Universidade do Minho

Escola de Economia, Gestão e Ciência Política

Clara Maria Braga Gonçalves

O Impacto das Estratégias de Cibersegurança na Confiança do Consumidor: Uma Análise das Práticas em Pequenas e Médias Empresas

abril de 2025

O Impacto das Estratégias de Cibersegurança na Confiança do Consumidor: Uma Análise das Práticas em Pequenas e Médias Empresas

Clara Maria Braga Gonçalves

UMinho | 2025

Universidade do Minho

Escola de Economia, Gestão e Ciência Política

Clara Maria Braga Gonçalves

O Impacto das Estratégias de Cibersegurança na Confiança do Consumidor: Uma Análise das Práticas em Pequenas e Médias Empresas

Dissertação de Mestrado

Mestrado em Gestão e Negócios

Trabalho efetuado sob a orientação do

Professor Doutor António Azevedo

e do

Professor Doutor Paulo Ramos

abril de 2025

DIREITOS DE AUTOR E CONDIÇÕES DE UTILIZAÇÃO DO TRABALHO POR TERCEIROS

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos.

Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada.

Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho



Atribuição-NãoComercial-SemDerivações

CC BY-NC-ND

https://creativecommons.org/licenses/by-nc-nd/4.0/

Agradecimentos

Apesar de a escrita de uma dissertação parecer, à partida, um caminho solitário, nada disto teria sido possível sem o apoio das pessoas a quem gostaria de expressar o meu carinho e profunda gratidão.

Em primeiro lugar, agradeço aos meus orientadores, Professor Doutor António Azevedo e Professor Doutor Paulo Ramos, por embarcarem nesta investigação e cuja orientação e disponibilidade foram fundamentais ao longo de todo o trabalho.

De seguida, o agradecimento mais fervoroso vai, sem dúvida, para a minha família. Durante estes meses intensos, foram a sua compreensão e força que me fizeram acreditar no meu próprio potencial. À minha mãe, por todos os momentos em que me deu liberdade, apoio e incentivo para tomar as decisões necessárias. À minha irmã, a minha maior sorte, pela companhia constante, pela paciência com as revisões de última hora e pela presença em todas as etapas da minha vida.

À Sara, companheira nesta aventura e em tantas outras, um agradecimento especial por ouvir as minhas dúvidas, ajudar a tomar decisões e por me fazer rir quando mais precisava.

À Maggy, por todas as gargalhadas, momentos felizes e apoio incondicional que me davam energia para continuar.

Às minhas amigas de todas as horas — Rita, Miranda, Letícia e Beatriz —, obrigada por todas as palavras de carinho quando mais precisei. Sinto-me verdadeiramente sortuda por vos ter conhecido durante a licenciatura.

A todos os meus amigos, antigos e mais recentes, que ao longo destes últimos anos me apoiaram, motivaram e acolheram, o meu profundo agradecimento por estarem ao meu lado.

Por fim, a todos aqueles que, direta ou indiretamente, contribuíram para este trabalho, o meu mais sincero obrigada.

I wave goodbye to the end of beginning

-Djo

DECLARAÇÃO DE INTEGRIDADE

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri à prática de plágio nem a qualquer forma de utilização indevida ou falsificação de informações ou resultados em nenhuma das etapas conducente à sua elaboração.
Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho.

O Impacto das Estratégias de Cibersegurança na Confiança do Consumidor: Uma Análise das Práticas em Pequenas e Médias Empresas

Resumo

Este estudo tem como objetivo principal analisar o impacto das estratégias de cibersegurança na confiança dos consumidores, centrando-se no setor das Pequenas e Médias Empresas (PME). Procura compreender de que modo a implementação de práticas eficazes de proteção de dados influencia a perceção de segurança por parte dos consumidores e a sua relação com a empresa.

Assim, foi adotada uma abordagem quantitativa, com a aplicação de um questionário a consumidores de PME através da amostra por conveniência, complementada por uma Revisão da Literatura que enquadra os principais conceitos relacionados com cibersegurança e confiança do consumidor no contexto empresarial. O enquadramento teórico baseia-se no paradigma do *Realismo Crítico*, permitindo uma análise contextualizada das relações entre práticas organizacionais e perceções individuais.

Os resultados do questionário com 232 respostas teve como objetivo avaliar a influência dos construtos Confiança na PME, Confiança do Consumidor, Privacidade, Lealdade e *Word of Mouth* (WOM). Os resultados mostram que a transparência das práticas de segurança, a formação contínua de colaboradores e a adoção de medidas técnicas robustas têm um impacto significativo na confiança do consumidor. Quanto maior o conhecimento dos consumidores sobre as práticas de cibersegurança, maior é a valorização da proteção dos seus dados. As variáveis Confiança na PME, Confiança do Consumidor e Privacidade apresentaram correlações positivas com a Lealdade e o WOM, destacando-se a mais forte entre a Confiança do Consumidor e o WOM (r=0,764).

Estes resultados servem de guia para as PME refletirem sobre as suas práticas de cibersegurança, onde esta deve ser entendida como um investimento estratégico essencial não apenas para a proteção dos ativos digitais, mas também para a sustentabilidade financeira das empresas.

Palavras-chave: Cibersegurança; Confiança Consumidores; Gestores; PME; Confiança na PME; Privacidade de Dados; Lealdade; *Word of Mouth* (WOM)

The Impact of Cybersecurity Strategies on Consumer Confidence: An Analysis of Practices in Small and Medium-Sized Companies

Abstract

The main objective of this study is to analyze the impact of cybersecurity strategies on consumer trust, focusing on the Small and Medium Enterprise (SME) sector. It seeks to understand how the implementation of effective data protection practices influences consumers' perception of security and their relationship with the company.

Thus, a quantitative approach was adopted, with the application of a questionnaire to SME consumers through convenience sampling, complemented by a Literature Review that frames the main concepts related to cybersecurity and consumer trust in the business context. The theoretical framework is based on the *Critical Realism* paradigm, allowing for a contextualized analysis of the relationships between organizational practices and individual perceptions.

The results of the questionnaire with 232 responses aimed to assess the influence of the constructs Trust in the SME, Consumer Trust, Privacy, Loyalty and Word of Mouth (WOM). The results show that transparency of security practices, continuous training of employees and the adoption of robust technical measures have a significant impact on consumer trust. The more consumers know about cybersecurity practices, the more they value protecting their data. The variables Trust in SME, Consumer Trust and Privacy showed positive correlations with Loyalty and WOM, with the strongest correlation between Consumer Trust and WOM (r=0.764).

These results serve as a guide for SME to reflect on their cybersecurity practices, where it should be understood as an essential strategic investment not only for the protection of digital assets, but also for the financial sustainability of companies.

Keywords: Cybersecurity; Consumer Confidence; Managers; SME; Trust in SME; Data Privacy; Loyalty; Word of Mouth (WOM)

ÍNDICE

Direitos De Autor E Condições De Utilização Do Trabalho Por Terceiros 2
Agradecimentos 3
Declaração De Integridade 4
Resumo 5
Abstract 6
Índice de Figuras 9
Índice de Tabelas 10
1. Capítulo 1: Introdução 10
1.1. Enquadramento do Tema 11
2. Capítulo 2: Revisão da Literatura 13
2.1. Paradigma e Abordagem 13
2.2. Cibersegurança 13
2.3. Ciberespaço 16
2.4. Cibercrime e Ciberameaça 17
2.5. Normas/Regulamentos 20
2.5.1. Selo Cibersegurança e Maturidade Digital 20
3. Capítulo 3: O Contexto das PME 22
3.1. Introdução às PME 22
3.2. Cibersegurança nas PME 22
4. Capítulo 4: Comportamento do Consumidor e Cibersegurança 25
4.1. Introdução ao Comportamento do Consumidor 25
4.2. Relacionamento entre as Variáveis 26
5. Capítulo 5: Metodologia 29
5.1. Tipo de Estudo e Abordagem Metodológica 29
5.2. Problemática e Objetivos 29
5.3. Paradigma de Investigação 30
5.4. Método de Recolha de Dados 30
6. Capítulo 6: Modelo Conceptual 31
6.1. Definição do Modelo Conceptual 31
6.2. Variáveis do Modelo Conceptual 32
7. Capítulo 7: Amostragem e Instrumentos de Pesquisa 35

7.1. Processo de Amostragem 35
7.2. *Design* do Questionário 35
8. Capítulo 8: Análise de Dados e Resultados 38
8.1. Método de Análise de Dados 38
8.2. Análise Descritiva das Variáveis 38
8.3. Caracterização da Amostra 38
8.4. Análise dos Construtos 47
8.5. Testes Estatísticos e de Confiabilidade 47
8.6. Análise dos Resultados do Modelo Conceptual 48
8.7. Análise das Correlações do Modelo Conceptual 56
8.8. Teste T para Análise das Variáveis 58
9. Capítulo 9: Considerações Finais 61
9.1. Discussão de Resultados e Principais Conclusões 61
9.2. Limitações do Estudo 64
9.3. Sugestões para Investigação Futura 65
10. Referências Bibliográficas 66
11. Anexo – Formulário do Questionário 70

Índice de Figuras

Figura 1 - Modelo Conceptual 31
Figura 2 - Cenário Fictício Criado no Questionário 37

Índice de Tabelas

Tabela 1 - Escalas de Medição das Variáveis dos Construtos Utilizados 34
Tabela 2 - Amostra do Género dos Inquiridos 39
Tabela 3 - Amostra da Idade dos Inquiridos 39
Tabela 4 - Amostra da Nacionalidade dos Inquiridos 40
Tabela 5 - Amostra do Concelho de Residência dos Inquiridos 42
Tabela 6 - Amostra do Nível de Escolaridade dos Inquiridos 42
Tabela 7 - Amostra da Ocupação/Profissão dos Inquiridos 45
Tabela 8 - Amostra da Definição de Cibersegurança 46
Tabela 9 - Amostra da Definição de Ciberataque 46
Tabela 10 - Amostra sobre o Conhecimento das Medidas de Segurança das Empresas 46
Tabela 11 - Amostra das Medidas a Implementar pelas PME segundo os Inquiridos 47
Tabela 12 - Análise dos Testes de Confiabilidade dos Construtos 48
Tabela 13 - Variável Construto Confiança na PME 49
Tabela 14 - Variável Construto Confiança na PME após Análise Descritiva 50
Tabela 15 - Estatísticas de Escala Confiança na PME 50
Tabela 16 - Variável Construto Lealdade 51
Tabela 17 - Variável Construto Lealdade após Análise Descritiva 51
Tabela 18 - Estatísticas de Escala Lealdade 52
Tabela 19 - Variável Construto WOM 52
Tabela 20 - Variável Construto WOM após Análise Descritiva 53
Tabela 21 - Estatísticas de Escala WOM 53
Tabela 22 - Variável Construto Confiança do Consumidor 54
Tabela 23 - Variável Construto Confiança do Consumidor após Análise Descritiva 54
Tabela 24 - Estatísticas de Escala Confiança do Consumidor 55
Tabela 25 - Variável Construto Privacidade de Dados 55
Tabela 26 - Variável Construto Privacidade de Dados após Análise Descritiva 56
Tabela 27 - Estatísticas de Escala Privacidade de Dados 56
Tabela 28 - Correlação do Teste de Pearson 56
Tabela 29 - Teste T 59
Tabela 30 - Teste Amostras Independentes 60

1. Capítulo 1: Introdução

1.1. Enquadramento do Tema

Com o rápido desenvolvimento das Tecnologias de Informação, a cibersegurança torna-se fulcral para proteger os dados no ciberespaço. A expansão deste espaço digital permitiu o surgimento de ciberataques inteligentes e cujo único intuito é prejudicar as suas vítimas. Deste modo, a criação de medidas de cibersegurança potenciam a proteção das organizações no ciberespaço, tornando-as menos suscetíveis a perdas de dados confidenciais e promovendo o bom funcionamento digital (Morales-Sáenz et al., 2024).

Com o aumento do trabalho desempenhado em plataformas digitais, com ligação constante à Internet e permitindo o contacto com qualquer pessoa no Mundo, surgiram dúvidas sobre se e como estamos seguros neste contexto. No Mundo digital atual, há cada vez mais exigências virtuais que as empresas precisam de adquirir, levantando questões como a privacidade de dados e a partilha de informação. Tal conduz as organizações a refletirem sobre a sua segurança, prevenindo potenciais crimes. Muitas das questões de segurança tornaram-se mais evidentes com a Pandemia da Covid-19 e a implementação do teletrabalho, que obrigou à digitalização de dados e métodos de trabalho em todas as organizações, independentemente da sua área de influência ou dimensão (Morales-Sáenz et al., 2024).

