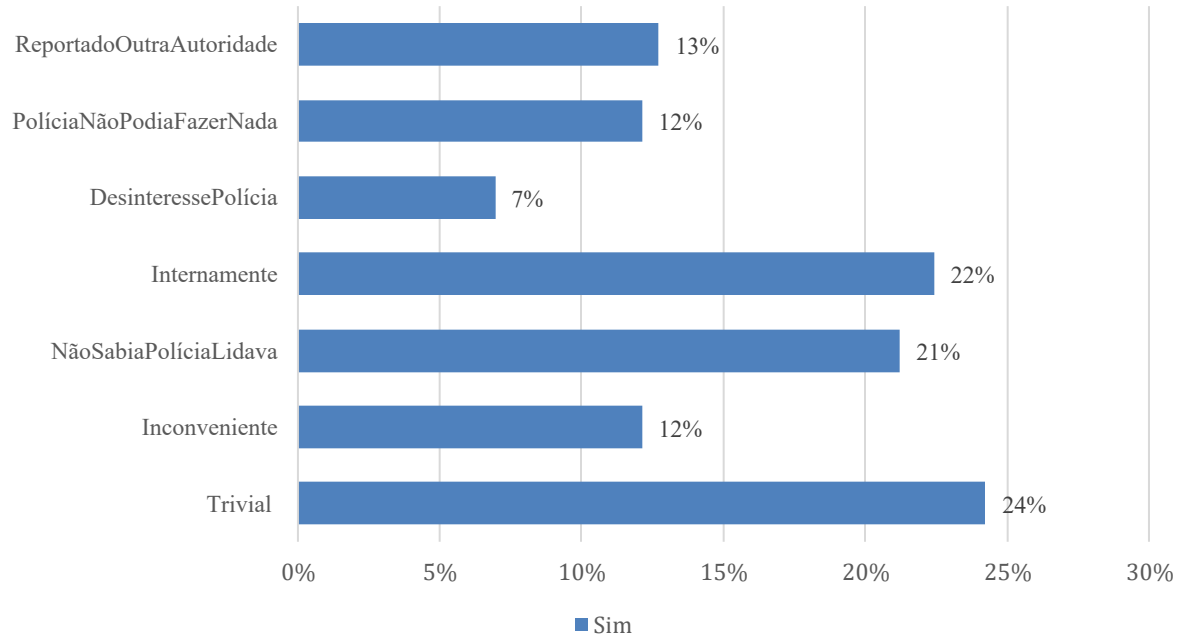

Figura 4.8 - Caracterização das variáveis referentes às Razões de Não Reporte

Seguidamente na Figura 4.8 foram apresentadas as variáveis relacionadas com as razões de não reporte de incidentes de cibersegurança às autoridades, ou seja, aos motivos indicados por aqueles que efetivamente não reportaram o incidente, permitindo compreender as barreiras que conduzem ao não reporte. É importante, em primeiro lugar, dizer que todas estas variáveis registaram uma elevada taxa de valores omissos de 67%, o que limita a generalização dos resultados e pode indicar algum constrangimento por parte das empresas em justificar a não comunicação destes incidentes. Ainda assim, a análise dos 33% de respostas válidas permitiu identificar padrões.

Entre as justificações mais frequentemente assinaladas, destacou-se a variável "*Trivial"*, em que 24% das empresas consideraram o ataque de menor importância, e sendo assim não se justificaria uma denúncia formal. Este dado sugeriu que uma parte dos inquiridos encarou determinados incidentes como pouco relevantes ou incapazes de provocar repercussões significativas na organização.

Em segundo lugar, surgiu a variável "*Internamente"*, com 22%, que revelou que algumas empresas optaram por gerir os incidentes dentro da própria estrutura, sem recorrer a entidades externas. Este comportamento pode estar associado à perceção de maior rapidez ou eficácia na resolução interna, mas também a preocupações com a imagem pública da organização perante terceiros.

Seguidamente, a variável "*NãoSabiaPolíciaLidava"*, com 21%, evidenciou uma falta de conhecimento sobre as competências das autoridades policiais em matéria de cibercrime. Foi possível verificar preocupações acerca do conhecimento e da formação dos colaboradores da empresa, pois indicou que uma parte das empresas não está ciente dos mecanismos institucionais de combate a este tipo de criminalidade, o que contribuiu para a subnotificação.

Outras razões apresentaram percentagens mais reduzidas, mas ainda relevantes. A variável "*ReportadoOutraAutoridade"* com 13%, mostrou que algumas empresas preferiram recorrer a outras entidades em vez da polícia. Já a variável "*PolíciaNãoPodiaFazerNada"*, apresentou uma percentagem de 12%, o que se traduziu numa perceção de ineficácia da intervenção policial, enquanto a variável "*Inconveniente"*, também com 12%, indicou que as algumas das empresas inquiridas consideraram o processo de denúncia demasiado burocrático, ou complexo e demorado.

A variável com menor significância foi a "*DesinteressePolícia"*, com apenas 7%, que sugeriu que são poucos os casos em que as empresas deixaram de reportar por acreditarem que a polícia não teria interesse em atuar.

No conjunto, estes resultados permitiram concluir que a subnotificação de ciberataques deveu-se principalmente a três fatores: a perceção de trivialidade, a tendência para resolução interna e o desconhecimento acerca do papel das autoridades competentes. Razões associadas a falta de confiança na polícia ou perceção de desinteresse apresentaram um impacto mais reduzido. Estes dados mostram que existe ainda uma significativa diferença entre a ocorrência

de cibercrimes e a comunicação destes às autoridades competentes, o que pode fragilizar o combate aos crimes informáticos.

4.2 Índice de Cibercrime

Tendo concluído a análise descritiva dos dados, o estudo avançou para uma análise de *clusters*, que tem por objetivo agrupar empresas com características semelhantes em relação ao seu perfil de ciberataques sofridos. Como descrito anteriormente, optou-se pela realização de uma análise de *clusters* hierárquica, especificamente aplicada ao Índice de Ciberataques, uma variável que sintetiza a ocorrência dos diferentes tipos de ataques estudados (Figura 4.9).

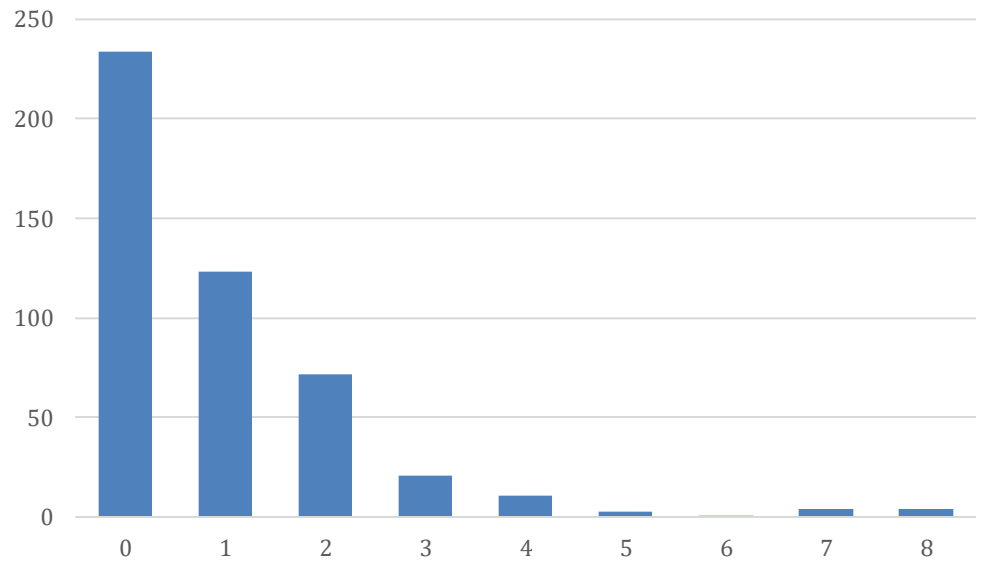

Figura 4.9 - Índice de Cibercrimes

Para realizar esta análise hierárquica, foi utilizado o método de Ward, um procedimento para minimizar a variância dentro dos grupos formados, que permite assim obter *clusters* mais homogéneos internamente e mais distintos entre si. Além disso, foi utilizada a distância euclidiana ao quadrado, que representa uma medida padrão para avaliar o nível de similaridade as empresas.

Como resultado desta análise hierárquica, foi obtido um dendrograma (Figura 4.10), que é um gráfico específico para ilustrar visualmente como as empresas se agrupam com base nas suas semelhanças relativas ao Índice de Ciberataques. O dendrograma revelou claramente a existência de três grupos distintos de empresas, permitindo identificar visualmente e intuitivamente quais empresas têm perfis semelhantes de exposição e ocorrência a ataques cibernéticos.

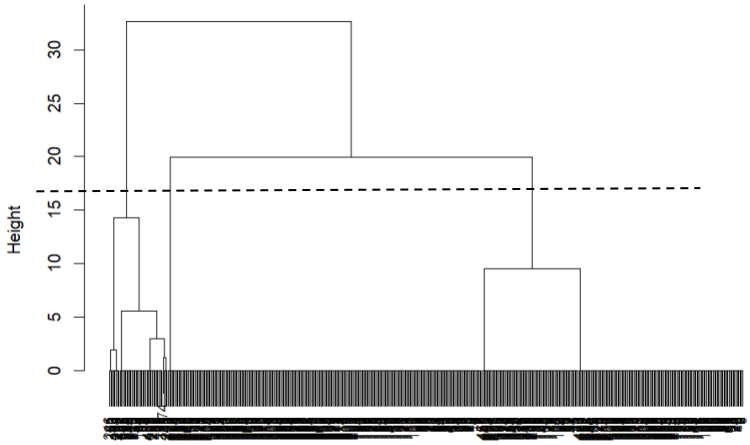

Figura 4.10 - Dendograma segundo o Método de Ward

4.3 Segmentação das Empresas pelo Índice de Cibercrime

Cada empresa foi atribuída a um dos três clusters, os quais foram caracterizados estatisticamente com base na média e no desvio padrão do índice. A divisão dos *clusters* foi feita da seguinte maneira (Figura 4.11): O *Cluster* 1 é inclui 195 empresas, o *Cluster* 2 que é o *cluster* de maior dimensão inclui 234 empresas e o *Cluster* 3 que comparativamente aos outros tem uma dimensão mais pequena inclui 44 empresas.

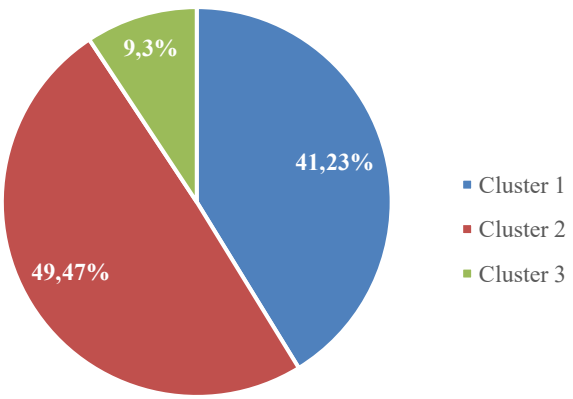

Figura 4.11 - Distribuição dos Clusters

- ***Cluster* 1**: Apresenta uma média de 1,37 e um desvio padrão de 0,48, o que indica um nível baixo de exposição a ciberataques.

- ***Cluster* 2**: Tem uma média e um desvio padrão de 0, o que significa que nenhuma das empresas deste cluster reportou incidentes, ou seja, é um perfil sem registo de ataques cibernéticos.

- ***Cluster* 3**: Regista uma média de 4,27, e um desvio padrão de 1,70, trata-se do grupo que sofreu um maior impacto quando se trata de crimes cibernéticos.

4.4 Caracterização dos Clusters de Cibercrime com as Variáveis Empresariais

Após a formação dos *clusters* com base no Índice de Ciberataques e à sua caracterização com base nesta variável de agrupamento, procedeu-se à avaliação da associação entre os *clusters* e as algumas variáveis de caracterização das empresas, nomeadamente o setor de atividade ("*SetorGrupo*"), os anos de atividade ("*AnosAtiv*"), o número de colaboradores ("*NColaboradores*") e o volume de negócios ("*Volume*"). O objetivo foi complementar a caracterização dos *clusters* e perceber se determinadas características estruturais ou operacionais das empresas estavam associadas de forma significativa ao risco de sofrer ataques cibernéticos.

Para esta análise recorreu-se ao V de Cramer, que se trata de uma medida de associação entre duas variáveis categóricas, serve para saber se existe, e/ou quão forte é uma relação entre essas variáveis, mesmo que não seja causal. Se o valor estiver próximo de 0 significa que a distribuição é igual entre os *clusters*, ou seja, não há relação. Caso o valor esteja perto de 1 a distribuição muda bastante entre os *clusters*, ou seja, as variáveis podem influenciar a formação dos *clusters*. De acordo com o Quadro 4.2, foi possível observar como se pode classificar as associações.