Contrariamente ao que sucede nas grandes empresas, as Pequenas e Médias Empresas (PME) possuem medidas de cibersegurança mais limitadas, tornando-se alvos vulneráveis a ciberataques. Em comparação com as grandes empresas, estas tendem a descurar a proteção de dados, a não atualizar o *software* ou a não procurar mais formação e conhecimento na área, deixando a sua segurança bastante frágil e vulnerável a ciberataques. Fernandez de Arroyabe et al. (2023) referem que grande parte da má conduta em relação à segurança é perpetuada pelos próprios funcionários, uma vez que os ataques não necessitam de ser particularmente sofisticados. Outro fator relevante é a limitação de recursos financeiros disponíveis para enfrentar estas situações. Esta restrição inclui não só os custos diretos associados à mitigação e recuperação de um sistema após um ataque, mas também o tempo necessário para restaurar a normalidade de forma duradoura. Além disso, um ataque pode resultar em danos significativos à reputação da empresa, comprometendo a confiança dos consumidores e parceiros. Dependendo da natureza do ataque, podem ainda surgir encargos legais adicionais, agravando o impacto financeiro e operacional da organização (Fernandez de Arroyabe et al., 2023; Fedele & Roner, 2021).

Posto isto, a questão de investigação deste estudo é: *O Impacto das Estratégias de Cibersegurança na Confiança do Consumidor: Uma Análise das Práticas em Pequenas e Médias Empresas.*

O principal objetivo da investigação é perceber qual o impacto do investimento em cibersegurança na confiança do consumidor por parte das PME. O foco passará por compreender como a implementação de estratégias de segurança pode condicionar a perceção dos consumidores sobre a proteção dos seus dados e como a sua tendência para confiar na empresa pode ser afetada, podendo resultar numa melhor relação consumidor-empresa. Através da análise dessa perceção, os gestores poderão avaliar as medidas a implementar e o impacto que estas terão.

De modo a responder a este tema, foi adotada uma abordagem quantitativa com a aplicação de um questionário a consumidores de PME, a fim de recolher informações sobre a sua perceção de confiança na cibersegurança dessas empresas. Além disso, recorrer-se-á ao paradigma do *Realismo Crítico* para identificar as estratégias que promovem maior confiança nos consumidores. Este defende que o mundo é percecionado como um "sistema aberto" onde é influenciado pelas ações de distintos indivíduos (Rieder et al., 2024). A abordagem dedutiva será utilizada para desenvolver o estudo com base em dados empíricos.

Este trabalho está estruturado em nove capítulos, onde o primeiro corresponde à introdução.

Os segundo, terceiro e quarto capítulos apresentam a Revisão da Literatura, abordando a importância da cibersegurança no contexto das PME, a confiança do consumidor e os construtos e conceitos fundamentais para o estudo.

O quinto capítulo detalha a metodologia adotada, incluindo os objetivos da investigação, abordagem metodológica, amostragem e recolha de dados.

No sexto, são apresentados novamente os construtos utilizados e o modelo conceptual.

O sétimo descreve o processo de amostragem e a construção do questionário.

O oitavo capítulo analisa os dados recolhidos, incluindo testes de confiança e apresentação dos resultados.

Por fim, o nono capítulo apresenta a discussão dos dados, principais conclusões, limitações do estudo e sugestões para futuras investigações.

2. Capítulo 2: Revisão da Literatura

2.1. Paradigma e Abordagem

Neste estudo, foi adotada a abordagem dedutiva, uma vez que esta parte de um princípio geral para um caso específico. Ou seja, baseia-se em teorias ou regras generalizadas, que são posteriormente aplicadas e testadas através de exemplos concretos (Glaser, 2016).

A relação entre as estratégias de cibersegurança e a confiança do consumidor é explorada através da perceção dos mesmos sobre estas práticas no contexto das PME.

A esta abordagem alia-se o paradigma do *Realismo Crítico* que defende que aquilo que é percecionado foi construído socialmente, sendo separado da ação humana. No contexto deste estudo e, tendo em consideração o defendido pelo paradigma, é pretendido analisar o efeito das estratégias de cibersegurança das PME na confiança do consumidor (Hu, 2018).

2.2. Cibersegurança

Segundo o Centro Nacional de Cibersegurança em Portugal, a cibersegurança é definida através de *"[...] medidas e ações de prevenção, monitorização, deteção, reação, análise e correção que visam manter o estado de segurança desejado e garantir a confidencialidade, integridade e disponibilidade da informação [...] no ciberespaço, e das pessoas que nele interagem" (CNCS - Glossário*, 2024). A proteção dos sistemas de informação, incluindo *software* e *hardware*, é essencial para salvaguardar os dados de todos os intervenientes que interagem no ciberespaço. Estes sistemas estão sujeitos a diversas ameaças e intimidações, tornando fundamental a implementação de medidas de segurança eficazes para garantir a integridade, confidencialidade e disponibilidade da informação (Bendler & Felderer, 2023).

Desta forma, é a implementação de políticas de segurança que condicionam possíveis ameaças e vulnerabilidades no ciberespaço, assegurando a confiabilidade da infraestrutura global. (Ali et al., 2025). A sua importância remete à crescente colisão entre os dois mundos, o mundo físico e real e o mundo digital. Tal acontecimento conduziu à denominação da "cibersegurança organizacional", destinando-se apenas aos procedimentos praticados por parte das organizações para proteger as suas informações. O seu intuito é preservar a informação armazenada pelos seus sistemas independentemente do modo como estes se encontram ou através de que tipo de ameaça ou vulnerabilidade podem ser afetados (Dalal et al., 2021).

A linguagem desenvolvida pelos investigadores de cibersegurança é bastante complexa e um tema ainda em desenvolvimento, constituindo desde o início uma barreira linguística relevante. Tal prejudica a ação por parte de indivíduos que não detenham conhecimentos relevantes de cibersegurança, o que, por sua vez, prejudica a forma como estes percecionam a segurança digital. Durante o seu artigo, Dalal et al. (2021), divide a população em duas subcategorias, os *end-users*, isto é, os utilizadores finais e os *cybersecurity-focused employees,* ou seja, funcionários focados em cibersegurança. A primeira divisão destina-se a todos os funcionários em contacto com a informação digital da organização para a qual trabalham. Estes podem não ter a predisposição para prejudicar a empresa de forma consciente, mas estariam mais suscetíveis a serem vítimas de ciberataques. Outras podem intencionalmente prejudicar a empresa através da prática de ciberataques perpetuados pelos mesmos (Dalal et al., 2021).

A segunda divisão da população destina-se aos colaboradores cujo trabalho envolve diretamente contactar com cibersegurança, seja através da mitigação de vulnerabilidades ou da melhoria dos sistemas de proteção e prevenção de ciberataques. No entanto, uma vez que estes colaboradores também são consumidores finais, inserem-se como subcategoria da primeira divisão. Assim, o modo como um colaborador lida com a cibersegurança estará relacionado com a sua atitude perante a empresa (Dalal et al., 2021).

Não são apenas os colaboradores e as medidas implementadas pelas empresas que influenciam a adoção da cibersegurança; a capacidade, perceção e recursos de um país também desempenham um papel determinante. Segundo Ali et al. (2025), embora a utilização limitada de infraestruturas digitais possa mitigar o risco de ciberataques, tal não implica necessariamente que estes sistemas sejam capazes de resistir a ataques sofisticados. Neste artigo, é analisado um caso prático em que a reduzida utilização de recursos digitais conduz a um menor risco de ciberataques. No entanto, esta limitação pode levar ao surgimento de ameaças distintas daquelas que ocorreriam num cenário com maior adoção tecnológica (Ali et al., 2025). O estudo sugere, ainda, que a natureza dos ciberataques pode ser influenciada pelo nível do desenvolvimento económico e tecnológico do país em questão, uma vez que este fator pode determinar o grau de interesse da informação disponível para os criminosos. A execução dos ataques envolve custos, o que pode condicionar a escolha dos alvos e a sofisticação das ameaças perpetradas. Um outro fator a considerar para a possível baixa perceção dos ciberataques é a inexistência de uma legislação robusta, o que origina um registo insuficiente de cibercrimes. A escassez de relatórios e dados concretos dificulta a compreensão das razões subjacentes à aparente tipologia de ciberataques e

sua frequência (Ali et al., 2025).

A cibersegurança assenta na implementação de diversas medidas destinadas a proteger redes de computadores contra cibercriminosos, prevenindo a introdução de *malware*, isto é, um *software* utilizado para proliferar vírus num dispositivo, e garantindo a integridade dos sistemas. Entre essas medidas, destaca-se a segurança do *software* através da utilização de antivírus, autenticação multifator, encriptação e *firewalls*. Um *malware,* segundo a *European Union Agency for Cybersecurity* (ENISA), é uma ação de *software* ou *firmware* com o intuito de prejudicar um sistema. No caso da *firewall*, esta caracteriza-se como um sistema que utiliza regras para controlar as comunicações numa rede. Estes mecanismos desempenham um papel fundamental na proteção das redes contra ameaças internas e externas. Com o desenvolvimento tecnológico constante, torna-se cada vez mais desafiante a aplicação de medidas de segurança, seja devido às limitações dos sistemas, seja pelo elevado custo associado à sua implementação (Alhasan et al., 2024; Alsharida et al., 2023; Ani et al., 2016; "ENISA Threat Landscape 2024," 2024).

A restrição de acesso a informação confidencial ou de elevado valor deve ser acompanhada de um sistema de rastreamento que registe quem acede aos dados, bem como os processos de armazenamento, divulgação e eliminação da informação (Alhasan et al., 2024).

A utilização da computação em nuvem pode representar uma vantagem significativa para o armazenamento seguro de dados, proporcionando avançados mecanismos de proteção. No entanto, a segurança organizacional não deve assentar exclusivamente em soluções tecnológicas, sendo essencial a formação contínua dos trabalhadores. Entre as boas práticas a promover, incluem-se normas como a não utilização de dispositivos *USB* desconhecidos, confidencialidade de informações sensíveis e precaução no acesso a *e-mails* suspeitos, prevenindo potenciais ataques (Alhasan et al., 2024).

De forma a assegurar a segurança dos sistemas, foi desenvolvida uma tríade fundamental na cibersegurança, designada por Confidencialidade, Integridade e Disponibilidade (CIA). Esta estrutura permite avaliar vulnerabilidades e definir soluções para garantir a proteção dos dados e dos sistemas de informação (Bagies, 2024).

A confidencialidade refere-se à garantia da privacidade dos dados, assegurando que apenas utilizadores autorizados possam aceder às informações. Para tal, são empregues técnicas como a encriptação e a classificação dos dados, protegendo-os contra acessos indevidos. A integridade visa prevenir alterações não autorizadas nos dados, garantindo que a informação permanece precisa e confiável. Para alcançar este objetivo, são implementadas medidas como cópias de

segurança (*backups*) e verificações regulares de segurança. A disponibilidade refere-se à capacidade de manter o sistema acessível e operacional, minimizando períodos de inatividade ou interrupções (Bagies, 2024).

A tríade CIA foi desenvolvida como um princípio fundamental para analisar vulnerabilidades e reforçar a segurança dos sistemas de informação. Um sistema que não contemple estes três elementos é considerado vulnerável e inadequado para garantir a proteção dos dados. No entanto, mesmo após sofrer um ciberataque, um sistema pode manter a confiabilidade da informação se possuir medidas de mitigação adequadas (Bagies, 2024).

A adoção de bloqueios complexos no sistema para manter estes princípios em funcionamento pode comprometer a disponibilidade, resultando na não concretização das medidas de prevenção propostas pela tríade (Ani et al., 2016).

2.3. Ciberespaço

O ciberespaço é uma espécie de mundo digital dinâmico onde qualquer ameaça, desequilíbrio ou dificuldade pode prejudicar o dia a dia de qualquer cidadão (Alhasan et al., 2024). Trata-se de um espaço intangível que alterou profundamente as fronteiras tradicionais dos Estados, tornando obsoleta a visão clássica da soberania territorial. Neste contexto, torna-se imprescindível a implementação de novas medidas de controlo, uma vez que os mundos físico e virtual se encontram cada vez mais interligados. A digitalização facilitou, entre outras transformações, a transmissão de informação em tempo real (Ciberdefesa, 2018).