Quadro 4.2 - V de Cramer

Valor de V	Grau de Associação
0 - 0,1	Muito Fraca
0,1- 0,3	Fraca
0,3 - 0,5	Moderada
>0,5	Forte

Para aferir a existência de uma possível associação entre os *clusters* identificados e as variáveis de caracterização empresarial, foi inicialmente considerada a totalidade dos clusters

(*Clusters* 1, 2 e 3). Contudo, após uma análise preliminar dos resultados, verificou-se que as associações apresentavam valores muito baixos, indicando relações estatisticamente fracas ou nulas. Diante disso, optou-se por refinar a análise, restringindo-a apenas aos *Clusters* 1 e 3. Esta decisão fundamenta-se no facto de que são estes os *clusters* que registam casos efetivos de ataques cibernéticos, ao contrário do *Cluster* 2, que não apresenta ocorrências reportadas deste tipo. A nova análise focou-se na relação entre a pertença aos *Clusters* 1 e 3 e o conjunto das 4 variáveis empresariais, já mencionadas anteriormente.

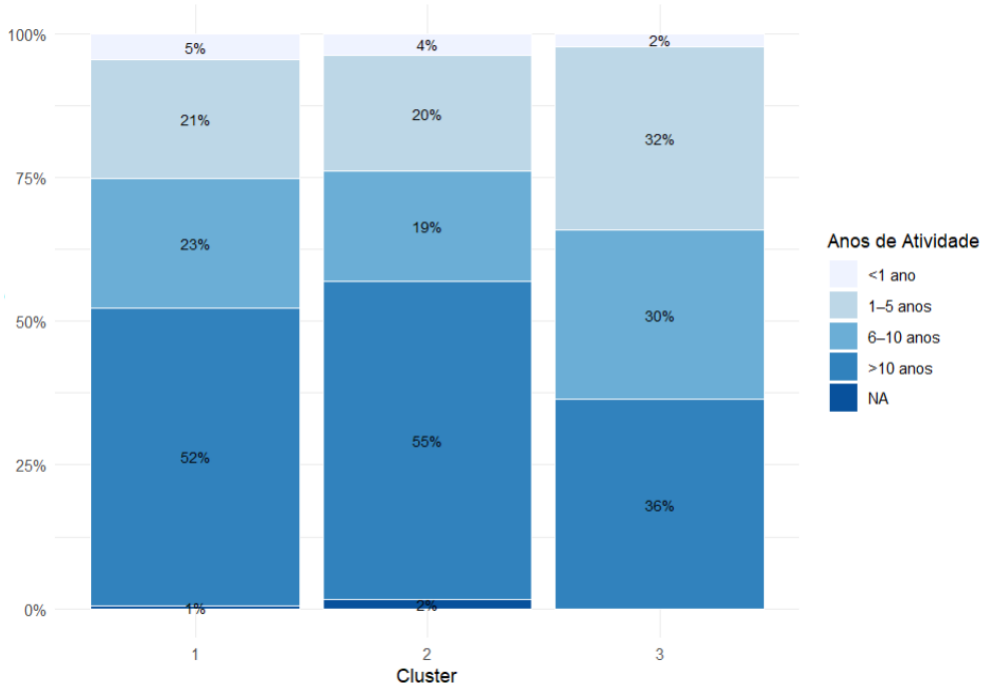

Figura 4.12 - Distribuição de Anos de Atividade dentro de cada cluster

De acordo com a Figura 4.12 e o Apêndice 8.D, é possível verificar a distribuição das empresas por categoria de anos de atividade, dentro de cada cluster. O *Cluster* 1 apresenta 5% de empresas com menos de 1 ano. De 1 a 5 anos e de 6 a 10 anos têm quase a mesma significância e apresentaram percentagens de 21% e 23% respetivamente. Já o grupo mais relevante é o das empresas com mais de 10 anos que representa 52%. O *Cluster* 2 comporta-se de forma semelhante ao *Cluster* 1, ou seja, com menos de 1 ano com 4%, as empresas com 1 a 5 anos e com 6 a 10 anos tem 20% e 19% respetivamente. E o grupo com mais importância é o de empresas com mais de 10 anos que têm uma representação de 55%.

No *Cluster* 3 as categorias estão melhor distribuídas, este *cluster* apresenta 2% para empresa com menos de 1 ano, 32% com 1 a 5 anos, 30% com 6 a 10 anos e 36% para empresas com mais de 10 anos. Em suma há uma predominância de empresas mais maduras nos *Clusters* 1 e 2 enquanto no *Cluster* 3 foi apresentada uma percentagem maior de empresas jovens.

Contudo, o V de Cramer calculado foi de 0,148, o que indica uma associação fraca entre os *clusters* e os anos de atividade. Assim, apesar das diferenças visuais no gráfico, não existe uma relação estatisticamente relevante entre estas duas variáveis.

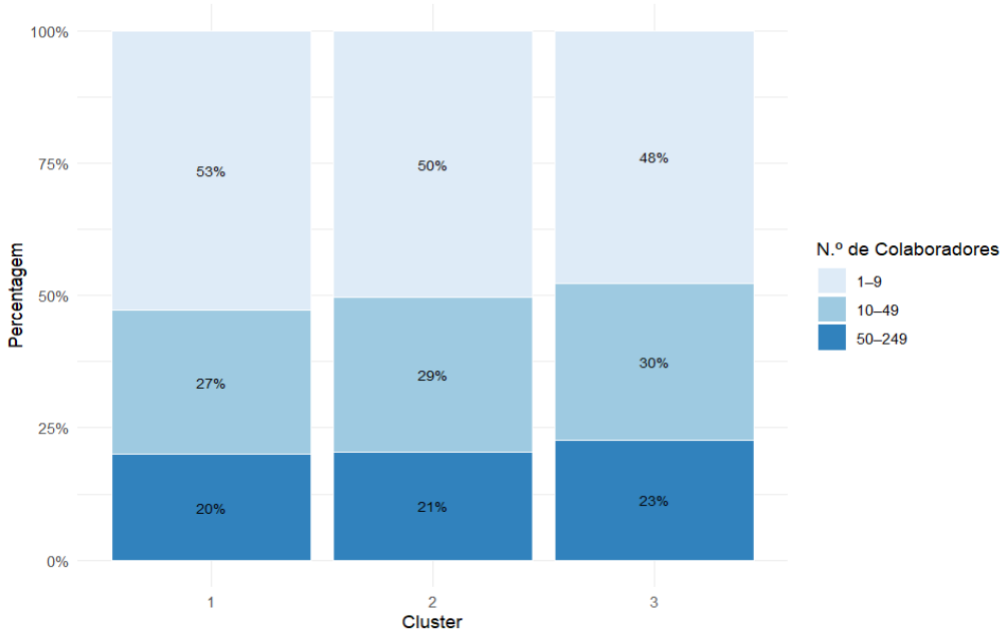

Figura 4.13 - Distribuição do Número de Colaboradores dentro de cada cluster

Seguidamente foi feita a análise com a variável "*NColaboradores*", para averiguar se o número de colaboradores de uma empresa está relacionado com os *clusters* definidos anteriormente. Segundo o Figura 4.13 e a Apêndice 8.E, é possível constatar relativamente à distribuição das empresas por número de colaboradores dentro de cada *cluster*, no *Cluster* 1, a maioria das empresas (53%) têm entre 1 a 9 colaboradores, 27% possuem 10 a 49 colaboradores e 20% têm 50 a 249 colaboradores. É possível concluir que existe uma predominância clara de pequenas empresas neste cluster. No *Cluster* 2 a distribuição é semelhante à do *Cluster* 1, com 50% das empresas com 1 a 9 colaboradores, 29% com 10 a 49, e 21% com 50 a 249.

No *Cluster* 3 representa a menor percentagem de microempresas, 48%, em comparação com os *Clusters* 1 e 2. Possui 30% de empresas com 10 a 49 colaboradores e 23% com 50 a 249 colaboradores. Neste grupo encontra-se a maior proporção de empresas maiores comparando aos outros *clusters*. E destaca-se ainda por ter uma composição ligeiramente mais distribuída entre as três categorias.

Apesar dessa variação, o V de Cramer foi de apenas 0,040, correspondendo a uma associação muito fraca. Isso significa que não existe evidência de que o número de colaboradores seja uma variável diferenciadora dos clusters.

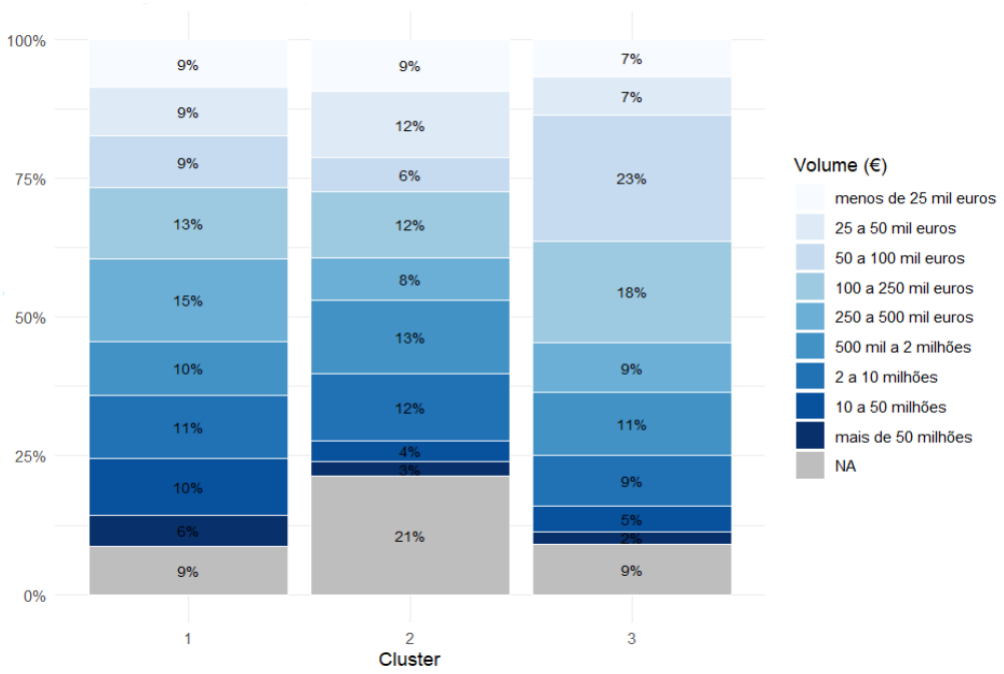

Figura 4.14 - Distribuição do Volume dentro de cada cluster

Posteriormente, procedeu-se à análise da variável "*Volume*", com o objetivo de perceber se os diferentes níveis de volume de negócios das empresas apresentam alguma relação com os *clusters* previamente definidos. Com base na Figura 4.14 e no Apêndice 8.F, observa-se a distribuição do volume dentro de cada *cluster*.

No *Cluster* 1, verifica-se uma distribuição relativamente homogénea entre as diferentes faixas de volume, embora sobressaiam as empresas com volumes de 250 a 500 mil euros, com 15%, e de 100 a 250 mil euros com 13%. Este *cluster* caracteriza-se, assim, por uma predominância de empresas com volumes médios.

Relativamente ao *Cluster* 2, destacam-se as categorias de 500 mil a 2 milhões de euros com 13%, seguida das categorias de 2 a 10 milhões de euros, de 100 a 250 mil euros e de 25 a 50 mil de euros, as três cada uma com 12%. Em suma este *cluster* agrega, portanto, um perfil de empresas mais diversificado, tanto com empresas de porte mais pequeno como empresas com maiores volumes.

Já o *Cluster* 3 distingue-se por apresentar a maior percentagem nas faixas de 50 a 100 mil euros com 23% e de 100 a 250 mil euros com 18%, o que sugere que este grupo é constituído maioritariamente por empresas com volumes de negócios pequenos e médios.

Apesar destas diferenças, o V de Cramer obtido foi de 0,213, que corresponde a uma associação fraca. Ou seja, não se pode afirmar que o volume de negócios tenha influência significativa na formação dos clusters.

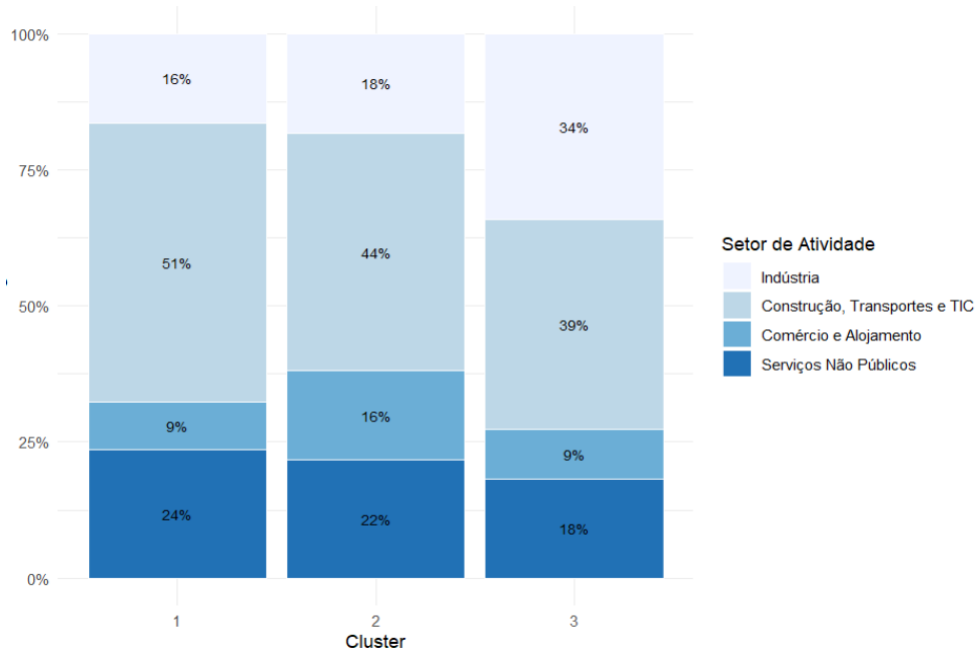

Figura 4.15 - Distribuição do Setor de Atividade dentro de cada cluster

A última variável qualitativa ordinal analisada foi a "*SetorGrupo*" que está relacionada com os setores de atividade. Foi elaborada uma tabela de contingência com vista a analisar a distribuição dos diferentes setores de atividade pelos *clusters* identificados. Observa-se que os grupos Serviços Públicos, e Agricultura e Pescas não possuem qualquer empresa.

Segundo a Figura 4.15 e o Apêndice 8.G, verifica-se que o *Cluster* 1 é dominado pelo setor da Construção, Transportes e TIC, que representa 51% das empresas deste grupo com 100 empresas. Segue-se o setor dos Serviços Não Públicos, com 24%, enquanto a Indústria assume um peso de 16% e o Comércio e Alojamento apresenta-se com 9% representativo de 17 empresas.

O *Cluster* 2 apresenta uma distribuição um pouco mais equilibrada, embora também com destaque para o setor da Construção, Transportes e TIC com 44%. O Comércio e

Alojamento ganhou aqui maior relevância, atingindo 16%, enquanto a Indústria representa 18%. Os Serviços Não Públicos estão presentes em 22%.

Já o *Cluster* 3 evidencia um perfil industrial, sendo a Indústria responsável por 34% das empresas, mas apesar disto o setor da Construção, Transportes e TIC aparece com maior representatividade com uma percentagem de 39%. O Comércio e Alojamento e os Serviços Não Públicos têm representações bastante inferiores, com apenas 9% e 18%, respetivamente.

Neste caso, o V de Cramer registou o valor de 0,175, classificando-se como uma associação fraca. Assim, apesar de se verificarem diferenças na distribuição setorial, estas não são estatisticamente significativas.

Quadro 4.3 – Classificação das Associações de V de Cramer

Variável	V de Cramer	Grau de Associação
SetorGrupo	0,175	Fraca
AnosAtiv	0,148	Fraca
NColaboradores	0,040	Muito Fraca
Volume	0,213	Fraca

Em síntese, os resultados da análise através do V de Cramer (Quadro 4.3 e o Apêndice 8.H) mostram que todas as variáveis consideradas, "SetorGrupo", "AnosAtiv", "NColaboradores" e "Volume", apresentaram associações fracas ou muito fracas com os clusters. Isto indica que estas variações não são estatisticamente relevantes.

Deste modo, foi possível concluir que o fenómeno dos ataques cibernéticos não se encontra condicionado por características estruturais específicas das empresas, como dimensão, maturidade, volume de negócios ou o setor onde atua.

Pelo contrário, os resultados reforçaram que qualquer empresa, independentemente do seu perfil, pode ser alvo de ataques cibernéticos, o que evidenciou que o fenómeno de cibercrime é transversal.

4.5 Caracterização dos Segmentos por Tipo de Ataques mais Frequentes

Foi realizada uma análise da frequência dos sete tipos de ataques cibernéticos nos *Clusters* 1 e 3, definidos anteriormente com base no índice de ciberataques.

A visualização apresentada na Figura 4.16 permite identificar rapidamente os tipos de ataque mais prevalentes em cada grupo e reforça a necessidade de estratégias diferenciadas de proteção.

Os resultados mostram que, no *Cluster* 3, os ataques mais frequentes são *malware* (79,5%), acesso não autorizado (70,5%) e *phishing* (56,8%). Já no *Cluster* 1, estes valores são substancialmente inferiores: 32,3%, 20% e 24,6%, respetivamente.

De forma geral, o *Cluster* 3 apresenta percentuais significativamente mais elevados em todos os tipos de ataques analisados, sugerindo uma maior exposição ou vulnerabilidade a incidentes cibernéticos. Por exemplo, 79,5% das empresas no *Cluster* 3 reportaram ocorrência de *malware*, comparado com apenas 32,3% no *Cluster* 1.

Além disso, outras categorias demonstram discrepâncias igualmente relevantes. Ataques associados a compromisso online são quatro vezes mais frequentes no *Cluster* 3 (45,5%) do que no *Cluster* 1 (11,3%), enquanto incidentes relacionados com *ransomware* também evidenciam um contraste acentuado, atingindo 47,7% no *Cluster* 3 face a 13,8% no *Cluster* 1. O mesmo padrão é observado nos ataques de negação de serviço, que afetam 38,6% das organizações do *Cluster* 3, comparativamente a 9,7% no *Cluster* 1.

Este conjunto de resultados evidencia um comportamento consistente: o *Cluster* 3 regista sempre valores entre duas a quatro vezes superiores aos observados no *Cluster* 1. Isto sugere que as organizações deste grupo apresentam maior superfície de ataque, práticas de segurança menos robustas ou menor maturidade operacional no âmbito da cibersegurança.

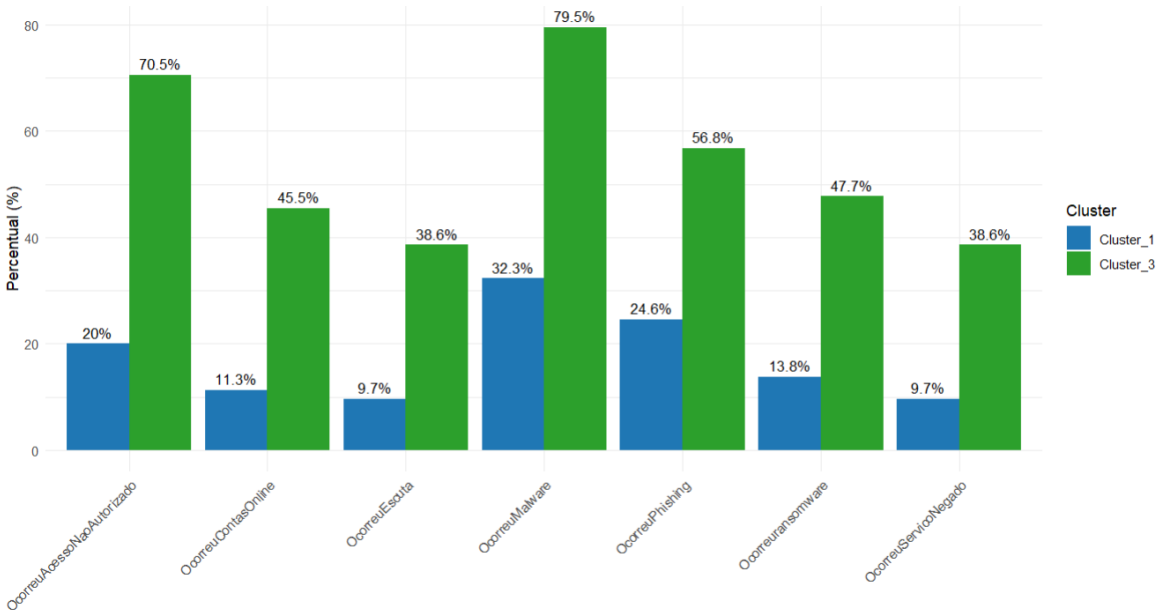

Figura 4.16 – Tipos de Ataques Cibernéticos por Cluster

4.6 Segmentos de Cibercrime e a Intenção de Reporte às Autoridades

Após a análise inicial dos clusters identificados no estudo, a investigação avançou para explorar de forma mais aprofundada as dinâmicas relacionadas às denúncias de incidentes de ciberataques às autoridades policiais. Para esta fase da pesquisa, a atenção concentrou-se primeiramente no *Cluster* 3 e posteriormente no *Cluster* 1.

Estes grupos foram os selecionados porque agregam as empresas com incidência de ciberataques entre os *clusters* analisados, apresentando assim um cenário particularmente relevante para o estudo das práticas de reporte de incidentes. Começou-se pela análise do *Cluster* 3 porque é o que tinha maior incidência de ataques cibernéticos.

O objetivo desta etapa foi compreender, em detalhe, com que frequência e sob que circunstâncias as empresas do *Cluster* 3 reportaram os diferentes tipos de incidentes cibernéticos às autoridades policiais. A análise foi conduzida com base nas variáveis derivadas da questão Q10_b do inquérito, a qual permitiu identificar, para cada tipo específico de incidente, se haveria ou não a intenção de reportar o caso à polícia.

Optou-se por utilizar a Q10_b (intenção de reportar) em vez da Q10_a (comportamento efetivo de reportar), pois nem todos os participantes vivenciaram situações em que pudessem efetivamente reportar, e desta forma, a variável de intenção garantiu uma amostra maior, enquanto a Q10_a teria poucos dados com os quais trabalhar.

As variáveis analisadas foram: "*MalwarePolícia*" (incidentes de malware), "*ServicoNegadoPolícia*" (ataques de interrupção ou negação de serviço), "*ContasOnlinePolícia*" (acesso não autorizado a contas bancárias online), "*PhishingPolícia*" (ataques de *phishing*), "*RansomwarePolícia*" (ataques de *ransomware*), "*AcessoNãoAutorizadoPolícia*" (acesso indevido a sistemas), "*EscutaPolícia*" (escuta ilegal de comunicações) e "*OutrosAtaquesPolícia*" (outros tipos de ataques não especificados anteriormente).

Com estas variáveis, foi possível avaliar a intenção de reporte face à de não reporte à polícia para cada uma das tipologias de ataque referidas. Para ilustrar de forma clara esta comparação, foi desenvolvida a Figura 4.17, que apresenta visualmente as taxas de notificação para cada tipo de incidente.

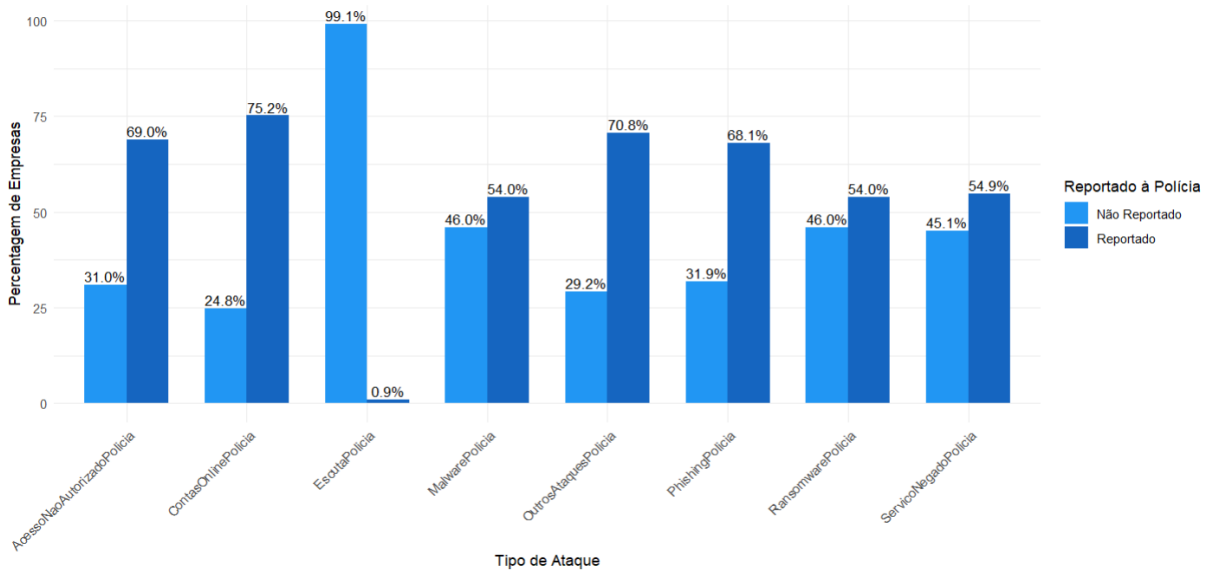

Figura 4.17 - Intenção de Reporte à Polícia no Cluster 3

A análise dos dados revelou que o ataque mais frequentemente reportado pelas empresas do *Cluster* 3 foi o de acesso indevido a contas bancárias online, correspondente à variável "*ContasOnlinePolícia*", que registou uma taxa de intenção de reporte de 75,2%. Este resultado evidenciou uma preocupação significativa das organizações com este tipo específico de violação, possivelmente devido ao elevado impacto financeiro direto e à facilidade de identificar perdas concretas associadas a este incidente. Logo a seguir, destacaram-se as variáveis "*OutrosAtaquesPolícia*" com 70,8%, "*AcessoNãoAutorizadoPolícia*" com 69% e "*PhishingPolícia*" com 68,1%, que também apresentaram percentagens bastante elevadas de notificação às autoridades. Estes resultados sugeriram que, para além dos incidentes

diretamente ligados a perdas financeiras, outros tipos de ataques considerados graves ou recorrentes foram igualmente alvo de reporte formal.