As definições de ciberespaço têm evoluído em função das necessidades emergentes e das finalidades das entidades oficiais (Ning et al., 2018). A sua principal finalidade reside na prestação eficiente de serviços digitais que satisfaçam necessidades críticas, como a proteção de dados, a segurança das comunicações globais, o armazenamento em nuvem, a gestão de reservas, entre outras (Ning et al., 2018).

A União Europeia reconhece o ciberespaço como o quinto domínio operacional, a par da terra, do mar, do ar e do espaço. Este domínio abrange redes de informação e telecomunicações, bem como sistemas informáticos, sendo cada vez mais contestado, dado que ataques neste âmbito têm o potencial de afetar simultaneamente as dimensões físicas e digitais da sociedade. Em resposta, os Estados-membros têm vindo a coordenar operações conjuntas com o objetivo de proteger os cidadãos europeus contra as ciberameaças, reforçando a defesa neste domínio. Em

2023, a assinatura da "Bússola Estratégica da UE" representou um marco nesse esforço conjunto, ao identificar o ciberespaço como um espaço de disputa estratégica, onde a competição entre países é influenciada por fatores históricos e dinâmicas internacionais. Assim, a política de defesa da União Europeia assenta na consolidação de uma estrutura robusta de cibersegurança, sustentada por um investimento contínuo de todos os Estados-membros. Esta abordagem visa proteger o ecossistema digital e estabelecer mecanismos comuns de defesa (Smith, 2023; Ciberdefesa, 2018).

Com o tempo, o ciberespaço tornou-se um campo privilegiado para a realização de ataques, frequentemente perpetrados por Estados soberanos com o intuito de desestabilizar outras sociedades, ameaçar atores internacionais e exercer formas de chantagem. O seu caráter complexo e a multiplicidade de atores envolvidos nas atividades maliciosas representam um desafio significativo. Por essa razão, torna-se fundamental implementar medidas de proteção e regulamentação, baseadas em normas educativas e formativas, que permitam à União Europeia fortalecer as suas políticas de cibersegurança e garantir uma defesa mais eficaz (Smith, 2023; Ciberdefesa, 2018).

2.4. Cibercrime e Ciberameaça

Determinados ataques de cibersegurança revelam-se uma ameaça significativa para as vítimas, muitas das vezes devido à sua falta de conhecimento sobre defesa e identificação de diversas tipologias de ataques, em especial aqueles provenientes de técnicas de engenharia social. Isto é, técnicas de coagir os indivíduos a revelar informação confidencial, conforme anteriormente referido, através de ficheiros corrompidos ou acesso a serviços comprometidos (Ali et al., 2024).

Em situações de maior gravidade, um ciberataque pode constituir uma ameaça direta a um Estado, cujos interesses podem ser severamente afetados tanto a nível físico como financeiro. Estes ataques podem comprometer ficheiros económicos governamentais ou interferir no tráfego aéreo e terrestre, causando danos significativos à segurança nacional, à estabilidade económica e ao quotidiano de todos os intervenientes (Alhasan et al., 2024).

No artigo apresentado por Alhasan et al. (2024), os autores afirmam que uma das principais dificuldades na caracterização do ciberespaço se encontra na ausência de uma definição universal e objetiva do que constitui um ciberataque. A falta dessa definição inicial impossibilita a implementação de medidas concretas, uma vez que não se conhecem claramente as suas

tipologias, dificultando a responsabilização dos perpetradores e a compreensão das consequências destes crimes. Esta lacuna pode gerar incoerências tanto na formulação de estratégias de defesa como na aplicação de medidas judiciais (Alhasan et al., 2024).

Um ciberataque pode ser definido como um conjunto de ações de aproximação através da manipulação psicológica, ciberguerra, exploração de redes informáticas e comprometimento de medidas de segurança. O objetivo central é interferir no funcionamento adequado dos serviços das redes de informação e nos processos de tomada de decisão. As motivações para a realização de ciberataques podem variar. Em muitos casos, estão relacionadas com objetivos políticos, manifestando-se através da disseminação de mensagens de posicionamento ideológico, ou podem ter motivações financeiras. (Alhasan et al., 2024).

Neste sentido, Alhasan et al. (2024) salienta a importância de distinguir cibercrime, ciberguerra e a interseção entre ciberguerra e ciberataque. No que respeita ao cibercrime, este é a prática de crimes informáticos perpetrados por indivíduos não pertencentes a governos e sem motivação política. Em contrapartida, a ciberguerra é frequentemente indetetável e constitui uma arma utilizada em contextos políticos, causando danos significativos. Trata-se de uma capacidade adquirida por vários Estados, como a Rússia e os Estados Unidos da América, através de práticas de pirataria informática, considerando o ciberespaço como um verdadeiro campo de batalha. Este tipo de ataque pode provocar danos na reputação de um Estado e na sua economia, originar ruturas em alianças diplomáticas, comprometer a sua rede doméstica e perturbar serviços essenciais, como as infraestruturas hospitalares. Estes incidentes têm vindo a aumentar, não apenas entre Estados, mas também entre outras organizações, incluindo grupos terroristas e movimentos independentistas. Um dos possíveis ataques no contexto da ciberguerra é o *Denial-of-Service* (DoS; Alhasan et al., 2024; Goel, 2011).

Um ataque de DoS refere-se à interrupção do normal funcionamento de um sistema, levando à sua sobrecarga e, em muitos casos, à exigência de chantagem ou extorsão para restaurar a operação do mesmo. Um exemplo clássico de ataque DoS é o programa *worm*, que consiste na repetição automática de um programa através das redes de computadores. Inicialmente, o objetivo dos *worms* era utilizar os períodos de inatividade dos sistemas para executar tarefas úteis, sem prejudicar os utilizadores. Contudo, quando empregados em contextos de ciberataques, esses programas podem multiplicar-se de forma exponencial, sobrecarregando os recursos do sistema e tornando-o incapaz de operar de forma eficiente, comprometendo, assim, o seu normal desempenho (Overill, 1999).

Por fim, a interseção entre ciberguerra e ciberataque corresponde a ataques políticos ou de segurança com o objetivo de comprometer as redes de informação, afetando a soberania e a estabilidade dos Estados envolvidos (Alhasan et al., 2024).

O estudo apresentado no *Threat Landscape* 2024 pela ENISA, é possível observar que, à imagem do ano anterior de 2023, os ataques de *Ransomware* e de DoS representam mais de metade das ameaças analisadas, sendo a geopolítica um grande propulsor de ameaças à cibersegurança. Um ataque de *Ransomware* é caracterizado pela ENISA por ser uma forma de ataque onde a vítima é alvo de extorsão para conseguir recuperar os dados aos quais perdeu o acesso. Caso a vítima não ceda às exigências, existe a ameaça de divulgação pública dos dados comprometidos. Durante a elaboração do *Threat Landscape 2024*, o ataque de *Ransomware* destacou-se como um dos mais recorrentes. O relatório salienta, ainda que, os setores da administração pública, dos transportes e das finanças foram os mais visados durante os meses de julho de 2023 e junho de 2024. As motivações destes criminosos podem variar, sendo as mais comuns a chantagem, espionagem, eliminação de dados e ideologia ("ENISA Threat Landscape 2024," 2024).

Em 2018, foi criado o Regulamento Geral de Proteção de Dados (RGPD), com o objetivo de assegurar legalmente a privacidade dos dados pessoais, protegendo os direitos individuais no contexto digital. Este regulamento dita a forma como os dados são processados e armazenados, estabelecendo sanções significativas para as entidades que não cumpram as suas disposições. O RGPD impõe obrigações às organizações que tratam os dados de qualquer cidadão da União Europeia, independentemente da sua localização geográfica (Wolford, 2025; *Regulations*, 2003).

A adoção deste regulamento representou uma tomada de posição por parte da Europa contra a violação de dados, reforçando o compromisso com a segurança das organizações e dos indivíduos. As PME, em particular, são contempladas com derrogações específicas, bem como com códigos de conduta que consideram as suas características particulares. Estes códigos visam orientar a atuação dos responsáveis pelo tratamento de dados, tendo em consideração os riscos associados a esse tratamento (Wolford, 2025; *Regulations*, 2003; *Commission*, 2003).

Dado que a ação humana constitui um dos fatores mais críticos para a cibersegurança, seja através de erros ou de inexperiência, os cibercriminosos recorrem frequentemente a técnicas psicológicas para perpetrar os seus crimes (Ali et al., 2024; Alsharida et al., 2023). Assim, é comum a utilização de estratégias de roubo de credenciais digitais e a criação de identidades falsas com o objetivo de cometer diversas infrações através da engenharia social, um exemplo de

técnica psicológica de crime. Estas abordagens baseiam-se na construção de empatia e confiança com a vítima, levando-a, de forma inadvertida, a fornecer informações que comprometem a sua segurança. Frequentemente, os cibercriminosos fazem-se passar por indivíduos da confiança da vítima, de autoridade ou por representantes de organizações conhecidas, de modo a aumentar a credibilidade do seu discurso e, assim, persuadir a vítima a cumprir as suas exigências. Habitualmente, o contacto inicial ocorre sob o pretexto de um pedido de ajuda ou de uma ameaça, explorando o fator emocional para induzir a vítima ao erro. Importa, ainda, salientar que os cibercriminosos tendem, após obter acesso a determinados dados, a explorar a possibilidade de reutilização das mesmas credenciais em diferentes sistemas pertencentes à mesma vítima (Veiga, 2024; Ali et al., 2024).

No que diz respeito ao *phishing*, esta prática, também ela de cariz psicológico, consiste no envio de mensagens enganosas com o objetivo de obter informações pessoais das vítimas. De acordo com Ali et al. (2024), os cibercriminosos recorrem frequentemente à estratégia do *fear of missing out* (FOMO), ou seja, induzem no indivíduo o receio de perder um determinado serviço se este não agir de imediato. Esta técnica explora a curiosidade humana, levando a vítima a aceder impulsivamente num *link* malicioso que contém *malware* (Ali et al., 2024).

Outro exemplo de ciberataque é o *Man-in-the-Middle*, no qual o cibercriminoso intercepta a comunicação entre um utilizador e o destinatário final, que pode ser um serviço de uma empresa. Neste tipo de ataque, o criminoso posiciona-se entre as partes envolvidas sem que estas se apercebam, recolhendo informações sensíveis (Michelena et al., 2023).

Neste contexto, torna-se imprescindível estabelecer uma base sólida ao nível da literacia digital, de modo a capacitar os cidadãos com conhecimentos e estratégias eficazes para se protegerem de forma adequada (Ali et al., 2024).

A crescente tendência para ciberataques, especialmente contra empresas, exige destas uma atenção redobrada na proteção dos seus sistemas, dos consumidores com quem interagem e da própria organização (Ani et al., 2016).

2.5. Normas/Regulamentos

2.5.1. Selo Cibersegurança e Maturidade Digital

A certificação de maturidade digital funciona como uma marca que valida o compromisso de uma organização com a segurança, a privacidade, a sustentabilidade e a acessibilidade no

ambiente digital. Esta certificação, acessível a qualquer empresa, seja do setor público ou privado, distingue as organizações que adotam boas práticas de cibersegurança e que demonstram um elevado nível de maturidade digital. Permite impulsionar o tecido empresarial através da adoção de tecnologias inovadoras nos negócios, garantindo simultaneamente a segurança e proteção dos consumidores (*Certificação de Maturidade Digital*, 2022).

Com esta certificação, as empresas evidenciam-se capacitadas a quatro níveis fundamentais: cibersegurança, acessibilidade, privacidade e sustentabilidade, bem como numa dimensão global que integra todas estas áreas. Para cada certificação, está designada uma entidade competente responsável pela respetiva fiscalização (*Certificação de Maturidade Digital*, 2022; *Regulamento de Utilização Da Marca Nacional Selos de Maturidade Digital*, 2021).