Por outro lado, ataques do tipo negação de serviço (DoS), representados pela variável "*ServiçoNegadoPolícia*", foram reportados por 54,9% das empresas do *cluster*, valor que, embora ainda acima da metade, foi substancialmente inferior ao dos incidentes anteriormente mencionados. No mesmo nível situaram-se os ataques de *ransomware* e *malware*, ambos com uma taxa de intenção de reporte de 54%, demonstrando que, apesar do seu potencial destrutivo, o reporte destes incidentes não foi tão consensual entre as empresas quanto no caso de acessos indevidos a contas bancárias ou ataques de *phishing*.

A tipologia de ataque que apresentou a taxa de intenção de reporte mais baixa foi a de "*EscutaPolícia*", com apenas 0,9% das empresas a indicar que notificaria as autoridades policiais em caso deste tipo de incidente, o que significou que uma percentagem significativa de 99,1% das organizações não considerariam reportar tal ocorrência.

De forma geral, observou-se que a maioria das tipologias de ataque analisadas apresentou taxas de intenção de reporte superiores a 50%, à exceção das escutas ilegais. Esta exceção podia estar associada à falta de sensibilização relativamente à gravidade deste tipo de crime, ou ainda à ausência de protocolos claros para lidar com este tipo de situação.

Em contraste, ataques que têm um impacto operacional ou financeiro direto e mensurável, como o *phishing* ou o comprometimento de contas bancárias online, foram mais prontamente notificados, uma vez que geram consequências imediatas e, muitas vezes, exigem ação rápida para limitar danos.

Dando continuidade à investigação, procedeu-se à realização da mesma análise relativamente ao *Cluster* 1, que corresponde ao segundo grupo com maior número de registos de ciberataques identificados no estudo. Esta análise procurou avaliar, tal como no *Cluster* 3, o padrão de intenção de reporte de incidentes às autoridades policiais por parte das empresas pertencentes a este *cluster*.

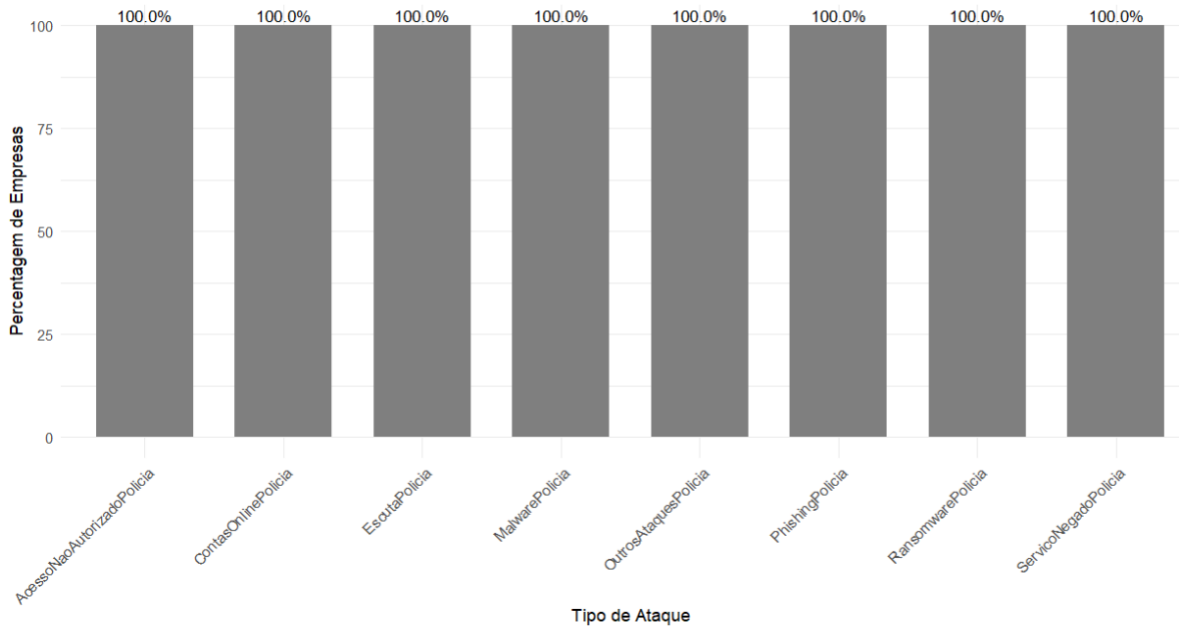

Figura 4.18 - Intenção de Não Reporte à Polícia no Cluster 1

A partir dos dados apresentados na Figura 4.18, foi possível constatar um resultado distinto e de particular relevância: em contraste com o observado no grupo anterior, nenhuma das empresas do *Cluster* 1 declarou ter a intenção de reportar formalmente qualquer tipo de incidente às autoridades policiais.

Este resultado levantou questões importantes sobre as práticas de gestão e resposta a incidentes neste segmento de organizações, o que sugeriu dinâmicas distintas. A diferença em relação ao comportamento de intenção de reporte identificado no *Cluster* 3 evidenciou que a abordagem à notificação de incidentes às autoridades não é uniforme entre os diversos clusters analisados.

Esta constatação será explorada de forma mais aprofundada na secção seguinte, onde serão analisados os fatores subjacentes a esta ausência de intenção de reporte, permitindo assim uma compreensão mais completa dos motivos que levam as empresas do *Cluster* 1 a não terem a intenção de notificar formalmente as autoridades policiais em caso de ciberataques.

Quadro 4.4 – Intenção de Reporte dos Ataques à Polícia

Tipos de Ataques	Intenção de Reporte à Polícia	
	Cluster 3	Cluster 1
AcessoNãoAutorizadoPolícia	69%	0%
ContasOnlinePolícia	75,20%	0%
EscutaPolícia	0,90%	0%
MalwarePolícia	54,00%	0%
OutrosAtaquesPolícia	70,80%	0%
PhishingPolícia	68,10%	0%
RansomwarePolícia	54,00%	0%
ServiçoNegadoPolícia	54,90%	0%

Em síntese, segundo o Quadro 4.4, a comparação entre os *Clusters* 3 e 1 evidenciou realidades bastante distintas no que diz respeito à intenção de reporte às autoridades policiais. Enquanto as empresas do *Cluster* 3 demonstraram uma predisposição significativa para notificar incidentes, sobretudo quando envolvem perdas financeiras diretas ou riscos operacionais claros, como no caso do acesso não autorizado a contas online ou ataques de *phishing*, as organizações do *Cluster* 1 revelaram uma ausência total de intenção de reporte em todas as tipologias de ataque analisadas.

Este contraste sugeriu não apenas diferentes níveis de sensibilização e maturidade em termos de resposta a incidentes cibernéticos, mas também possíveis divergências na perceção de risco, nas práticas de gestão ou na confiança nas autoridades policiais. Assim, confirmou-se que a intenção de reportar os incidentes não é homogénea entre os *clusters*, constituindo um aspeto crítico para compreender as barreiras e motivações que moldaram o comportamento organizacional face ao cibercrime.

4.6 Razões de Não Reporte dos Eventos de Cibercrime às Autoridades

Com base nas variáveis obtidas a partir da questão Q11, foi realizada uma análise detalhada das motivações apresentadas pelas empresas para não reportarem os ciberataques às autoridades

policiais. Esta análise considerou um conjunto abrangente de opções, incluindo: classificação do incidente como trivial, perceção de inconveniência no processo de denúncia, desconhecimento de que a polícia estaria habilitada a lidar com tais situações, decisão de resolver o problema internamente, desinteresse atribuído à polícia, convicção de que a polícia não teria capacidade de intervir e, por fim, a possibilidade de o incidente ter sido reportado a outra autoridade distinta da polícia.

Para permitir uma compreensão mais granular do fenómeno da subnotificação, os resultados foram segmentados entre os *Clusters* 1 e 3, que como visto anteriormente, são precisamente aqueles que apresentaram registos de empresas vítimas de ciberataques. Esta segmentação revelou diferenças importantes entre os dois grupos no que respeita às razões invocadas para não proceder ao reporte formal dos incidentes.

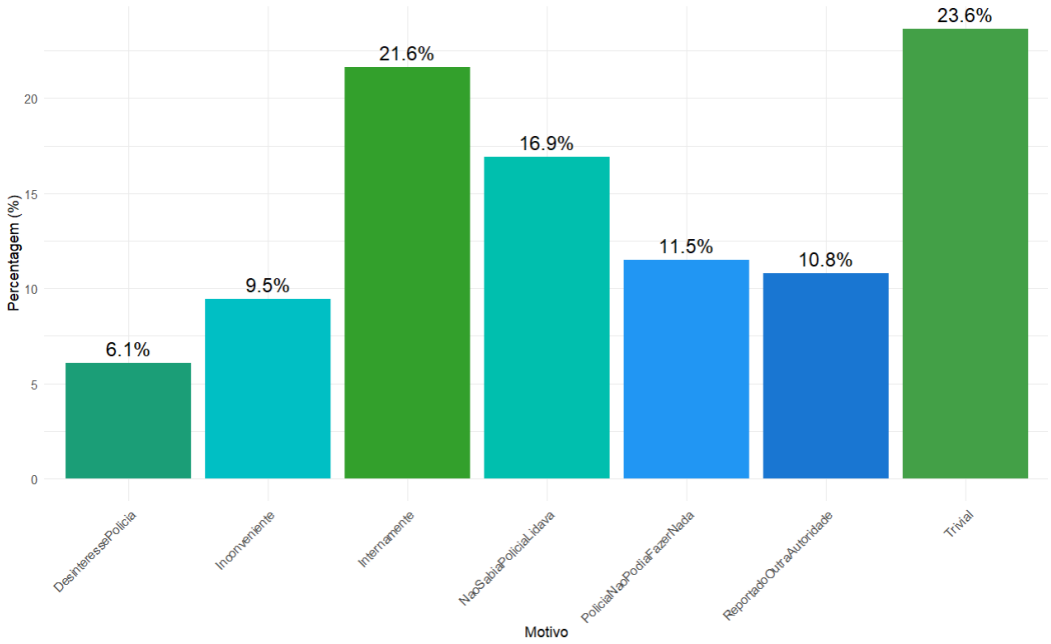

Figura 4.19 - Razões para Não Reportar à Polícia no Cluster 1

No que diz respeito ao *Cluster* 1 (Figura 4.19), observa-se que as principais motivações referidas para a não comunicação dos incidentes à polícia centram-se, sobretudo, na perceção de irrelevância dos ataques e na preferência por soluções internas.

O motivo mais apontado pelas empresas deste grupo foi a consideração do incidente como trivial com uma percentagem de 23,6%, o que indica uma tendência para minimizar o impacto de determinados ciberataques ou, eventualmente, a perceção de que os danos não justificam um procedimento formal de denúncia.

Em segundo lugar, destaca-se a decisão de resolver o incidente internamente com 21,6%, sugerindo uma preferência por manter o controlo sobre a situação dentro da própria organização, evitando, assim, potenciais exposições externas ou eventuais consequências reputacionais.

Também merecem destaque o desconhecimento de que a polícia poderia efetivamente atuar nestas situações que está representado com 16,9%, bem como a perceção de que a polícia não teria capacidade de intervir com 11,5% e a opção pelo reporte a uma outra autoridade competente com 10,8%. Estes dados evidenciam que, para uma parte significativa das empresas, persistem dúvidas quanto ao papel das autoridades policiais na resposta a cibercrimes, ou mesmo uma falta de confiança na sua capacidade de resposta. As motivações ligadas à inconveniência do processo com 9,5% e ao desinteresse atribuído à polícia com 6,1%, surgem com menor expressão, mas ainda assim refletem barreiras que dificultam o reporte.

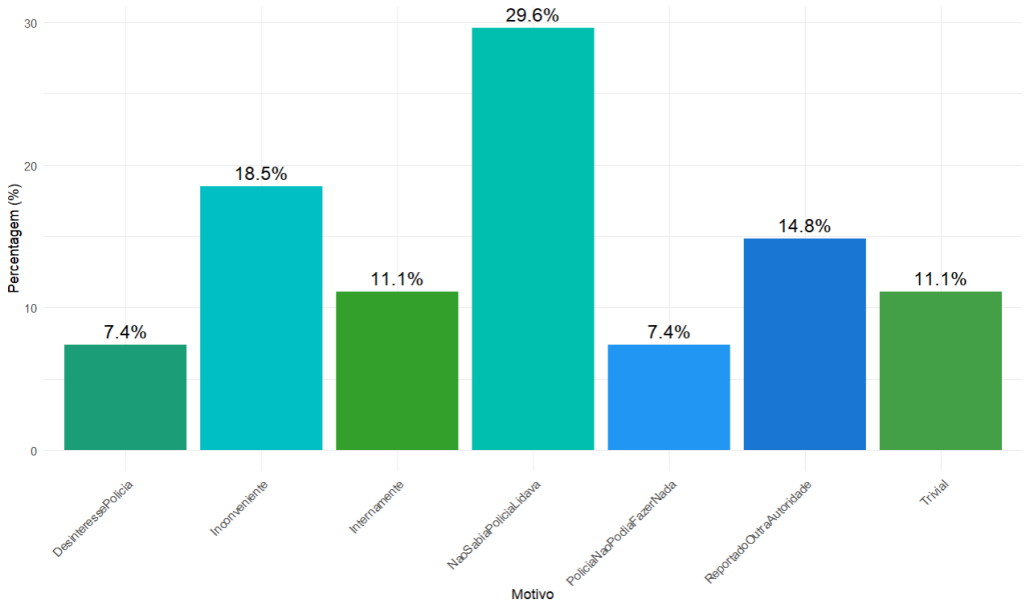

Figura 4.20 - Razões para Não Reportar à Polícia no Cluster 3

No *Cluster* 3 (Figura 4.20), por sua vez, o perfil das respostas revela algumas diferenças significativas. Neste grupo, a principal razão apresentada para não reportar os ciberataques foi o desconhecimento de que a polícia estaria preparada para lidar com este tipo de crime, com uma expressiva percentagem de 29,6%. Este dado indica uma lacuna importante na comunicação e sensibilização, apontando para a necessidade de informar melhor as organizações sobre as competências das autoridades policiais no domínio do cibercrime.

Em seguida, surge a perceção de inconveniência com 18,5%, o que sugere que, para muitas empresas, o processo de denúncia é visto como burocrático ou que pode trazer problemas reputacionais, constituindo um obstáculo prático significativo.

A opção por resolver internamente o problema foi referida por 11,1% das empresas, valor inferior ao observado no *Cluster* 1, o que pode indicar uma maior predisposição deste grupo para recorrer a entidades externas em caso de necessidade.

O incidente ser considerado trivial com 11,1%, a preferência por reportar a outra autoridade com 14,8%, bem como fatores relacionados com a falta de confiança na atuação policial, designadamente o desinteresse da polícia e a perceção de que nada poderia ser feito, ambos com 7,4%, também foram mencionados, ainda que com menor frequência.

Comparando os dois *clusters*, é possível identificar tendências distintas: enquanto no *Cluster* 1 predomina a tendência para desvalorizar os incidentes ou gerir internamente as respostas, no *Cluster* 3 sobressai de forma clara a falta de informação quanto ao papel da polícia e os obstáculos práticos associados ao reporte. Apesar das diferenças, em ambos os grupos subsiste uma fatia relevante de empresas que aponta questões de confiança e preferências por outras entidades como fatores determinantes para não comunicar os incidentes às autoridades policiais.

Capítulo 5 | Conclusões

A presente investigação teve como objetivo central analisar a incidência de cibercrime nas empresas portuguesas, identificar padrões de exposição a ataques e compreender os fatores determinantes para a intenção de reporte, ou para a ausência da intenção de reporte, destes incidentes às autoridades competentes.

Para tal, recorreu-se aos dados do questionário *Flash Eurobarometer 496* (Comissão Europeia, 2021) e a uma metodologia baseada na análise de *clusters* hierárquica, o que permitiu segmentar o universo empresarial nacional em grupos distintos de acordo com o seu nível de exposição ao fenómeno dos ciberataques.

A construção de um Índice de Ciberataques, resultante da soma dos ataques ocoridos, possibilitou a identificação de três *clusters* com características diferenciadas. O *Cluster* 3 destacou-se por uma maior vulnerabilidade, reunindo assim as empresas que registaram o número mais elevado de incidentes, o Cluster 1 apresentou uma média substancialmente mais baixa, enquanto o *Cluster* 2 foi caracterizado por reunir as empresas que não sofreram qualquer tipo de ataque cibernético.

Os incidentes de cibersegurança experienciados pelas empresas foram, sobretudo *malware*, *phishing* e acessos não autorizados. Contudo, verificou-se uma discrepância marcante entre a ocorrência de ataques e o respetivo reporte, ou seja, nem todos os incidentes experienciados foram comunicados às autoridades.

No que respeita à intenção de reporte, observou-se que as taxas eram razoáveis no *Cluster* 3, excepto no caso das escutas, mas inexistentes no *Cluster* 1, o que evidenciou um problema de subnotificação no contexto português.

As razões apontadas para a ausência de comunicação às autoridades variaram consoante o grupo. No *Cluster* 1, predominaram a perceção de trivialidade dos ataques, a opção pela resolução interna e o desconhecimento relativamente às competências policiais neste domínio. Já no *Cluster* 3 destacaram-se a inconveniência de reportar e a falta de consciência de que a polícia lidava com este tipo de crimes.

Em síntese a partir destes resultados é possível concluir que existe uma cultura organizacional ainda marcada pela desvalorização do risco e pela ausência de práticas sistemáticas de reporte. Constatou-se, assim, que a subnotificação de ciberataques constitui um

obstáculo relevante à compreensão do impacto real do cibercrime nas empresas portuguesas, o que compromete a produção de estatísticas fidedignas e limitando a eficácia das políticas públicas de prevenção e resposta.

O envolvimento ativo das empresas no reporte é uma condição indispensável para uma resposta nacional mais eficaz e para o desenvolvimento de estratégias adequadas ao contexto português. Os dados agora analisados evidenciam, por isso, desafios claros em matéria de comunicação, confiança institucional e operacionalização do reporte, sublinhando a necessidade de uma abordagem integrada que promova o diálogo entre setor privado e autoridades e que fomente práticas consistentes e informadas em todo o tecido empresarial.

A análise estatística realizada demonstrou, adicionalmente, que não existem associações estatisticamente significativas entre o grau de exposição ao cibercrime e as variáveis estruturais como o setor de atividade, o número de colaboradores, o volume de negócios ou os anos de existência. Assim foi possível afirmar que o cibercrime é um fenómeno transversal, que afeta empresas de diferentes dimensões, áreas de atuação e níveis de maturidade, exigindo, por isso, respostas integradas e abrangentes. Importa ainda destacar a relevância de aprofundar futuras investigações, considerando variáveis complementares como o grau de digitalização das empresas e o tipo de soluções de segurança adotadas, de modo a ampliar a compreensão dos fatores que potenciam ou mitigam a exposição ao cibercrime.

Em síntese, este estudo contribui para o conhecimento do panorama atual do cibercrime no contexto empresarial português, para a persistência da subnotificação e para a necessidade urgente de medidas proativas que aumentem a resiliência digital. Apenas através de uma abordagem concertada, envolvendo empresas, autoridades e decisores políticos, será possível reforçar a proteção do tecido empresarial nacional face aos desafios crescentes do ciberespaço. Para inverter este cenário, seguidamente serão mencionadas algumas recomendações.

5.1 Recomendações

À luz dos resultados obtidos nesta investigação, é possível identificar um conjunto de recomendações estratégicas que visam reforçar a cibersegurança no tecido empresarial português, particularmente junto das pequenas e médias empresas, e contribuir para a mitigação das principais fragilidades identificadas, com especial destaque para a elevada subnotificação dos incidentes cibernéticos.

Em primeiro lugar, destaca-se a necessidade de reforçar a sensibilização e a formação em cibersegurança. Uma parte significativa das empresas inquiridas revelou falta de conhecimento relativamente aos riscos e procedimentos associados à denúncia de ciberataques, o que contribui para a perceção de trivialidade dos incidentes e para a tendência de resolver internamente as ocorrências.

Neste sentido, recomenda-se a implementação de campanhas nacionais de sensibilização, com iniciativas direcionadas ao setor empresarial, recorrendo a diversos canais de comunicação, como a televisão, as redes sociais e a imprensa. Estas campanhas deverão ser complementadas por ações regulares de formação para gestores e colaboradores, com enfoque na identificação de ameaças comuns, como por exemplo os tipos de engenharia social e os tipos de *malware*, bem como no desenvolvimento de respostas adequadas.

Adicionalmente, a elaboração de guias práticos, com linguagem acessível e orientados para as pequenas e médias empresas, poderá facilitar a tradução dos conceitos técnicos em procedimentos concretos e eficazes no dia a dia das organizações.

Em segundo lugar, torna-se imprescindível o reforço das medidas internas de segurança nas empresas. A definição de políticas claras para o uso de dispositivos, gestão de palavras-passe e controlo de acessos deve ser uma prioridade, garantindo simultaneamente a atualização regular de todos os sistemas.

Recomenda-se, ainda, a realização periódica de auditorias de cibersegurança, com o objetivo de identificar e mitigar vulnerabilidades existentes. Importa sublinhar a relevância da adoção de ferramentas básicas, mas eficazes, como *firewalls*, antivírus, sistemas de autenticação multifator e backups automáticos, bem como a promoção de parcerias que facilitem o acesso das PME a serviços especializados de cibersegurança a custos ajustados. As políticas de segurança deverão, sempre que possível, ser personalizadas em função da dimensão, setor e perfil de risco de cada organização, de modo a garantir uma proteção eficaz e proporcional.

A facilitação do reporte e da denúncia de cibercrimes constitui igualmente uma prioridade, sobretudo face à subnotificação identificada. A criação de uma linha de apoio específica, acessível e anónima, permitiria ultrapassar alguns dos receios mais frequentemente manifestados pelas empresas, nomeadamente os relacionados com a reputação ou possíveis retaliações.

Para além disso, esta linha de apoio podia estar ligada a uma plataforma digital centralizada, gerida por entidades como a Polícia Judiciária ou até mesmo o Centro Nacional de Cibersegurança de Portugal, onde as empresas possam denunciar incidentes, consultar informação relevante e aceder a recursos de apoio. É igualmente fundamental garantir que as entidades que reportam recebam feedback sobre as denúncias efetuadas, compreendendo o destino dos dados e recebendo orientações para prevenção de futuros incidentes.

A promoção de uma cultura de colaboração e partilha de informação assume particular relevância num contexto de ameaças em constante evolução. Sugere-se, por isso, a criação de parcerias público-privadas, envolvendo o governo, associações empresariais e grandes empresas tecnológicas que permitam a troca de experiências para que em conjunto possam solucionar melhor os ataques e criar estratégias para se prevenirem dos mesmos.

Outra recomendação diz respeito à introdução de mecanismos de certificação em cibersegurança, que poderá, servir de incentivo ao cumprimento das melhores práticas e reconhecer publicamente o esforço das empresas mais diligentes neste domínio. A existência de certificações reconhecidas poderá funcionar como um selo de confiança no mercado, valorizando as organizações que investem seriamente na proteção dos seus sistemas e dados. Para além de promover uma cultura de responsabilidade e melhoria contínua, este tipo de mecanismo pode ainda estimular a competitividade saudável entre empresas, contribuindo para o aumento geral dos níveis de segurança digital no tecido empresarial nacional.

Finalmente, importa salientar a importância da promoção de uma cultura organizacional de segurança e confiança. A denúncia de incidentes deve ser encarada como um ato de responsabilidade e não como sinal de fraqueza. Neste contexto, sugere-se a inclusão de conteúdos de cibersegurança nos canais de comunicação, bem como a divulgação de exemplos de sucesso de empresas que, através da adoção de boas práticas, conseguiram superar ciberataques. Este esforço de normalização contribuirá para desmistificar o fenómeno e incentivar uma atitude mais proativa e colaborativa por parte das organizações.

Por último, recomenda-se que o estudo e a monitorização do fenómeno sejam contínuos, promovendo a análise sistemática de novos dados sobre o impacto dos ciberataques. Esta atualização permitirá ajustar as políticas e estratégias, promovendo um ambiente empresarial mais resiliente para os desafios da era digital.