No domínio da cibersegurança, a certificação comprova que a organização está preparada para enfrentar ciberataques e implementar estratégias eficazes de mitigação, sendo a entidade competente o Centro Nacional de Cibersegurança (CNCS). Esta segue o Quadro Nacional de Referência para a Cibersegurança (QNRCS) que se baseia nos parâmetros europeus. No que diz respeito à acessibilidade, promove-se uma melhoria na interação entre a organização e os utilizadores, a responsabilidade recai sobre a Agência para a Modernização Administrativa (AMA). No campo da privacidade, a certificação reflete a adoção de práticas rigorosas na gestão e armazenamento de dados pessoais, reforçando a proteção dos consumidores e restantes intervenientes, e a autoridade competente é a Comissão Nacional de Proteção de Dados (CNPD). Relativamente à sustentabilidade, incentiva-se a redução da pegada ecológica das empresas, promovendo a adoção de tecnologias e processos mais sustentáveis, a supervisão é assegurada pela Direção-Geral das Atividades Económicas (DGAE; *Certificação de Maturidade Digital*, 2022; *Regulamento de Utilização Da Marca Nacional Selos de Maturidade Digital*, 2021; *Selo de Cibersegurança, 2025*).

Dentro deste sistema de certificação, existem três níveis de exigência, designados por bronze, prata e ouro, que determinam o grau de compromisso da organização com os requisitos estabelecidos. O selo de maturidade digital global é atribuído às organizações que, no mínimo, atinjam o nível bronze em todas as categorias avaliadas, sendo o somatório dos pontos de cada nível (bronze – dois pontos, prata – três pontos e ouro – quatro pontos). Estes selos são reconhecidos pelo *Digital with Purpose,* um movimento internacional que visa promover modelos de negócio sustentáveis e tecnologicamente inovadores, alinhados com os Objetivos de Desenvolvimento Sustentável da ONU para 2030. Em Portugal, estas certificações são validadas

pelo Instituto Português de Acreditação (IPAC; *Certificação de Maturidade Digital*, 2022; *Regulamento de Utilização Da Marca Nacional Selos de Maturidade Digital*, 2021).

Para apoiar a transformação digital, especialmente em PME, o programa *Coaching 4.0* prevê incentivos financeiros destinados a fomentar a adoção da Certificação de Maturidade Digital, incentivando estas a expandirem a sua presença digital segura e a reforçarem a sua competitividade no mercado (*Certificação de Maturidade Digital*, 2022).

3. Capítulo 3: O Contexto das PME

3.1. Introdução às PME

Uma PME é uma categoria de empresas que engloba micro, pequenas e médias empresas com menos de 250 colaboradores e um volume de negócio atual inferior a 50 milhões de euros, isto é, um balanço anual de 43 milhões de euro máximos (*Commission*, 2003).

No caso das pequenas empresas, estas empregam um máximo de 50 trabalhadores e apresentam um volume de negócio anual de 10 milhões de euros. Já as microempresas são empresas com cerca de 10 funcionários e um volume de negócio anual igualmente limitado de 2 milhões de euros (*Commission*, 2003).

As PME, devido a sua dimensão necessitam de proprietários conhecedores e devidamente informados das melhores formas destas obterem sucesso, uma vez que os seus recursos e apoios são limitados, quer seja através da interação com os consumidores ou com outras empresas (Geneste & Galvin, 2013).

3.2. Cibersegurança nas PME

Com o contínuo avanço das tecnologias, os ataques à cibersegurança têm aumentado proporcionalmente, especialmente nos últimos anos. De acordo com Ali et al. (2025), um dos principais fatores que contribuem para este crescimento é o recurso à Inteligência Artificial, que, por sua vez, tem intensificado os custos associados a estes ataques, demonstrando um crescimento constante desde 2018 e sugere uma tendência de aumento até 2029. A fraca consistência na aplicação de medidas de prevenção nas PME, aliada à implementação do trabalho à distância, veio agravar a situação (Ali et al., 2025; Fedele & Roner, 2021).

Neste contexto, torna-se essencial proteger qualquer tipo de informação e dados no

ciberespaço através da implementação de medidas eficazes de cibersegurança. Os cibercriminosos veem as PME como alvos fáceis pelo facto de estas guardarem informações valiosas e por serem deficitárias em medidas de cibersegurança. Torna-se imperativo analisar a origem das ameaças, a capacidade de resposta e a ação da gestão (Saha & Anwar, 2024).

Quanto mais ataques estas empresas sofrem, mais evidente se torna o interesse nos dados que estas armazenam, uma vez que estes criminosos sabem que nem todas as empresas se preocupam da mesma forma com a cibersegurança (Saha & Anwar, 2024).

Segundo a tabela apresentada por Parsaei (2024), 66,1% dos inquiridos identificaram as redes como o principal alvo destes ataques, seguidas pelo *baiting*, técnica em que as vítimas descarregam *malware* de forma inadvertida, com 7,34%, e pelo *phishing*, com uma incidência de 6,21% (Parsaei, 2024).

Uma forma eficaz de garantir boas práticas de cibersegurança passa pelo investimento, por parte das PME, em medidas adequadas, tais como a realização de formações especializadas. Estas formações devem proporcionar aos colaboradores conhecimentos fundamentais sobre cibersegurança. A realização de simulações realistas de ciberataques, acompanhadas da implementação de estratégias de defesa e mitigação das mesmas, pode reforçar a capacidade de resposta das organizações. Para assegurar uma proteção contínua, é essencial que estas formações sejam periódicas, permitindo aos colaboradores manterem-se atualizados face às constantes evoluções no panorama das ciberameaças (Ali et al., 2024; Fallatah et al., 2024).

Além disso, as organizações devem adotar abordagens dinâmicas e contínuas no processo de aprendizagem. Este deve basear-se na avaliação do conhecimento e análise das atitudes dos colaboradores em relação à cibersegurança. Através da análise do conhecimento, dos valores, das atitudes e das crenças, torna-se possível prevenir e otimizar o comportamento da empresa e dos seus colaboradores no domínio da cibersegurança. (Ali et al., 2024; Alyami et al., 2023).

O programa *Security Education, Training, and Awareness* (SETA), por exemplo, visa a implementação de estratégias eficazes para a proteção dos ativos de informação e a redução de falhas de segurança. Este programa assume particular importância na prevenção de vulnerabilidades decorrentes de comportamentos inadequados por parte dos colaboradores. O SETA promove a adoção de boas práticas de segurança digital, o desenvolvimento de competências para a criação de soluções eficazes e a minimização de riscos, contribuindo, assim, para a consolidação de uma cultura organizacional estável e resiliente face às ameaças (Alyami et al., 2023). No entanto, como afirmado por Ali et al. (2024), este programa ainda apresenta

margem para melhorias, de modo a tornar-se mais eficaz e benéfico para as empresas.

Para garantir a segurança contínua, é essencial que as PME implementem protocolos de segurança que incluam atualizações regulares, autenticação multifator, palavras-passe robustas, e a contratação de gestores especializados. Estes profissionais devem avaliar a segurança da empresa e promover melhorias contínuas no *software* e manutenção dos sistemas, prevenindo erros e garantindo uma proteção mais robusta contra ameaças (Ali et al., 2024; Alhasan et al., 2024; Ani et al., 2016).

As empresas, ao recorrerem cada vez mais a meios digitais para a realização dos seus serviços, torna-se essencial adotar uma abordagem flexível e robusta frente às novas ameaças. Para além das estratégias anteriormente mencionadas, devem aliar a formação dos recursos humanos a medidas robustas para a proteção dos seus ativos digitais, acompanhando a evolução dos ciberataques (Ani et al., 2016; Balzano & Marzi, 2024).

A proteção e a resiliência são elementos essenciais da cibersegurança, permitindo às organizações mitigar e superar ataques maliciosos, frequentemente resultantes de políticas inadequadas e da insuficiência de conhecimentos especializados (Rawindaran et al., 2023; Veiga, 2024).

A implementação do RGPD estabelece diretrizes que promovem a cibersegurança, garantindo a proteção e a privacidade dos dados, de modo a evitar o seu extravio ou utilização pelos cibercriminosos. No entanto, o cumprimento dessas diretrizes exige um reforço significativo da segurança digital nas organizações, o que pode implicar investimentos financeiros consideráveis (Balzano & Marzi, 2024).

Além dos desafios na implementação de cibersegurança, as empresas devem enfrentar a necessidade de alinhar as suas políticas com normas nacionais e internacionais, adotar tecnologias avançadas e considerar questões éticas. Paralelamente, é crucial que as organizações integrem as estratégias de negócio com a responsabilidade social corporativa, promovam a sensibilização e incentivem a adoção das melhores práticas em cibersegurança. Este processo deve permitir a adaptação e evolução digital das suas infraestruturas, assegurar o cumprimento das leis, respeitando a privacidade e a proteção da informação armazenada e partilhada (Balzano & Marzi, 2024).

Quanto maior for o investimento de uma empresa em cibersegurança, menor será a probabilidade de ser alvo de um ataque. Um elevado nível de proteção aumenta a confiança dos consumidores, tornando a empresa uma escolha mais atrativa e fortalecendo a sua imagem no

mercado. Outro fator crucial é a concorrência. Se uma empresa concorrente investir mais em cibersegurança e, consequentemente, atrair mais consumidores devido à maior confiança e proteção dos seus dados, a empresa em questão terá de acompanhar esse investimento para não ficar em desvantagem competitiva. (Balzano & Marzi, 2024; Fedele & Roner, 2021).

Por fim, a implementação de medidas de cibersegurança envolve custos elevados, levando muitas empresas com recursos limitados a ponderar se devem ou não adotá-las. Estes investimentos são dispendiosos, irreversíveis e exigem atualizações constantes, o que pode levar algumas empresas a adiar a sua implementação para um momento mais oportuno. A baixa recorrência de ataques pode criar a perceção de que tais medidas não são prioritárias. Outro fator que contribui para essa hesitação é a ideia de que certas soluções de cibersegurança não apresentam resultados imediatos ou exigem complementação para serem eficazes (Fedele & Roner, 2021).

4. Capítulo 4: Comportamento do Consumidor e Cibersegurança

4.1. Introdução ao Comportamento do Consumidor

A cibersegurança não é apenas uma preocupação interna para as PME, mas também uma questão que influencia diretamente a relação com os consumidores e o seu comportamento de compra. As exigências da cibersegurança impactam diretamente a forma como as PME gerem os seus recursos tecnológicos e financeiros (Hoong et al., 2024).

Como explicado anteriormente, fatores como desafios financeiros, estrutura organizacional, o processo de digitalização e recursos tecnológicos insuficientes levam as PME a subestimar a cibersegurança. Em vez de adotar medidas preventivas, muitas PME preferem esperar pela ocorrência de um ataque, adotando uma postura reativa ao invés de proativa (Hoong et al., 2024).

Estas empresas enfrentam diariamente ciberameaças que condicionam o bom funcionamento dos seus sistemas, analisando apenas as ameaças que são visíveis, tornando-as vulneráveis às restantes condicionantes. A falta de infraestruturas de *software* e *hardware* e os medos de mudança impossibilitam a implementação de soluções de cibersegurança.

De acordo com Adjei et al. (2009), quando a segurança de uma marca é comprometida, a perceção negativa gerada tende a influenciar de forma muito mais intensa a decisão de compra, afetando negativamente a credibilidade da marca e dificultando a atração de novos consumidores. Por outro lado, a informação positiva contribui para a redução do risco percebido e para a

diminuição da desconfiança por parte do consumidor, favorecendo uma maior predisposição para a compra (Adjei et al., 2009).

4.2. Relacionamento entre as Variáveis

A Confiança do Consumidor resulta, em grande parte, do esforço das equipas de *marketing* em criar uma ligação sólida entre o consumidor e a empresa. Destaca-se que o risco influencia significativamente o processo de tomada de decisão dos consumidores. Quando existe uma probabilidade de confiança, especialmente se esta for positiva, aumenta também a predisposição do consumidor para realizar uma ação potencialmente favorável (Delgado-Ballester, 2004). Neste estudo, centramos apenas essa confiança relacionada à cibersegurança.

Este fator ajuda a explicar por que razão nem todas as PME aproveitam as oportunidades de expansão ou divulgação da mesma forma. O acesso limitado a recursos ou a dependência de outras organizações para a promoção dos seus produtos ou serviços, condiciona a forma como estas desenvolvem e estruturam as suas campanhas, moldando-as de maneira distinta (Delgado-Ballester, 2004).

Manter uma relação de confiança estável e duradoura com o consumidor revela-se crucial para o sucesso da empresa a longo prazo. No entanto, verifica-se que as PME tendem a estabelecer relações mais pontuais com os consumidores, o que as leva a investir em esforços adicionais para fortalecer esse tipo de ligação e em beneficiar da mobilidade dos consumidores entre empresas (Delgado-Ballester, 2004; Geneste & Galvin, 2013).