Capítulo 6 | Referências

Abikoye, O.C., Abubakar, A., Dokoro, A.H. *et al.* A novel technique to prevent SQL injection and cross-site scripting attacks using Knuth-Morris-Pratt string match algorithm. *EURASIP J. on Info. Security* 2020, 14 (2020). https://doi.org/10.1186/s13635-020-00113-y

Alam, S. (2022). *Cybersecurity: Past, present and future* (Versão rev. 3, arXiv:2207.01227). arXiv. https://doi.org/10.48550/arXiv.2207.01227

Anderson, R., Barton, C., Bohme, R., Clayton, R., van Eeten, M., Levi, M., ... & Savage, S. (2019). Measuring the costs of cybercrime. *Journal of Cybersecurity, 5*(1), 1-20. https://doi.org/10.1093/cybsec/tyz015

Ansori, A., Damyati, F., & Dhestyani, S. A. (2023). *Mitigation of malware ransomware virus*. ResearchGate.https://www.researchgate.net/publication/384274065_Mitigation_of_Malware_Ransomware_Virus

Campelo, E., Junior, A., Volny, C. do N., & Santos, F. V. dos. (2020). *Crimes virtuais: Uma abordagem jurídica sobre os crimes cibernéticos e seus mecanismos de prevenção*. Revista de Direito e Segurança, 1(2). https://doi.org/10.35265/2236-6717-201-9042

Centro Nacional de Cibersegurança (2023). *Relatório de riscos e conflitos no ciberespaço*. https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs15m.pdf

Centro Nacional de Cibersegurança. (2024). *Riscos e conflitos no ciberespaço 2024* (Relatório OBCiber-CNCS). https://www.cncs.gov.pt/docs/rel-riscosconflitos2024-obcibercncs15m.pdf

CNN Portugal. (2022, 28 de abril). *Ataque informático: Garcia de Orta garante que os dados dos utentes não foram comprometidos*. https://cnnportugal.iol.pt/hospital-garcia-de-orta/almada/ataque-informatico-garcia-de-orta-garante-que-os-dados-dos-utentes-nao-foram-comprometidos/20220428/626ae48b0cf26256cd2130ac

CNPD (Comissão Nacional de Proteção de Dados). (2023). *Relatório de atividades 2022*. https://www.cnpd.pt/media/tutpevyh/relato-rio_2022.pdf

Comissão Europeia. (2021). *SMEs and cybercrime: Eurobarometer survey 2280*. https://europa.eu/eurobarometer/surveys/detail/2280

Curtis, J., & Oxburgh, G. (2023). Understanding cybercrime in 'real world' policing and law enforcement. *The Police Journal*, 96(4), 573-592. https://doi.org/10.1177/0032258X221107584

Demilie, W. B., & Deriba, F. G. (2022). Detection and prevention of SQLI attacks and developing compressive framework using machine learning and hybrid techniques. *Journal of Big Data, 9*(1), Article 124. https://doi.org/10.1186/s40537-022-00678-0

ESET (2024). *Relatório de ameaças: Portugal regista aumento nas deteções de spyware para Android*. https://blog.eset.pt/2024/03/relatorio-de-ameacas-portugal-regista-aumento-nas-detecoes-de-spyware-para-android/

Eurostat. (2022). *Cybersecurity incidents: Statistics on enterprises in the EU.* https://ec.europa.eu/eurostat/statistics-explained/SEPDF/cache/9132.pdf

Gangan, S. (2015). *A review of Man-in-the-Middle attacks*. *arXiv preprint.* https://arxiv.org/abs/1504.02115

Gomes, V. N. (2020). *Análise dos impactos dos ataques cibernéticos nas organizações: Um estudo de caso* (Dissertação de Mestrado, Instituto Universitário de Lisboa - ISCTE-IUL). Repositório ISCTE. https://repositorio.iscte-iul.pt/bitstream/10071/20286/1/Master_Vanessa_Nunes_Gomes.pdf

Gonçalves, P. (2022, fevereiro 8). *Vodafone afetada por ataque cibernético. Em atualização.* Sapo 24. https://24.sapo.pt/atualidade/artigos/ciberataque-a-vodafone-o-que-se-sabe-ate-ao-momento

Guo Y. (2023). A Survey of Machine Learning-Based Zero-Day Attack Detection: Challenges and Future Directions. *Computer communications*, *198*, 10.1016/j.comcom.2022.11.001. https://doi.org/10.1016/j.comcom.2022.11.001

Hamza, A. A., & Al-Janabi, R. J. S. (2024). Detecting brute force attacks using machine learning. *BIO Web of Conferences, 97*, 00045. https://doi.org/10.1051/bioconf/20249700045

Indra, K. (2020). *Cyber crime and security*. Journal of Emerging Technologies and Innovative Research, 7(6), 289–299. https://www.jetir.org/papers/JETIR2006289.pdf

Ministério Público. (2023). *Denúncias de Cibercrime 2023*. https://Cibercrime.ministeriopublico.pt/sites/default/files/documentos/pdf/denuncias_Cibercrime_2023_2024-09-11.pdf

Polícia Judiciária. (2024, 22 de agosto). *Detido em Lisboa suspeito de integrar grupo transnacional de cibercrime* [Comunicado de imprensa]. Polícia Judiciária. https://www.policiajudiciaria.pt/detido-em-lisboa-por-burla-qualificada-falsificacao-de-documentos-e-branqueamento/

RBE (Rede de Bibliotecas Escolares). (2023). *Relatório de cibersegurança em Portugal*. Blogue da Rede de Bibliotecas Escolares. https://blogue.rbe.mec.pt/relatorio-ciberseguranca-em-portugal-2466757

Ruddin, I., & Zein, S. G. N. (2024). Evolution of cybercrime law in legal development in the digital world. *Jurnal Multidisiplin Madani*. https://doi.org/10.55927/mudima.v4i1.7962

Sangari, S., Dallal, E., & Whitman, M. (2022). Modeling under-reporting in cyber incidents. *Risks, 10*(11), 200. https://doi.org/10.3390/risks10110200

Secretariado-Geral da Administração Interna. (2022). *Relatório anual de segurança interna 2021 (RASI 2021)*. Secretaria-Geral da Administração Interna. https://ssi.gov.pt/publicacoes/relatorio-anual-de-seguranca-interna/RASI_2021.pdf

Sivakumar, P., Nagarajan, R., Naresh, K., & Anand, B. (2023). A Comprehensive Review of Recent Advances in Deep Learning Techniques for Remote Sensing Applications. *Electronics, 12*(3), 573. https://doi.org/10.3390/electronics12030573

Suayyid, S. A., Al-Ghamdi, M. S., Al-Muhaideb, H., & Almuhaideb, A. M. (2023). A systematic literature review on cyber threat intelligence for organizational cybersecurity resilience. *Sensors*, 23(16), 7273. https://doi.org/10.3390/s23167273

Sunil, C., Pawar, R., Mente, B., & Chendage, D. (2021). *Cyber Crime, Cyber Space and Effects of Cyber Crime* (16). https://doi.org/10.32628/CSEIT217139

UNICRI (2014). *Cybercrime risks for the economy and enterprises at the EU and Italian level*. https://www.combattingcybercrime.org/files/virtual-library/phenomena-challenges-cybercrime/cybercrime-risks-for-the-economy-and-enterprises-at-the-eu-and-italian-level.pdf

Wadhwa, A., & Arora, N. (2017). *A review on cyber crime: Major threats and solutions*. International Journal of Advanced Research in Computer Science, 8(5). https://www.ijarcs.info/index.php/Ijarcs/article/view/4067

Capítulo 7 | Anexos

Anexo 7.A - Questionário Flash Eurobarometer 496

D1 What is the main activity of your company?
(READ OUT MAIN CATEGORIES FIRST, THEN SUBCATEGORIES - ONE ANSWER ONLY)

1	Industry	
	MINING AND QUARRYING	1
	MANUFACTURING	2
	ELECTRICITY, GAS, STEAM AND AIR CONDITIONING SUPPLY	3
	WATER SUPPLY; SEWERAGE, WASTE MANAGEMENT AND REMEDIATION ACTIVITIES	4
2	Construction, transport, ICT	
	CONSTRUCTION	5
	TRANSPORTATION AND STORAGE	6
	INFORMATION AND COMMUNICATION	7
3	Trade, accommodation and food services	
	WHOLESALE AND RETAIL TRADE; REPAIR OF MOTOR VEHICLES AND MOTORCYCLES	8
	ACCOMMODATION AND FOOD SERVICE ACTIVITIES	9
4	Non-public services	
	FINANCIAL AND INSURANCE ACTIVITIES	10
	REAL ESTATE ACTIVITIES	11
	PROFESSIONAL, SCIENTIFIC AND TECHNICAL ACTIVITIES	12
	ADMINISTRATIVE AND SUPPORT SERVICE ACTIVITIES	13
	ARTS, ENTERTAINMENT AND RECREATION	14
	OTHER SERVICE ACTIVITIES	15
	ACTIVITIES OF HOUSEHOLDS AS EMPLOYERS; UNDIFFERENTIATE GOODS AND SERVICES PRODUCING ACTIVITIES OF HOUSEHOLDS FOR OWN USE	16
	ACTIVITIES OF EXTRATERRITORIAL ORGANISATIONS AND BODIES	17
5	Public services	
	PUBLIC ADMINISTRATION AND DEFENCE; COMPULSORY SOCIAL SECURITY	18
	EDUCATION	19
	HUMAN HEALTH AND SOCIAL WORK ACTIVITIES	20
6	Agriculture, Forestry and Fishing	
	AGRICULTURE, FORESTRY AND FISHING	21
	Don't know/No Answer (DO NOT READ OUT)	998
	(Stop interview if D1=21 (NACE A), 18 (NACE O), 15, 16, 17 (NACE S, T, U) or 998)	

D2 How many employees (in full-time equivalents) does your company currently have?
ADD, IF NEEDED: If you are not sure, please provide your best estimate.
(READ OUT IF NECESSARY - ONE ANSWER ONLY)

1 to 9 employees	1
10 to 49 employees	2
50 to 249 employees	3
250 to 499 employees	4
500 or more employees	5
None, sole trader (DO NOT READ OUT)	0
Don't know/No Answer (DO NOT READ OUT)	998
(Stop interview if D2 =5 or 998)	

D3_v2 How long has your company been in business?
(READ OUT - ONE ANSWER ONLY)

Less than 1 year	1
Between 1 and 5 years	2
Between 6 and 10 years	3
More than 10 years	4
Don't know/No Answer (DO NOT READ OUT)	998

D5 What was your company's total turnover in 2020?
ADD, IF NEEDED: If you are not sure, please provide your best estimate.
(READ OUT IF NECESSARY - ONE ANSWER ONLY)

Less than 25,000 euro	1
More than 25,000 to 50,000 euro	2
More than 50,000 to 100,000 euro	3
More than 100,000 to 250,000 euro	4
More than 250,000 to 500,000 euro	5
More than 500,000 to 2 million euro	6
More than 2 to 10 million euro	7
More than 10 to 50 million euro	8
More than 50 million euro	9
Don't know/No Answer (DO NOT READ OUT)	998

Q1 Which of the following does your company currently have or use?
(READ OUT - MULTIPLE ANSWERS POSSIBLE)

An online bank account	1
An online ordering and payment service for customers	2
Online ordering or payment systems of suppliers, consultants or other business partners	3
A website for your business	4
Web-based applications for payroll processing, e-signature etc.	5
Cloud computing or storage	6
Internet-connected 'smart' devices	7
A company intranet	8
An internet-based video or voice calling service	9
Other (DO NOT READ OUT)	10
None of the above (DO NOT READ OUT)	11
Don't know (DO NOT READ OUT)	998

Q2 Do employees in your company use personally-owned devices such as smartphones, tablets, laptops or desktop computers to carry out regular business-related activities?
This includes devices that are subsidized by your company.
[SINGLE ANSWER]

Yes	1
No	2
Don't know (DO NOT READ OUT)	998

Q3 How well informed do you feel about the risks of cybercrime?
(READ OUT - ONE ANSWER ONLY)

Very well informed	1
Fairly well informed	2
Not very well informed	3
Not at all informed	4
Don't know (DO NOT READ OUT)	998

Q4 How well informed do you feel your employees are about the risks of cybercrime?
(READ OUT - ONE ANSWER ONLY)

Very well informed	1
Fairly well informed	2
Not very well informed	3
Not at all informed	4
Don't know (DO NOT READ OUT)	998

Q5 In the last 12 months, has your company provided employees with any training or awareness raising about the risks of cybercrime?
[SINGLE ANSWER]

Yes	1
No	2
Don't know (DO NOT READ OUT)	998

Q6 When using the internet for business-related activities, such as selling goods or online banking, are you concerned about any of the following risks?
(READ OUT – ONE ANSWER PER LINE)

Q6_1 Viruses, spyware or malware (excluding ransomware)
Q6_2 Denial of service attacks
Q6_3 Hacking (or attempts to hack) online bank accounts
Q6_4 Phishing, account takeover or impersonation attacks
Q6_5 Ransomware
Q6_6 Unauthorised accessing of files or networks
Q6_7 Unauthorised listening in to video conferences or instant messages
Q6_8 Any other breaches or attacks

Very concerned	1
Somewhat concerned	2
Not at all concerned	3
Don't know (DO NOT READ OUT)	998

Q7 Has your company experienced any of the following types of cybercrime in the last 12 months?
(READ OUT – ONE ANSWER PER LINE)

Q7_1 Viruses, spyware or malware (excluding ransomware)
Q7_2 Denial of service attacks
Q7_3 Hacking (or attempts to hack) online bank accounts
Q7_4 Phishing, account takeover or impersonation attacks
Q7_5 Ransomware
Q7_6 Unauthorised accessing of files or networks
Q7_7 Unauthorised listening in to video conferences or instant messages
Q7_8 Any other breaches or attacks

Yes	1
No	2
Don't know (DO NOT READ OUT)	998

ASK ANY Q7_1 TO Q7_8=1

Q8 Thinking about the most serious incident, how was this attack carried out?
(READ OUT - MULTIPLE ANSWERS POSSIBLE)

Exploiting software, hardware, or network vulnerabilities	1
Password cracking	2
Identity theft	3
Scams and fraud	4
Malicious software	5
Denial of service (false traffic to overwhelm website or network)	6
Disruption or defacing of web presence	7
Other (DO NOT READ OUT)	8
Don't know (DO NOT READ OUT)	998

Q9 Still thinking about the most serious incident, how was your business impacted?
(READ OUT - MULTIPLE ANSWERS POSSIBLE)

Loss of revenue	1
Loss of suppliers, customers, or partners	2
Repair or recovery costs	3
Ransom money	4
Prevented the use of resources or services	5
Prevented employees from carrying out day-to-day work	6
Additional time required to respond to the cybercrime incident(s)	7
Damage to the reputation of the company	8
Discouraged us from carrying out an activity that was planned	9
Not impacted in any of the ways described above (DO NOT READ OUT)	10
Don't know (DO NOT READ OUT)	998