Este comportamento pode ser explicado pelo facto de as PME, por norma, disporem de menos recursos, o que as obriga a adotar uma posição de maior proximidade e confiança, de forma a compensar essa limitação (Geneste & Galvin, 2013).

É fundamental, portanto, que estas empresas invistam no conhecimento do negócio e dos seus consumidores, reconhecendo-o como uma fonte valiosa de competitividade face a outras empresas e como base para interações mais significativas (Geneste & Galvin, 2013).

Com o avanço da digitalização, as redes das empresas passaram a concentrar grandes volumes de dados pessoais que exigem uma proteção robusta. A possibilidade de que pessoas não autorizadas acedam a esses dados, seja de forma intencional ou acidental, compromete a confidencialidade das informações dos consumidores e colaboradores que interagem com a organização (Demirci & Yardan, 2023).

Neste contexto, a Privacidade assume um papel central ao impedir o acesso não autorizado a dados sensíveis. Quando os dados são partilhados em sistemas sem o consentimento explícito dos consumidores, torna-se imperativo que os gestores implementem medidas que assegurem o correto armazenamento e tratamento da informação. Paralelamente, os consumidores devem poder aceder, de forma clara e transparente, às políticas e práticas de gestão dos seus dados pessoais (Demirci & Yardan, 2023).

A adoção de estratégias eficazes de proteção da privacidade pode contribuir significativamente para o fortalecimento da confiança e da lealdade dos consumidores, incentivando o seu compromisso e envolvimento contínuo com a empresa (Demirci & Yardan, 2023).

O construto da Confiança nas PME está intrinsecamente relacionado com a lealdade dos consumidores. Quanto maior for o sentimento de confiança em relação a uma determinada marca ou empresa, maior será a probabilidade de esta beneficiar de vantagens como a captação de novos consumidores e a redução dos custos associados à sua divulgação (Chaudhuri & Holbrook, 2001).

Neste contexto, o consumidor tende a desenvolver uma ligação pessoal com a empresa, sentindo-se comprometido a recorrer novamente aos seus serviços e, em alguns casos, disposto a pagar mais pelo bem-estar e pela experiência proporcionados. Assim, fomenta-se o desejo mútuo de estabelecer uma relação mais duradoura e valiosa entre as partes (Chaudhuri & Holbrook, 2001).

O conceito de Lealdade pode ser definido como a escolha contínua de uma determinada marca por parte do consumidor, em detrimento de outras marcas concorrentes no mesmo nicho de mercado, ao longo de um período prolongado. Esta preferência mantém-se mesmo quando outras marcas apresentam alternativas potencialmente mais vantajosas (McMullan & Gilmore, 2003). Segundo Oliver (1999), a lealdade do consumidor corresponde à probabilidade de este voltar a adquirir um produto da mesma marca no futuro, mesmo perante tentativas de persuasão por parte da concorrência (McMullan & Gilmore, 2003).

A lealdade do consumidor pode também ser influenciada pela confiança, uma vez que este tende a aproximar-se de uma empresa cujos valores se alinham com os seus. Esta relação resulta na criação de uma aliança baseada no respeito e no compromisso entre o consumidor e a marca (Sirdeshmukh et al., 2002). A lealdade assume-se como um fator fundamental para os gestores, pois permite compreender as razões que levam os consumidores a permanecer fiéis a uma empresa, mesmo quando têm a possibilidade de mudar para a concorrência. Além disso,

possibilita a identificação dos motivos que levam à mudança de marca e das iniciativas que poderiam ter sido adotadas para evitar essa decisão (Mcmullan, 2005). Por isso, a lealdade exige que a relação de confiança seja continuamente cultivada (Yague-Guillen et al., 2003).

O *marketing* desempenha um papel fundamental na construção da lealdade positiva de uma empresa. No contexto das PME, a sua influência reflete-se no empenho no negócio, especialmente através da partilha de conteúdo nas redes sociais, que pode impactar potenciais consumidores (Prasad et al., 2017).

A utilização das redes sociais permite às PME expandir os seus nichos de mercado, aumentando a sua visibilidade e, consequentemente, os lucros. Esse crescimento financeiro proporciona uma maior margem para inovação e desenvolvimento. Assim, ao reforçar a confiança do consumidor, fortalece-se também a sua lealdade à marca (Prasad et al., 2017).

De acordo com o artigo de Haudi et al. (2022), recomenda-se a implementação de uma autenticação multifator para a proteção de dados na utilização das redes sociais, contribuindo para a segurança da informação e a confiança dos consumidores (Haudi et al., 2022).

O conceito de *Word of Mouth* (WOM) refere-se à intenção de um consumidor partilhar a sua experiência com um produto ou serviço, seja esta positiva ou negativa, influenciando, assim, a perceção de outros consumidores. Tal influência pode levar à adoção de um comportamento positivo ou negativo em relação a determinada empresa (Alexandrov et al., 2013).

Segundo Alexandrov et al. (2013), existem dois tipos de WOM: a positiva e a negativa. A WOM positiva resulta da satisfação do consumidor ao ver as suas necessidades atendidas, enquanto a WOM negativa ocorre quando o consumidor procura comparar empresas ou serviços de forma crítica, com o intuito de validar a sua opinião e auxiliar outros consumidores na tomada de decisões informadas (Alexandrov et al., 2013).

A execução do WOM pode ocorrer de forma direta, através da comunicação verbal entre consumidores acerca de uma questão específica, ou de forma indireta, através da divulgação nas redes sociais e outras plataformas digitais. Antes de recorrerem a uma empresa, os consumidores tendem a procurar informações ou opiniões sobre a mesma, como forma de garantir que a sua decisão é a mais segura e consciente (Delgado-Ballester, 2004).

No caso específico das PME, é comum que os consumidores investiguem se a organização já foi alvo de um ciberataque ou procurem conhecer a perceção pública relativamente ao tratamento de dados pessoais. Esta procura de informação baseada em consumidores ou ex-consumidores da empresa pode impactar a decisão do consumidor em interagir ou não com a mesma (Delgado-

Ballester, 2004).

Este é um dos construtos mais assentes na interação social e nos benefícios subsequentes para a empresa, resultantes da experiência do consumidor. Uma experiência negativa pode prejudicar seriamente a reputação da organização, dificultando a atração de novos consumidores, sobretudo se for disseminada a perceção de que o consumidor não se sentiu valorizado. Assim, o WOM é caracterizado pela carga emocional e pela opinião social que os consumidores partilham com o seu círculo de influência (Alexandrov et al., 2013).

5. Capítulo 5: Metodologia

5.1. Tipo de Estudo e Abordagem Metodológica

A metodologia constitui a base da dissertação, orientando o processo de recolha e análise de dados cruciais para o desenvolvimento da mesma. Assim, o capítulo seguinte é dedicado à descrição desse processo, em especial aos métodos de recolha e análise utilizados.

A estrutura inicial deste capítulo foi anteriormente delineada na Revisão de Literatura pertencente ao capítulo 2 e seguintes, de modo a desconstruir e clarificar alguns dos conceitos fundamentais do estudo.

Para além da apresentação do modelo de recolha e análise de dados, esta fase inclui ainda a abordagem ao paradigma de investigação adotado, ao modelo conceptual utilizado, assim como às hipóteses e variáveis em estudo.

Para possibilitar a medição das variáveis, foi adotada a escala de *Likert* com sete categorias, variando entre 1 – Discordo Totalmente e 7 – Concordo Totalmente. Esta escala foi utilizada como instrumento de medição no questionário aplicado para recolha de opiniões, permitindo assegurar uma maior confiabilidade nas respostas. Através desta escala, é possível aferir o grau de concordância dos inquiridos face às afirmações apresentadas (Pescaroli et al., 2020).

5.2. Problemática e Objetivos

A problemática levantada por este estudo debate-se com a perceção dos consumidores sobre a cibersegurança das PME e como esta afeta a sua confiança. Sendo assim, a investigação debate como o impacto das medidas de proteção de cibersegurança implementadas pelas PME afetam a confiança dos consumidores.

Posto isto, os objetivos do estudo passam pela análise da perceção dos consumidores em relação às medidas de cibersegurança, avaliação do impacto dessas medidas na construção positiva ou negativa da confiança dos consumidores, identificação das práticas mais valorizadas e as recomendações finais às PME sobre como reforçar a sua cibersegurança segundo a perceção do público-alvo.

O foco do estudo encontra-se no consumidor e nas medidas de cibersegurança que este considera mais relevantes para que a sua proteção seja assegurada.

5.3. Paradigma de Investigação

A utilização do método quantitativo revela-se essencial para a tomada de decisões informadas, baseadas em dados concretos, como números e análises objetivas (Lim, 2024).

Com o avanço da digitalização, torna-se cada vez mais premente o acesso a dados fiáveis, sendo o método quantitativo particularmente adequado, uma vez que permite a formulação e análise de hipóteses de forma célere, conduzindo a conclusões objetivas e imediatas (Lim, 2024).

Este método, não só possibilita a criação de estratégias relevantes para a prática real, como também assegura um elevado grau de rigor científico, ultrapassando a mera produção de dados académicos (Lim, 2024).

Neste estudo, realiza-se a recolha de dados que permitem identificar a confiança dos consumidores nas PME baseada nas práticas adotadas.

5.4. Método de Recolha de Dados

O presente estudo adota uma abordagem quantitativa, descritiva e de correlação, com o objetivo de analisar a relação entre as variáveis Confiança, perceção de cibersegurança, Lealdade e comportamento do consumidor quanto às PME.

Foi, por isso, criado um questionário *online* a diferentes consumidores com recurso às escalas já existentes e validadas na literatura.

6. Capítulo 6: Modelo Conceptual

6.1. Definição do Modelo Conceptual

Inicialmente, o modelo conceptual foi voltado para a perceção dos gestores sobre a importância da cibersegurança para a Confiança do Consumidor. O modelo explora a relação entre a implementação de estratégias de cibersegurança, confiança do consumidor e variáveis como a Lealdade e o *Word of Mouth* (WOM).

No entanto, com o desenvolvimento do estudo, surgiram dificuldades em abordar um tema tão sensível. Posto isto, o foco principal do modelo foi alterado para abranger também os consumidores das PME, passando a integrar um questionário destinados aos consumidores.

A Lealdade e o WOM surgem como consequência da relação com as variáveis, Perceção/Conhecimento sobre a estratégia de cibersegurança, Confiança na PME, Privacidade de dados e Confiança do Consumidor.

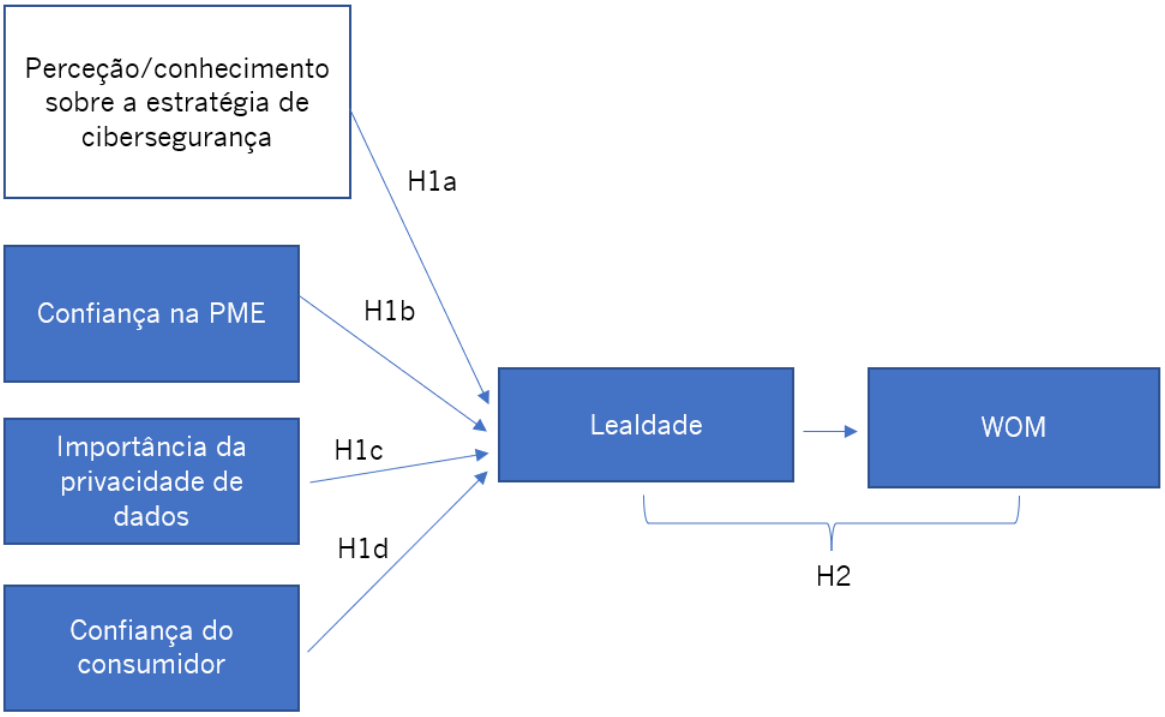


Figura 1 - Modelo Conceptual

Fonte – Conceção Própria

As variáveis que fundamentam o modelo conceptual originaram duas hipóteses principais e quatro sub-hipóteses. Cada uma dessas hipóteses corresponde a uma correlação entre duas

variáveis, as quais foram recolhidas e analisadas no estudo utilizando o método quantitativo.

O estudo pressupõe a existência de uma relação entre a perceção dos consumidores, a Confiança, a Privacidade dos dados e a Confiança do Consumidor, variáveis que se encontram correlacionadas com a Lealdade e o WOM.

Assim, as hipóteses são:

Hipótese 1a: A perceção/conhecimento dos consumidores sobre as estratégias de cibersegurança adotadas pela empresa está positivamente correlacionada com a Lealdade do consumidor. Tal implica que, à medida que aumenta o nível de conhecimento dos consumidores sobre as práticas de cibersegurança, aumenta também a sua predisposição para se manter fiel à empresa.

Hipótese 1b: A Confiança na PME está positivamente correlacionada com a Lealdade do consumidor. Neste contexto, destaca-se que a credibilidade e a fiabilidade da empresa influenciam diretamente a confiança dos consumidores.

Hipótese 1c: A importância atribuída pelos consumidores à Privacidade de Dados está positivamente correlacionada com a Lealdade do consumidor. Os consumidores que atribuem grande importância à proteção dos seus dados pessoais tendem a manter-se fiéis às empresas que valorizam essa preocupação.

Hipótese 1d: A Confiança do Consumidor está positivamente correlacionada com a Lealdade do consumidor. Esta é influenciada pela satisfação do consumidor e pelas suas experiências anteriores, servindo de base para as conclusões que formula sobre a empresa.

Hipótese 2: A Lealdade do consumidor está positivamente correlacionada com o WOM positivo. Dessa forma, os consumidores tendem a recomendar as empresas com as quais sentem uma maior ligação emocional, assumindo o papel de promotores da marca.

6.2. Variáveis do Modelo Conceptual

Construto	Escala	Referência
Confiança PME (Trust)	Escala de 7 pontos: 1 = discordo fortemente, 7 = concordo fortemente -Confio nesta marca -Conto com esta marca	(Chaudhuri & Holbrook, 2001)

	-Esta é uma marca honesta -Esta marca é segura Afeto pela marca: Sinto-me bem quando uso esta marca Esta marca faz-me feliz	
Lealdade (Loyalty)	Escala de 7 pontos: 1 = discordo fortemente, 7 = concordo fortemente -[Marca], gosto de comprar em qualquer altura -[Marca], comprarei na minha próxima ida (às compras) -[Marca], comprarei frequentemente nos próximos meses -[Marca], comprarei mais do que comprarei concorrentes	(Heinberg et al., 2015) (Oliver, 1999)
WOM - Word of Mouth	Escala de 7 pontos: 1 = discordo fortemente, 7 = concordo fortemente Qual seria a probabilidade de fazer uma das seguintes ações ... -Dizer coisas positivas sobre esta marca -Recomendar esta marca a outras pessoas -Recomendar esta marca a outra pessoa que procure o meu conselho	(Alexandrov et al., 2013)

Confiança consumidor	A [X] a é uma marca que corresponde às minhas expectativas Sinto-me confiante na marca [X] [X] é uma marca que nunca me desilude A marca [X] garante-me satisfação A marca [X] seria honesta e sincera na resposta às minhas preocupações Posso confiar na marca [X] para resolver um problema A marca [X] faria todos os esforços para me satisfazer A marca [X] compensar-me-ia de alguma forma pelo problema com o [produto]	(Delgado-Ballester, 2004)
Privacidade	Benefício e satisfação Segurança Partilha Privacidade Utilização	(Demirci & Yardan, 2023)

Tabela 1 - Escalas de Medição das Variáveis dos Construtos Utilizados

Como demonstrado na Revisão de Literatura, estes constructos assumem uma posição determinante no modelo. A Confiança assume-se como um fator importante para a lealdade dos consumidores nas PME, o que influencia diretamente a sua relação e preferência pela marca face às investidas da concorrência (Delgado-Ballester, 2004).

O WOM adquire um fator relevante neste contexto podendo impactar a perceção dos consumidores de uma empresa de forma positiva ou negativa. A este construto une-se a cibersegurança e a gestão da empresa, também eles fulcrais na manutenção da confiança do consumidor (Alexandrov et al., 2013). Tendo em consideração os recursos limitados das PME, o

aumento da relação de confiança e proximidade para com o consumidor tem de depender de conhecimentos do mercado relativamente à competitividade (Geneste & Galvin, 2013).

A Lealdade é construída e reforçada através da conexão dos valores do consumidor para com a empresa a que este recorre, sendo ela também influenciada pela confiança (Sirdeshmukh et al., 2002).

Por último, a Privacidade de Dados torna-se critica quando os consumidores avaliam as ações da empresa quanto às medidas de cibersegurança antes de tomar uma decisão informada (Demirci & Yardan, 2023).

Assim, estes construtos convergem em prol da competitividade e sustentabilidade das PME no ambiente digital. Estes foram medidos num questionário *online* segundo a escala da *Likert* de 7 pontos.

7. Capítulo 7: Amostragem e Instrumentos de Pesquisa

7.1. Processo de Amostragem

Para o desenvolvimento da presente investigação, recorreu-se ao método de amostragem por conveniência. Foi utilizado o recurso ao *Google Forms* para elaborar o *design* do questionário e este foi distribuído através de diversas plataformas *online*, nomeadamente o *e-mail* institucional, a rede social *Facebook* (em grupos específicos dedicados à partilha de questionários para dissertações) e a aplicação *WhatsApp*.

A recolha de dados decorreu entre os dias 6 de fevereiro e 16 de março, período durante o qual o questionário se manteve ativo com o objetivo de obter o maior número de respostas possível. Ao ser encerrado, o questionário registou 233 respostas, das quais 232 foram consideradas válidas.

Os dados recolhidos foram posteriormente processados e analisados com recurso ao *software* de análise estatística *Statistical Package for the Social Sciences* (SPSS).

7.2. *Design* do Questionário

O questionário desenvolvido foi dividido em duas partes, sendo a primeira sobre questões sociodemográficas (género, idade, nível de escolaridade, nacionalidade, ocupação/profissão, concelho de residência, conhecimento de cibersegurança e ciberataque, se está ciente das

medidas que as empresas adotam ao nível da cibersegurança e quais as ações que as empresas deveriam tomar). A segunda parte composta por itens relacionados às variáveis que constam no modelo conceptual. Foi concebido de forma a não ultrapassar os 4 a 5 minutos de duração, visando garantir uma maior colaboração por parte dos inquiridos.

As questões foram formuladas com caráter obrigatório e organizadas de acordo com uma sequência lógica, desde dar um conhecimento prévio das definições dos conceitos, à criação de um cenário fictício até às questões sobre as variáveis, orientando os participantes durante o preenchimento.

Para facilitar a compreensão, foi criada uma empresa fictícia, com um cenário modelo, para contextualizar os consumidores e permitir respostas mais informadas. Além disso, foram fornecidas definições de cibersegurança, ciberataque e PME, a fim de situar adequadamente os inquiridos.

A primeira secção consistia numa questão relacionada com a disposição dos inquiridos em participar no estudo. A segunda secção era composta pelas perguntas sociodemográficas previamente mencionadas.

A terceira secção, composta por quatro questões, tinha como objetivo avaliar o entendimento dos inquiridos sobre a definição de cibersegurança e ciberataque, bem como o seu conhecimento acerca das medidas de proteção implementadas pelas PME e as ações que consideravam necessárias para prevenir ciberataques. Nesta secção, as perguntas eram formuladas em formato de resposta “Sim” ou “Não” e em “escolha múltipla” para que os inquiridos selecionassem a ação mais relevante para si.

A quarta secção apresentava a descrição da empresa fictícia, seguida de oito perguntas relacionadas com o cenário da PME apresentado, solicitando aos inquiridos que indicassem como agiriam nas situações descritas, com recurso à variável Confiança na PME (Chaudhuri & Holbrook, 2001).

O cenário fictício era o seguinte:

A empresa *Jorge*, uma PME bem estabelecida no mercado nacional, sofreu recentemente um ciberataque que bloqueou o acesso aos vários sistemas da empresa.

Imediatamente após a deteção da ameaça, a equipa de cibersegurança da empresa ativou o protocolo de resposta a incidentes e comunicou aos consumidores o ocorrido.

Apesar de todos os esforços para controlar os danos e reforçar a segurança, as reações dos consumidores foram mistas. Alguns perderam completamente a confiança na empresa, considerando o ataque inaceitável, enquanto outros apreciaram a forma transparente como a empresa comunicou o sucedido. No entanto, uma outra parte, embora não vissem a sua confiança afetada, preferiam não ter sido informados sobre o ataque.

Figura 2 - Cenário Fictício Criado no Questionário

Nas secções subsequentes, tal como ocorreu na quarta secção, as perguntas foram formuladas com base na escala de *Likert*, variando de 1 -Discordo Totalmente a 7 - Concordo Totalmente. Os participantes deveriam considerar o cenário da empresa "Jorge" ao responder.

Na quinta secção, composta por quatro questões, os inquiridos foram convidados a avaliar a variável da Lealdade (Heinberg et al., 2015; Oliver, 1999) que sentiam em relação à empresa, abrangendo desde o seu gosto por comprar na empresa até à sua disposição para continuar a realizar compras após o incidente descrito.

A sexta secção, com três questões, abordava a predisposição dos inquiridos para recomendar a empresa através da variável WOM (Alexandrov et al., 2013).

A sétima secção, composta por oito perguntas, investigava a variável Confiança do Consumidor (Delgado-Ballester, 2004) na empresa, abordando questões como o nível de proteção percebido, se se sentiam desiludidos ou confiantes em relação à mesma.

Por fim, a última secção, com cinco questões, questionava os inquiridos sobre a sua satisfação em relação à variável Privacidade dos Dados (Demirci & Yardan, 2023), se consideravam que a empresa tomava as melhores decisões quanto à partilha e tratamento das suas informações e se tinham conhecimento sobre as práticas adotadas pela empresa nesse sentido.

O modelo do formulário encontra-se no Capítulo 11 - Anexo.

8. Capítulo 8: Análise de Dados e Resultados

8.1. Método de Análise de Dados

O Capítulo 8 é dedicado à análise dos dados recolhidos e à sua respetiva apresentação. Assim, este capítulo encontra-se organizado em três partes: a análise descritiva dos dados e das variáveis utilizadas, a caracterização da amostra e a análise das correlações identificadas.

8.2. Análise Descritiva das Variáveis

Ao abordar a análise quantitativa, é inevitável associá-la à análise estatística dos dados, uma vez que o seu principal objetivo consiste em transformar os dados recolhidos em informação relevante e significativa (Coutinho, 2020).

Inicialmente, será utilizada a estatística descritiva, permitindo organizar e descrever os dados, identificar valores extremos, estabelecer relações, testar hipóteses e, em última instância, responder ao problema em estudo. Esta abordagem proporciona uma primeira leitura dos dados recolhidos e permite definir a forma mais adequada de prosseguir com a investigação (Coutinho, 2020).