ASK ANY Q7_1 TO Q7_8=1; SHOW ONLY ITEMS FOR WHICH Q7=1

Q10a Who, if anyone, did you report this incident to?
(READ OUT – MULTIPLE ANSWER PER LINE)

Q10a_1 Viruses, spyware or malware (excluding ransomware)
Q10a_2 Denial of service attacks
Q10a_3 Hacking (or attempts to hack) online bank accounts
Q10a_4 Phishing, account takeover or impersonation attacks
Q10a_5 Ransomware
Q10a_6 Unauthorised accessing of files or networks
Q10a_7 Unauthorised listening in to video conferences or instant messages
Q10a_8 Any other breaches or attacks

Did not report to anyone	1
The police	2
Another official authority	3
Seller or service provider	4
Your Internet service provider	5
A consumer protection organisation	6
A business representative body or trade body	7
Someone else (DO NOT READ OUT)	8
Don't know (DO NOT READ OUT)	998

ASK IF (Q7_1 =2 or 998) AND (Q7_2 =2 or 998) AND (Q7_3=2 or 998) AND (Q7_4 =2 or 998) AND (Q7_5 =2 or 998) AND (Q7_6=2 or 998) AND (Q7_7 =2 or 998) AND (Q7_8 =2 or 998)

Q10b If you were to experience or be a victim of any of the following incidents, who, if anyone, would you report the incident to?
(READ OUT – MULTIPLE ANSWER PER LINE)

Q10b_1 Viruses, spyware or malware (excluding ransomware)
Q10b_2 Denial of service attacks
Q10b_3 Hacking (or attempts to hack) online bank accounts
Q10b_4 Phishing, account takeover or impersonation attacks
Q10b_5 Ransomware
Q10b_6 Unauthorised accessing of files or networks
Q10b_7 Unauthorised listening in to video conferences or instant messages
Q10b_8 Any other breaches or attacks

Would not report to anyone	1
The police	2
Another official authority	3
Seller or service provider	4
Your Internet service provider	5
A consumer protection organisation	6
A business representative body or trade body	7
Someone else (DO NOT READ OUT)	8
Don't know (DO NOT READ OUT)	998

ASK IF NONE OF THE ITEMS IN Q10a=2

Q11 Why did you not report the incident (or incidents) to the police?
(READ OUT, MULTIPLE ANSWERS POSSIBLE)

Expected it would be reported by another authority (e.g. Internet provider/bank)	1
The police couldn't have done anything	2
Tried to report it but police were not interested	3
Dealt with the incident internally	4
Did not know the police dealt with this type of incident	5
Inconvenient/too much trouble	6
Too trivial/not worth reporting	7
Other (DO NOT READ OUT)	8
Don't know (DO NOT READ OUT)	998

Capítulo 8 | Apêndices

Apêndice 8.A - Variáveis da Base de Dados

Nome da Variável	**Descrição**	**Tipologia**	**Intervalo**
ID	Código de cada empresa.	Numérica	10351 a 10861
SetorGrupo	Nova variável que resulta do agrupamento da variável Atividade.	Categórica	1 - Indústria 2 - Construção, Transportes e TIC 3 - Comércio e Alojamento 4 -Serviços Não Públicos 5 - Serviços Públicos 6 - Agricultura e Pescas
NColaboradores	Número de colaboradores.	Categórica	1 - 1 a 9 empregados 2 - 10 a 49 empregados 3 - 50 a 249 empregados 4 - 250 a 499 empregados 5 - 500 ou mais empregados 0 - empresário em nome individual.
AnosAtiv	Anos de atividade.	Categórica	1 indica menos de 1 ano, o 2 significa entre 1 a 5 anos, o 3 de 6 a 10 anos e o 4 indica mais de 10 anos.
Volume	Volume de negócios total em 2020.	Categórica	1 - menos de 25 mil euros 2 - 25 a 50 mil euros 3 - 50 a 100 mil euros 4 - 100 a 250 mil euros 5 - 250 a 500 mil euros 6 - 500 mil a 2 milhões 7 - 2 a 10 milhões 8 - 10 a 50 milhões 9 - mais de 50 milhões.
ContaOnline	Possui uma conta bancária online.	Binária	0 ou 1
EncPagClientes	Possui um serviço de encomendas e pagamentos online para clientes.	Binária	0 ou 1

EncPagFornecedores	Possui um sistemas de encomendas ou pagamentos online de fornecedores,consultores ou outros parceiros comerciais.	Binária	0 ou 1
Site	Possui um site para o seu negócio.	Binária	0 ou 1
AppWeb	Possui aplicações baseadas na Web para processamento de salários, assinatura eletrónica.	Binária	0 ou 1
Cloud	Possui computação em nuvem ou armazenamento.	Binária	0 ou 1
DispositivosInteligentes	Possui dispositivos “inteligentes” ligados à Internet.	Binária	0 ou 1
Intranet	Possui uma intranet empresarial.	Binária	0 ou 1
Chamadas	Possui um serviço de chamadas de vídeo ou de voz baseado na Internet.	Binária	0 ou 1
DispositivosPessoais	Possuem dispositivos de propriedade pessoal para uso empresarial.	Binária	0 ou 1
Conscientização	Quão informado se sente sobre os riscos do cibercrime?	Categórica	1- Muito bem informado 2- Bastante bem informado 3- Não muito bem informado 4- Nada reportado
ConscientizaçãoColaboradores	Quão informado pensa que os seus colaboradores estão?	Categórica	1- Muito bem informado 2- Bastante bem informado 3- Não muito bem informado 4- Nada reportado
Formação	Houve formação sobre os riscos cibernéticos nos últimos 12 meses?	Binária	0 ou 1
PreocupaçãoMalware	Nível de preocupação com Vírus, Spyware ou outro tipo de malware.	Categórica	1- Muito preocupado 2- Um pouco preocupado 3- Nem um pouco

			preocupado
PreocupaçãoServiçoNegado	Nível de preocupação com ataques de serviço negado ou interrompido.	Categórica	1- Muito preocupado 2- Um pouco preocupado 3- Nem um pouco preocupado
PreocupaçãoContasOnline	Nível de preocupação com hacking de contas de bancos online.	Categórica	1- Muito preocupado 2- Um pouco preocupado 3- Nem um pouco preocupado
PreocupaçãoPhishing	Nível de preocupação com ataques de phishing, invasão de conta ou representação falsa.	Categórica	1- Muito preocupado 2- Um pouco preocupado 3- Nem um pouco preocupado
PreocupaçãoRansomware	Nível de preocupação com ransomware.	Categórica	1- Muito preocupado 2- Um pouco preocupado 3- Nem um pouco preocupado
PreocupaçãoAcessonãoautorizado	Nível de preocupação com acesso não autorizado a ficheiros ou redes.	Categórica	1- Muito preocupado 2- Um pouco preocupado 3- Nem um pouco preocupado
PreocupaçãoEscuta	Nível de preocupação com escuta não autorizada em videoconferências ou mensagens instantâneas.	Categórica	1- Muito preocupado 2- Um pouco preocupado 3- Nem um pouco preocupado
PreocupaçãoOutrosAtaques	Nível de preocupação com quaisquer outras violações ou ataques.	Categórica	1- Muito preocupado 2- Um pouco preocupado 3- Nem um pouco preocupado
OcorreuMalware	Nos últimos 10 meses ocorreu um ataque de vírus, spyware ou outro tipo malware.	Binária	0 ou 1
OcorreuServiçoNegado	Nos últimos 10 meses ocorreram ataques de negação de serviço.	Binária	0 ou 1
OcorreuContasOnline	Nos últimos 10 meses ocorreu um ataque de hacking de contas de bancos online.	Binária	0 ou 1
OcorreuPhishing	Nos últimos 10 meses	Binária	0 ou 1

	ocorreram ataques de phishing, invasão de conta ou representação falsa.		
Ocorreuransomware	Nos últimos 10 meses ocorreu ransomware.	Binária	0 ou 1
OcorreuAcessoNãoAutorizado	Nos últimos 10 meses ocorreu Acesso não autorizado a ficheiros ou redes	Binária	0 ou 1
OcorreuEscuta	Nos últimos 10 meses ocorreu Escuta não autorizada em videoconferências ou mensagens instantâneas	Binária	0 ou 1
OcorreramOutrosAtaques	Nos últimos 10 meses ocorreu outros ataques	Binária	0 ou 1
SoftHardware	O incidente mais grave foi através da exploração de vulnerabilidades de softwares, hardwares ou de redes	Binária	0 ou 1
QuebraPasse	O incidente mais grave foi através da quebra de palavra-passe	Binária	0 ou 1
RouboIdentidade	O incidente mais grave foi através do roubo de identidade	Binária	0 ou 1
Fraudes	O incidente mais grave foi através das burlas e fraudes	Binária	0 ou 1
SoftwareMalicioso	O incidente mais grave foi através do software malicioso	Binária	0 ou 1
ServiçoNegado	O incidente mais grave foi através da negação ou interrupção de serviço	Binária	0 ou 1
Interrupção	O incidente mais grave foi através da interrupção ou desfiguração da presença na web	Binária	0 ou 1
PerdaReceita	O negócio da empresa foi impactado através da perda de receita	Binária	0 ou 1

PerdaParceiros	O negócio da empresa foi impactado através da perda de fornecedores, clientes ou parceiros	Binária	0 ou 1
CustosRecuperação	O negócio da empresa foi impactado através dos custos de reparação ou recuperação	Binária	0 ou 1
DinheiroResgate	O negócio da empresa foi impactado através do dinheiro de resgate	Binária	0 ou 1
ImpedimentoRecursos	O negócio da empresa foi impactado através do impedimento da utilização de recursos ou serviços	Binária	0 ou 1
ImpedimentoTrabalho	O negócio da empresa foi impactado através do impedimento que os colaboradores realizassem o trabalho diário	Binária	0 ou 1
TempoAdicional	O negócio da empresa foi impactado através do tempo adicional necessário para responder ao(s) incidente(s) de cibercrime	Binária	0 ou 1
DanosReputação	O negócio da empresa foi impactado através dos danos na reputação da empresa	Binária	0 ou 1
CancelamentoAtividade	O negócio da empresa foi impactado através do desencorajamento de realizar uma atividade que estava planeada	Binária	0 ou 1
MalwareNinguém	Se ocorresse um ataque de vírus, spyware ou outro tipo de malware a empresa não denunciaria a ninguém.	Binária	0 ou 1
MalwarePolícia	Se ocorresse um ataque de vírus, spyware ou outro tipo de malware a empresa denunciaria à polícia.	Binária	0 ou 1
MalwareOutraAutoridade	Se ocorresse um ataque	Binária	0 ou 1

	de vírus, spyware ou outro tipo de malware a empresa denunciaria a outra autoridade oficial.		
MalwareFornecedorServiços	Se ocorresse um ataque de vírus, spyware ou outro tipo de malware a empresa denunciaria a um vendedor ou fornecedor de serviços.	Binária	0 ou 1
MalwareFornecedorInternet	Se ocorresse um ataque de vírus, spyware ou outro tipo de malware a empresa denunciaria a um fornecedor de serviços de internet.	Binária	0 ou 1
MalwareOrgConsumidor	Se ocorresse um ataque de vírus, spyware ou outro tipo de malware a empresa denunciaria a uma organização de proteção do consumidor.	Binária	0 ou 1
MalwareOrgComercial	Se ocorresse um ataque de vírus, spyware ou outro tipo de malware a empresa denunciaria a um organismo representativo das empresas ou organismo comercial.	Binária	0 ou 1
ServiçoNegadoNinguém	Se ocorresse um ataque de negação de serviço não reportaria a ninguém	Binária	0 ou 1
ServiçoNegadoPolícia	Se ocorresse um ataque de negação de serviço reportaria à polícia	Binária	0 ou 1
ServiçoNegadoOutraAutoridade	Se ocorresse um ataque de negação de serviço reportaria a outra autoridade oficial	Binária	0 ou 1
ServiçoNegadoVendedorServiços	Se ocorresse um ataque de negação de serviço reportaria a um vendedor ou prestador de serviços	Binária	0 ou 1
ServiçoNegadoFornecedorInternet	Se ocorresse um ataque de negação de serviço reportaria ao fornecedor de serviços de Internet	Binária	0 ou 1

ServiçoNegadoOrgConsumidor	Se ocorresse um ataque de negação de serviço reportaria a uma organização de proteção do consumidor	Binária	0 ou 1
ServiçoNegadoOrgComercial	Se ocorresse um ataque de negação de serviço reportaria a um organismo representativo de uma empresa ou organismo comercial	Binária	0 ou 1
ContasOnlineNinguém	Se pirateassem as contas bancárias online não denunciaria a ninguém	Binária	0 ou 1
ContasOnlinePolícia	Se pirateassem as contas bancárias online denunciaria à polícia	Binária	0 ou 1
ContasOnlineOutraAutoridade	Se pirateassem as contas bancárias online denunciaria a outra autoridade oficial	Binária	0 ou 1
ContasOnlineVendedorServiços	Se pirateassem as contas bancárias online denunciaria a um vendedor ou prestador de serviços	Binária	0 ou 1
ContasOnlineFornecedorInternet	Se pirateassem as contas bancárias online denunciaria ao fornecedor de serviços de Internet	Binária	0 ou 1
ContasOnlineOrgConsumidor	Se pirateassem as contas bancárias online denunciaria a uma organização de proteção do consumidor	Binária	0 ou 1
ContasOnlineOrgComercial	Se pirateassem as contas bancárias online denunciaria a um organismo representativo de empresas ou organismo comercial	Binária	0 ou 1
PhishingNinguém	Se ocorresse um ataque de phishing, controlo de conta ou falsificação de identidade não denunciaria a ninguém.	Binária	0 ou 1

PhishingPolícia	Se ocorresse um ataque de phishing, controlo de conta ou falsificação de identidade denunciaria à polícia.	Binária	0 ou 1
PhishingOutraAutoridade	Se ocorresse um ataque de phishing, controlo de conta ou falsificação de identidade denunciaria a outra autoridade oficial.	Binária	0 ou 1
PhishingVendedorServiços	Se ocorresse um ataque de phishing, controlo de conta ou falsificação de identidade – Vendedor ou fornecedor de serviços.	Binária	0 ou 1
PhishingFornecedorInternet	Se ocorresse um ataque de phishing, controlo de contas ou falsificação de identidade – o seu fornecedor de serviços de Internet	Binária	0 ou 1
PhishingOrgConsumidor	Se ocorresse um ataque de phishing, controlo de conta ou falsificação de identidade – Uma organização de proteção do consumidor	Binária	0 ou 1
PhishingOrgcomercial	Se ocorresse um ataque de phishing, controlo de conta ou falsificação de identidade - um organismo representativo de empresas ou organismo comercial	Binária	0 ou 1
RansomwareNinguém	Se ocorresse Ransomware não denunciaria a ninguém	Binária	0 ou 1
RansomwarePolícia	Se ocorresse Ransomware denunciaria à polícia	Binária	0 ou 1
RansomwareOutraAutoridade	Se ocorresse Ransomware denunciaria a outra autoridade oficial	Binária	0 ou 1
RansomwareVendedorServiços	Se ocorresse Ransomware denunciaria ao vendedor ou prestador	Binária	0 ou 1

	de serviços		
RansomwareFornecedorInternet	Se ocorresse Ransomware denunciaria ao seu fornecedor de serviços de Internet	Binária	0 ou 1
RansomwareOrgConsumidor	Se ocorresse Ransomware denunciaria a uma organização de proteção do consumidor	Binária	0 ou 1
RansomwareOrgComercial	Se ocorresse Ransomware denunciaria a um organismo representativo das empresas ou organismo comercial	Binária	0 ou 1
AcessoNãoAutorizadoNinguém	Se ocorresse acesso não autorizado a ficheiros ou redes não denunciaria a ninguém	Binária	0 ou 1
AcessoNãoAutorizadoPolícia	Se ocorresse acesso não autorizado a ficheiros ou redes denunciaria à polícia	Binária	0 ou 1
AcessoNãoAutorizadoOutraAutoridade	Se ocorresse acesso não autorizado a ficheiros ou redes denunciaria a outra autoridade oficial	Binária	0 ou 1
AcessoNãoAutorizadoVendedorServiços	Se ocorresse acesso não autorizado a ficheiros ou redes denunciaria ao vendedor ou prestador de serviços	Binária	0 ou 1
AcessoNãoAutorizadoFornecedorInternet	Se ocorresse acesso não autorizado a ficheiros ou redes denunciaria ao seu fornecedor de serviços de Internet	Binária	0 ou 1
AcessoNãoAutorizadoOrgConsumidor	Se ocorresse acesso não autorizado a ficheiros ou redes denunciaria a uma organização de proteção do consumidor	Binária	0 ou 1
AcessoNãoAutorizadoOrgComercial	Se ocorresse acesso não autorizado a ficheiros ou redes denunciaria a um organismo comercial	Binária	0 ou 1

	representativo ou um organismo comercial		
EscutaNinguém	Se ocorresse escuta não autorizada em videoconferências ou mensagens instantâneas não denunciaria a ninguém	Binária	0 ou 1
EscutaPolícia	Se ocorresse escuta não autorizada em videoconferências ou mensagens instantâneas denunciaria à polícia	Binária	0 ou 1
EscutaOutraAutoridade	Se ocorresse escuta não autorizada em videoconferências ou mensagens instantâneas denunciaria a outra autoridade oficial	Binária	0 ou 1
EscutaVendedorServiços	Se ocorresse escuta não autorizada em videoconferências ou mensagens instantâneas denunciaria ao vendedor ou prestador de serviços	Binária	0 ou 1
EscutaFornecedorInternet	Se ocorresse escuta não autorizada em videoconferências ou mensagens instantâneas denunciaria ao seu fornecedor de serviços de Internet	Binária	0 ou 1
EscutaOrgConsumidor	Se ocorresse escuta não autorizada em videoconferências ou mensagens instantâneas denunciaria a uma organização de proteção do consumidor	Binária	0 ou 1
EscutaOrgComercial	Se ocorresse escuta não autorizada em videoconferências ou mensagens instantâneas denunciaria a um organismo representativo das empresas ou um organismo comercial	Binária	0 ou 1
OutrosAtaquesNinguém	Se ocorresse quaisquer outras violações ou ataques não denunciaria	Binária	0 ou 1

	a ninguém.		
OutrosAtaquesPolícia	Se ocorresse quaisquer outras violações ou ataques denunciaria à polícia.	Binária	0 ou 1
OutrosAtaquesOutraAutoridade	Se ocorresse quaisquer outras violações ou ataques denunciaria a outra autoridade oficial,	Binária	0 ou 1
OutrosAtaquesVendedor	Se ocorresse quaisquer outras violações ou ataques denunciaria a um vendedor ou prestador de serviços.	Binária	0 ou 1
OutrosAtaquesFornecedorInternet	Se ocorresse quaisquer outras violações ou ataques denunciaria ao fornecedor de serviços de Internet.	Binária	0 ou 1
OutrosAtaquesOrgConsumidor	Se ocorresse quaisquer outras violações ou ataques denunciaria a uma organização de proteção do consumidor.	Binária	0 ou 1
OutrosAtaquesOrgComercial	Se ocorresse quaisquer outras violações ou ataques denunciaria a um organismo representativo das empresas ou um organismo comercial.	Binária	0 ou 1
ReportadoOutraAutoridade	Não denunciei o incidente à polícia porque esperava que fosse reportado por outra autoridade (ex: banco)	Binária	0 ou 1
PolíciaNãoPodiaFazerNada	Não denunciei o incidente à polícia porque a polícia não podia ter feito nada	Binária	0 ou 1
DesinteressePolícia	Tentei denunciar o incidente, mas a polícia não estava interessada	Binária	0 ou 1
Internamente	Não denunciei o incidente à polícia porque lidei com o incidente internamente	Binária	0 ou 1

NãoSabiaPolíciaLidava	Não denunciei o incidente à polícia porque não sabia que a polícia lidava com este tipo de incidentes.	Binária	0 ou 1
Inconveniente	Não denunciei o incidente à polícia porque era inconveniente.	Binária	0 ou 1
Trivial	Não denunciei o incidente à polícia porque não valia a pena relatar.	Binária	0 ou 1

Apêndice 8.B - Tabelas de Frequência para as variáveis qualitativas ordinais

```
$SetorGrupo
  Category Count Percent
1        1    90    19.0
2        2   219    46.3
3        3    59    12.5
4        4   105    22.2

$NColaboradores
  Category Count Percent
1        1   242    51.2
2        2   134    28.3
3        3    97    20.5

$AnosAtiv
  Category Count Percent
1        1    19     4.0
2        2   101    21.4
3        3   102    21.6
4        4   246    52.0
5        5     5     1.1

$Volume
   Category Count Percent
1         1    42     8.9
2         2    48    10.1
3         3    42     8.9
4         4    61    12.9
5         5    51    10.8
6         6    55    11.6
7         7    54    11.4
8         8    31     6.6
9         9    18     3.8
10     <NA>    71    15.0
```

Apêndice 8.C - Tabelas de Frequência para as variáveis qualitativas nominais binárias

```
$OcorreuMalware
  Category Count Percent
1        0   375    79.3
2        1    98    20.7

$OcorreuServiçoNegado
  Category Count Percent
1        0   437    92.4
2        1    36     7.6

$OcorreuContasOnline
  Category Count Percent
1        0   431    91.1
2        1    42     8.9

$OcorreuPhishing
  Category Count Percent
1        0   400    84.6
2        1    73    15.4

$Ocorreuransomware
  Category Count Percent
1        0   425    89.9
2        1    48    10.1

$OcorreuAcessoNãoAutorizac
  Category Count Percent
1        0   403    85.2
2        1    70    14.8

$OcorreuEscuta
  Category Count Percent
1        0   437    92.4
2        1    36     7.6

$MalwarePolícia
  Category Count Percent
1        0   119    25.2
2        1   115    24.3
3     <NA>   239    50.5

$ServiçoNegadoPolícia
  Category Count Percent
1        0   101    21.4
2        1   133    28.1
3     <NA>   239    50.5

$ContasOnlinePolícia
  Category Count Percent
1        0    58    12.3
2        1   176    37.2
3     <NA>   239    50.5

$PhishingPolícia
  Category Count Percent
1        0    67    14.2
2        1   167    35.3
3     <NA>   239    50.5

$RansomwarePolícia
  Category Count Percent
1        0    99    20.9
2        1   135    28.5
3     <NA>   239    50.5

$AcessoNãoAutorizadoPolícia
  Category Count Percent
1        0    68    14.4
2        1   166    35.1
3     <NA>   239    50.5

$EscutaPolícia
  Category Count Percent
1        0    70    14.8
2        1   164    34.7
3     <NA>   239    50.5

$OutrosAtaquesPolícia
  Category Count Percent
1        0    69    14.6
2        1   165    34.9
3     <NA>   239    50.5

$ReportadoOutraAutoridade
  Category Count Percent
1        0   136    28.8
2        1    20     4.2
3     <NA>   317    67.0

$PolíciaNãoPodiaFazerNada
  Category Count Percent
1        0   137      29
2        1    19       4
3     <NA>   317      67

$DesinteressePolícia
  Category Count Percent
1        0   145    30.7
2        1    11     2.3
3     <NA>   317    67.0

$Internamente
  Category Count Percent
1        0   121    25.6
2        1    35     7.4
3     <NA>   317    67.0

$NãoSabiaPolíciaLidava
  Category Count Percent
1        0   123      26
2        1    33       7
3     <NA>   317      67

$Inconveniente
  Category Count Percent
1        0   137      29
2        1    19       4
3     <NA>   317      67

$Trivial
  Category Count Percent
1        0   118    24.9
2        1    38     8.0
3     <NA>   317    67.0
```

Apêndice 8.D - Distribuição dos Anos de Atividade por cluster

```
> table(dados$Cluster, dados$AnosAtiv)

    1  2  3   4
1   9 40 44 101
2   9 47 45 129
3   1 14 13  16
```

Apêndice 8.E - Distribuição do Número de Colaboradores por cluster

```
table(dados$Cluster, dados$NColaboradores)

    1   2   3
1 103  53  39
2 118  68  48
3  21  13  10
```

Apêndice 8.F - Distribuição do Volume por cluster

```
table(dados$Cluster, dados$Volume)

   1  2  3  4  5  6  7  8  9
1 17 17 18 25 29 19 22 20 11
2 22 28 14 28 18 31 28  9  6
3  3  3 10  8  4  5  4  2  1
```

Apêndice 8.G - Distribuição do Setor de Atividade por cluster

```
> table(dados$SetorGrupo, dados$Cluster)

    1   2   3
1  32  43  15
2 100 102  17
3  17  38   4
4  46  51   8
```

Apêndice 8.H - Resultados das Associações de V de Cramer

```
> print(calcular_v_cramer(dados_filtrados$Cluster, dados_filtrados$Setor_Grupo_Num))
                   X^2 df P(> X^2)
Likelihood Ratio 6.6658  3 0.083347
Pearson          7.3498  3 0.061547

Phi-Coefficient   : NA
Contingency Coeff.: 0.173
Cramer's V        : 0.175
>
> print(calcular_v_cramer(dados_filtrados$Cluster, dados_filtrados$AnosAtiv))
                   X^2 df P(> X^2)
Likelihood Ratio 5.3811  4  0.25038
Pearson          5.2072  4  0.26669

Phi-Coefficient   : NA
Contingency Coeff.: 0.146
Cramer's V        : 0.148
> print(calcular_v_cramer(dados_filtrados$Cluster, dados_filtrados$Volume))
                   X^2 df P(> X^2)
Likelihood Ratio 9.3925  8  0.31028
Pearson          9.8681  8  0.27441

Phi-Coefficient   : NA
Contingency Coeff.: 0.208
Cramer's V        : 0.213
> print(calcular_v_cramer(dados_filtrados$Cluster, dados_filtrados$NColaboradores))
                    X^2 df P(> X^2)
Likelihood Ratio 0.38167  2  0.82627
Pearson          0.38251  2  0.82592

Phi-Coefficient   : NA
Contingency Coeff.: 0.04
Cramer's V        : 0.04
```