As variáveis apresentadas, como analisado durante a Revisão de Literatura, correspondem a construtos previamente existentes. Para medir a Confiança na PME recorreu-se à escala utilizada por Chaudhuri & Holbrook (2001) e para medir a Lealdade foi utilizada a escala combinada dos autores Heinberg et al. (2015) e de Oliver (1999). Para a medição da recomendação da empresa foi utilizado o WOM referente ao autor Alexandrov et al. (2013) e para medir a Confiança do Consumidor ao nível da cibersegurança surgiu a escala de Delgado-Ballester (2004). Por fim, a Privacidade de Dados foi avaliada segundo Demirci & Yardan (2023).

8.3. Caracterização da Amostra

Começando pela análise das primeiras questões de carácter sociodemográfico, e conforme apresentado na Tabela 2, das 232 respostas válidas, 168 inquiridos identificaram-se como sendo do género feminino (72,4%), enquanto 58 se identificaram como do género masculino (25%).

No campo "outros", 2 inquiridos indicaram a opção "não-binário" (0,9%) e 4 selecionaram "prefiro não dizer" (1,7%), perfazendo um total de 6 respostas (2,6%).

Género

	Frequência	Percentagem
Feminino	168	72,4
Masculino	58	25,0
Outro	6	2,6
Total	232	100,0

Tabela 2 - Amostra do Género dos Inquiridos

Seguindo com a análise dos dados sociodemográficos, foi questionada a idade dos inquiridos, a qual variou entre os 18 e os 56 anos ou mais.

A maior parte dos inquiridos encontra-se na faixa etária dos 18-35 anos, totalizando 201 participantes, o que corresponde a 86,6% do universo da amostra.

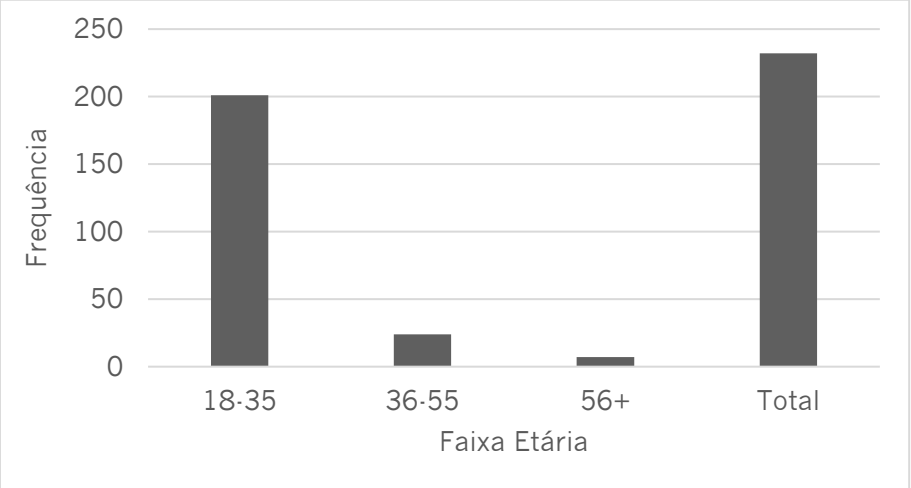


Tabela 3 - Amostra da Idade dos Inquiridos

Relativamente à nacionalidade, a maioria dos inquiridos é de nacionalidade portuguesa, totalizando 221 participantes, o que corresponde a 95,3% da amostra. A seguir, encontram-se os inquiridos de nacionalidade brasileira (3 participantes, 1,3%), angolana (2 participantes, 0,9%), francesa (2 participantes, 0,9%), cabo-verdiana (1 participante, 0,4%), chilena (1 participante, 0,4%) e indiana (1 participante, 0,4%). Por fim, 1 inquirido (0,4%) optou por não revelar a sua nacionalidade.

Nacionalidade

	Frequência	Percentagem
Prefiro não dizer	1	0,4
Angolana	2	0,9
Brasileira	3	1,3
Cabo-verdiana	1	0,4
Chilena	1	0,4
Francesa	2	0,9
Indiana	1	0,4
Portuguesa	221	95,3
Total	232	100,0

Tabela 4 - Amostra da Nacionalidade dos Inquiridos

No que concerne ao local de residência, a distribuição dos inquiridos encontra-se representada na tabela seguinte, sendo a região Norte aquela que concentra a maioria dos participantes.

Destaca-se, em particular, o concelho de Braga, com 60 inquiridos, correspondendo a 25,9% da amostra.

Concelho de residência

	Frequência	Percentagem
Prefiro não dizer	3	1,3
Internacional	3	1,2
Almada	1	0,4
Amarante	2	0,9
Amares	2	0,9
Armamar	4	1,7
Aveiro	2	0,9
Barcelos	21	9,1
Braga	60	25,9
Bragança	1	0,4
Caldas da Rainha	1	0,4

Chamusca	1	0,4
Chaves	1	0,4
Coimbra	1	0,4
Esposende	1	0,4
Fafe	3	1,3
Faro	1	0,4
Felgueiras	1	0,4
Funchal	1	0,4
Golegã	1	0,4
Gondomar	9	3,8
Guimarães	11	4,7
Lamego	1	0,4
Leiria	1	0,4
Lisboa	4	1,7
Loures	1	0,4
Lousã	1	0,4
Lousada	2	0,9
Maia	9	3,9
Mangualde	1	0,4
Marco de Canaveses	1	0,4
Matosinhos	7	3,0
Odivelas	1	0,4
Ovar	2	0,9
Pacos de Ferreira	1	0,4
Porto	31	13,4
Póvoa de Lanhoso	1	0,4
Póvoa de Varzim	1	0,4
Seixal	1	0,4
Sintra	2	0,9
Trofa	1	0,4
Valongo	5	2,2

Viana do Castelo	4	1,7
Vila do Conde	2	0,9
Vila Nova de Cerveira	1	0,4
Vila Nova de Famalicão	10	4,3
Vila Nova de Gaia	5	2,2
Vila Real	3	1,3
Vila Verde	2	0,9
Total	232	100,0

Tabela 5 - Amostra do Concelho de Residência dos Inquiridos

Relativamente ao nível de escolaridade concluído, a maioria dos inquiridos indicou possuir o grau de licenciatura, totalizando 115 participantes (49,6%). No total, cerca de 181 inquiridos (78%) referiram ter formação ao nível do ensino superior

Nível de escolaridade (concluído)

	Frequência	Percentagem
1º ciclo (4º ano)	1	0,4
2º ciclo (6º ano)	3	1,3
3º ciclo (9º ano)	1	0,4
Doutoramento	4	1,7
Ensino secundário	46	19,8
Licenciatura	115	49,6
Mestrado	51	22,0
Pós-graduação	11	4,7
Total	232	100,0

Tabela 6 – Amostra do Nível de Escolaridade dos Inquiridos

No que se refere à ocupação ou profissão, a maioria dos inquiridos indicou ser estudante, totalizando 125 participantes, o que representa 53,9% da amostra.

Ocupação/Profissão

	Frequência	Percentagem
Account Manager	1	0,4
Administração/gestão	2	0,8
Advogada	1	0,4
Analista de Inovação	1	0,4
Analista Financeiro	1	0,4
Aposentada	1	0,4
Assessora Comercial	1	0,4
Assistente administrativa	1	0,4
Assistente comercial	1	0,4
Assistente de vendas	1	0,4
Astrofísica	1	0,4
Auxiliar de saúde	1	0,4
Bancária	2	0,8
Canalizador	1	0,4
Clinical geneticist scientist	1	0,4
Comercial têxtil	1	0,4
Comerciante	1	0,4
Construtor Civil	1	0,4
Contabilista	1	0,4
Data analyst	1	0,4
Desempregada	4	1,8
Designer	3	1,3
Direção	1	0,4
Diretor de obras	1	0,4
Enfermeira	1	0,4
Engenharia industrial	1	0,4
Engenheira química	1	0,4
Engenheiro informático	4	1,7
Ensino	1	0,4

Escriturária	1	0,4
Estágio curricular	1	0,4
Estudante	125	53,9
Estudante/Bolseira de investigação	5	2,2
Financeira	1	0,4
Fisioterapeuta	1	0,4
Funcionário público	2	0,8
Gestão de Marketing	1	0,4
Gestão de Projetos	3	1,2
Inspetor Tributário	1	0,4
Investigador	2	0,8
Jogadora Futebol	1	0,4
Manager Recursos Humanos	1	0,4
Marketing Digital	1	0,4
Master Data Analyst	1	0,4
Operador Call Center	1	0,4
Operador de máquinas	1	0,4
Operador de supermercado	2	0,9
Operadora caixa	1	0,4
Operadora de loja	1	0,4
Operadora de supermecado	1	0,4
Professora	2	0,9
Profissional de estética animal	1	0,4
Profissional de saúde	1	0,4
Programador	1	0,4
Psicóloga	1	0,4
Quality Production Leader	1	0,4
Rececionista	2	0,8
Service Manager	1	0,4
Serviço ao cliente em loja	1	0,4
Software developer	1	0,4

Tech Consultant	1	0,4
Técnica auxiliar de saúde	1	0,4
Técnica de laboratório	1	0,4
Tecnica radiologia	1	0,4
Técnica superior	1	0,4
Técnico de Recursos Humanos	9	3,9
Técnico Solar FV	1	0,4
Terapeuta Ocupacional	1	0,4
Trabalhador-estudante	10	4,3
Uber eats	1	0,4
Total	232	100,0

Tabela 7 - Amostra da Ocupação/Profissão dos Inquiridos

Com o objetivo de aferir o nível de conhecimento sobre cibersegurança e ciberataques, os inquiridos foram questionados sobre esta temática. A análise dos dados revela que a maioria dos participantes demonstrou saber o que é um ciberataque (215 inquiridos, 92,7%) e o que é a cibersegurança (223 inquiridos, 96,1%).

No entanto, este conhecimento contrasta com o desconhecimento relativamente às práticas de cibersegurança implementadas pelas PME, expresso por 130 inquiridos (56%).

Relativamente às medidas consideradas mais prementes a adotar pelas PME, destacam-se o investimento em ferramentas de cibersegurança (90 respostas, 38,8%) e a monitorização contínua das redes e dos sistemas da empresa com o objetivo de prevenir ameaças (64 respostas, 27,6%).

Esta análise permite compreender a perceção dos consumidores relativamente ao conhecimento das medidas de cibersegurança. Ainda que demonstrem estar conscientes do que é a cibersegurança e reconheçam a gravidade dos ciberataques, a maioria (130 indivíduos, correspondendo a 56%) revela desconhecimento quanto às medidas de cibersegurança adotadas pelas empresas com as quais mantêm relações.

Este dado evidencia que a consciencialização relativamente ao risco permanece insuficiente e que muitos consumidores continuam a preferir expor os seus dados, assumindo esse risco.

Antes da definição apresentada, tinha conhecimento sobre o conceito de "cibersegurança"?

	Frequência	Percentagem
Não	9	3,9
Sim	223	96,1
Total	232	100,0

Tabela 8 - Amostra da Definição de Cibersegurança

Antes da definição apresentada, tinha conhecimento sobre o conceito de "ciberataque"?

	Frequência	Percentagem
Não	17	7,3
Sim	215	92,7
Total	232	100,0

Tabela 9 - Amostra da Definição de Ciberataque

Está ciente das medidas que as empresas adotam para proteger os seus dados pessoais após a sua recolha?

	Frequência	Percentagem
Não	130	56,0
Sim	102	44,0
Total	232	100,0

Tabela 10 - Amostra sobre o Conhecimento das Medidas de Segurança das Empresas

Na sua opinião, qual deve ser a ação das empresas para proteger os dados dos utilizadores contra ciberataques?

	Frequência	Percentagem
Evitar ao máximo ter dados que não precisa, que são 99% dos dados que detêm no momento.	1	0,4
Implementar políticas que limitem o acesso a dados sensíveis	24	10,3
Investir em ferramentas de cibersegurança	90	38,8
Monitorizar redes e sistemas da empresa de forma contínua para prevenir ameaças	64	27,6
Realizar avaliações de risco regulares para identificar novas ameaças	15	6,5
Realizar backups regulares de dados críticos	14	6,0
Realizar formações constantes a todos os colaboradores	13	5,6
Todas as anteriores	11	4,5
Total	232	100,0

Tabela 11 - Amostra das Medidas a Implementar pelas PME segundo os Inquiridos

8.4. Análise dos Construtos

De forma a facilitar a interpretação das perguntas por parte dos inquiridos, bem como a sua posterior análise, as questões foram organizadas de acordo com os respetivos construtos.

Estes foram submetidos a uma análise descritiva e serão posteriormente testados, com recurso ao Teste do Coeficiente *Alfa de Cronbach*, de modo a verificar a sua correlação com as hipóteses previamente formuladas.

8.5. Testes Estatísticos e de Confiabilidade

O *Alfa de Cronbach* é o teste de confiabilidade mais utilizado no contexto das ciências sociais para avaliar a coerência interna de instrumentos de recolha de dados, como, por exemplo, um

questionário (Bonett & Wright, 2015). Este teste pressupõe que os itens avaliados apresentem um valor superior a 0,7 para serem considerados fiáveis (Bonett & Wright, 2015).

No caso do presente estudo, e tendo em conta que o questionário recorreu a uma escala de *Likert* de 1 a 7, o *Alfa de Cronbach* será utilizado para medir a confiabilidade dos construtos definidos, permitindo, assim, retirar conclusões válidas a partir dos dados recolhidos (Bonett & Wright, 2015).

Variável	Alfa de Cronbach	Itens na escala
Confiança na PME	0,608	8
Lealdade	0,898	4
WOM	0,302	3
Confiança no Consumidor	0,899	8
Privacidade de Dados	0,827	5

Tabela 12 - Análise dos Testes de Confiabilidade dos Construtos

Analisando a tabela 12, é possível verificar que a maioria das variáveis apresenta um nível de confiabilidade elevado (α = 0,8), à exceção das variáveis WOM e Confiança na PME que apresentam uma confiabilidade reduzida.

8.6. Análise dos Resultados do Modelo Conceptual

Na análise inicial dos dados, recorreu-se à estatística descritiva com o objetivo de verificar se as hipóteses formuladas poderiam apresentar resultados positivos.

Deste modo, procede-se à apresentação da análise individual de cada uma das variáveis utilizadas na investigação. Para cada variável, são indicados a média, a mediana, o desvio padrão, as opções de resposta disponíveis, bem como a distribuição das respostas fornecidas pelos inquiridos. Toda a análise foi realizada com recurso ao *software* SPSS.

As respostas relativas a cada variável foram construídas com base numa escala de *Likert* de 1 a 7, em que 1 corresponde a "Discordo Totalmente" e 7 a "Concordo Totalmente". Esta escala permitiu aos inquiridos posicionarem-se de acordo com os seus sentimentos e o grau de concordância relativamente às afirmações apresentadas.

Iniciando a análise pela variável Confiança na PME, esta foi avaliada com recurso a oito itens de questionário. A primeira pergunta revelou um nível de confiança tendencialmente positivo, com

a maioria dos inquiridos (34,1%) a escolherem o valor 6.

Na segunda e terceira perguntas, observou-se um nível de concordância distribuído entre os valores 3 e 5, sendo o valor 5 o mais assinalado na segunda pergunta (32,2%) e o valor 4 o mais frequente na terceira (29,3%).

As quarta e quinta perguntas evidenciam igualmente uma tendência positiva, com os valores mais escolhidos a situarem-se no nível 5 (34,1%) e no nível 4 (27,2%), respetivamente.

Relativamente às sextas e sétimas perguntas, ambas registaram o valor máximo de respostas no nível 7, com 49,6% e 38,8% dos inquiridos, respetivamente. Por fim, na oitava pergunta, a maioria dos participantes posicionou-se no extremo negativo da escala, selecionando o nível 1 ("Discordo Totalmente") como resposta mais frequente.

Itens	Escala de Likert (percentagem)						
	1	2	3	4	5	6	7
1 - Considero que as PME enfrentam mais dificuldades em termos de acesso a financiamento e recursos adequados para cibersegurança em comparação com empresas de maior dimensão.	0	2,2	4,7	11,2	26,7	34,1	21,1
2 - Considero que, apesar do incidente de cibersegurança, continuo a confiar nesta empresa.	2,6	6,5	13,8	27,6	32,3	11,6	5,6
3 - Considero que posso contar com esta empresa para proteger os meus dados enquanto consumidor.	5,2	14,2	19	29,3	21,1	9,1	2,2
4 - Considero que a empresa reagiu de forma honesta após o ciberataque, o que reforçou a minha confiança.	1,3	1,3	1,7	16,4	34,1	24,1	21,1
5 - Considero que, após o ataque, continuo a sentir segurança para utilizar os serviços da empresa.	3	8,6	18,5	27,2	26,7	11,2	4,7
6 - Considero que me sentiria melhor se a empresa investisse mais em práticas de cibersegurança.	0	0,4	0,9	6,9	12,1	30,2	49,6
7 - Considero que o investimento em cibersegurança é um fator importante para a minha felicidade com a empresa.	0,4	2,2	2,2	8,6	19,4	28,4	38,8
8 - Considero que sentiria maior confiança face à empresa se esta não tivesse exposto o ataque.	31,9	17,7	8,2	12,9	9,1	10,3	9,9

Tabela 13 - Variável Construto Confiança na PME

Com base na análise descritiva desta variável, optou-se pela exclusão da pergunta número 8 — "Considero que sentiria maior confiança face à empresa se esta não tivesse exposto o ataque" —, uma vez que a sua remoção contribuía para uma melhoria no nível de confiabilidade da escala.

Esta decisão foi igualmente sustentada pelo facto de a referida pergunta apresentar a correlação item-total negativa (-0,038), bem como por apresentar a média mais baixa e o maior desvio padrão entre os itens.

Após a exclusão deste item, o valor do *Alfa de Cronbach* da variável aumentou para 0,729, considerando os sete itens remanescentes.

Estatísticas de item

	Média	Erro Desvio
1 - Considero que as PME enfrentam mais dificuldades em termos de acesso a financiamento e recursos adequados para cibersegurança em comparação com empresas de maior dimensão.	5,49	1,202
2 - Considero que, apesar do incidente de cibersegurança, continuo a confiar nesta empresa.	4,38	1,337
3 - Considero que posso contar com esta empresa para proteger os meus dados enquanto consumidor.	3,83	1,404
4 - Considero que a empresa reagiu de forma honesta após o ciberataque, o que reforçou a minha confiança.	5,38	1,228
5 - Considero que, após o ataque, continuo a sentir segurança para utilizar os serviços da empresa.	4,19	1,385
6 - Considero que me sentiria melhor se a empresa investisse mais em práticas de cibersegurança.	6,19	1,003
7 - Considero que o investimento em cibersegurança é um fator importante para a minha felicidade com a empresa.	5,85	1,248

Tabela 14 - Variável Construto Confiança na PME após Análise Descritiva

Estatísticas de escala

Média	Variância	Erro Desvio	N de itens
35,30	29,822	5,461	7

Tabela 15 - Estatísticas de Escala Confiança na PME

No que respeita à variável Lealdade, esta foi avaliada com recurso a quatro perguntas. Os resultados revelam que, de forma geral, os inquiridos demonstraram um nível de resposta centrado

no valor 4, interpretado como um ponto intermédio na escala. Tal distribuição sugere que a maioria dos participantes não possui uma posição vincadamente definida relativamente à confiança que depositam na empresa "Jorge", a qual foi alvo de um ciberataque.

Este posicionamento neutro poderá, em parte, estar associado ao facto de, em perguntas anteriores, os inquiridos terem indicado desconhecimento relativamente às políticas de cibersegurança nas PME.

Essa falta de conhecimento pode justificar a ausência de uma opinião clara, podendo dever-se também à falta de experiência direta com situações semelhantes, o que os impede de tomar uma posição mais determinada.

Itens	Escala de Likert (percentagem)						
	1	2	3	4	5	6	7
1 – Gosto de comprar nesta empresa em qualquer altura.	1,7	3,0	10,3	35,3	29,3	14,7	5,6
2 – Na minha próxima compra, escolherei esta empresa.	3,9	6,9	16,8	35,8	24,1	9,9	2,6
3 – Nos próximos meses, comprarei frequentemente nesta empresa.	5,2	13,8	17,2	34,5	18,5	8,6	2,2
4 -Nos próximos meses, comprarei mais nesta empresa do que nos seus concorrentes, mesmo se soubesse que a sua segurança de dados não foi afetada.	5,6	10,8	20,3	31,9	19,0	8,6	3,9

Tabela 16 - Variável Construto Lealdade

Dado que o coeficiente *Alfa de Cronbach* se apresentou num nível satisfatório (0,898), não se revelou necessário excluir nenhum item da escala proposta.

Estatísticas de item

	Média	Erro Desvio
1 - Gosto de comprar nesta empresa em qualquer altura	4,54	1,216
2 - Na minha próxima compra, escolherei esta empresa.	4,09	1,289
3 - Nos próximos meses, comprarei frequentemente nesta empresa.	3,82	1,374
4 - Nos próximos meses, comprarei mais nesta empresa do que nos seus concorrentes, mesmo se soubesse que a sua segurança de dados não foi afetada.	3,89	1,421

Tabela 17 - Variável Construto Lealdade após Análise Descritiva

Estatísticas de escala			
Média	Variância	Erro Desvio	N de itens
16,34	21,604	4,648	4

Tabela 18 - Estatísticas de Escala Lealdade

O construto seguinte diz respeito ao WOM, o qual se refere à partilha da opinião sobre a empresa com o objetivo de atrair novas oportunidades para a mesma.

Nesta análise, a primeira pergunta arrecadou o nível 4 (35,3%), assim como na terceira pergunta (30,2%). A segunda pergunta apresentou um rácio positivo, com o valor máximo no nível 5 (29,3).

Itens	Escala de Likert (percentagem)						
	1	2	3	4	5	6	7
1 – Considero dizer coisas positivas sobre a empresa após o ciberataque.	0,9	4,7	13,4	35,3	28,9	12,1	4,7
2 – Considero que a minha experiência pós-ataque influenciaria a minha decisão de recomendar esta empresa a outros consumidores.	1,7	1,3	9,9	18,5	29,3	25,4	13,8
3 – Considero recomendar a empresa a alguém que peça o meu conselho	0,4	6,9	18,5	30,2	28,4	11,2	4,3

Tabela 19 - Variável Construto WOM

Conforme mencionado anteriormente, o teste de confiabilidade apresentou um valor relativamente reduzido (0,302), o que comprometeu a sua adequação para efeitos de análise.

Nesse sentido, foi proposta a remoção da segunda pergunta — *"Considero que a minha experiência pós-ataque influenciaria a minha decisão de recomendar esta empresa a outros consumidores"*—, mantendo-se apenas os dois restantes itens do construto.

Após esta alteração, a confiabilidade da escala aumentou, registando-se um *Alfa de Cronbach* de 0,768, valor considerado aceitável para efeitos de consistência interna.

Estatísticas de item

	Média	Erro Desvio
1 – Considero dizer coisas positivas sobre a empresa após o ciberataque.	4,42	1,196
3 – Considero recomendar a empresa a alguém que peça o meu conselho	4,30	1,239

Tabela 20 - Variável Construto WOM após Análise Descritiva

Estatísticas de escala

Média	Variância	Erro Desvio	N de itens
8,72	4,817	2,195	2

Tabela 21 - Estatísticas de Escala WOM

No que respeita à variável Confiança do Consumidor, os resultados revelam uma tendência globalmente positiva nas respostas. Tal evidência sugere que, apesar do incidente de cibersegurança, a transparência e sinceridade demonstradas pela empresa contribuíram para preservar a confiança dos consumidores, levando-os a continuar a recorrer aos serviços da PME.

A primeira, terceira e quarta perguntas registaram uma maior concentração de respostas no nível 4, indicando uma posição mais neutra, onde os inquiridos demonstraram alguma hesitação em identificar-se plenamente com a atuação da empresa. As percentagens observadas foram de 30,6%, 32,8% e 42,4%, respetivamente.

Por outro lado, nas restantes perguntas, o nível 5 foi o mais assinalado, revelando que os consumidores concordam parcialmente com a ideia de que a empresa reagiu de forma adequada à situação. Além disso, indicam que o incidente não comprometeu significativamente a sua decisão de continuar a utilizar os serviços da empresa. Assim, a Confiança do Consumidor assume um papel central na relação entre uma marca e seus consumidores, sendo determinante no processo de decisão de compra. Quanto mais forte for essa relação, maior a probabilidade de fidelização e maior a confiança na marca.

Itens	Escala de Likert (percentagem)						
	1	2	3	4	5	6	7
1 – A empresa corresponde às minhas expectativas.	1,3	5,6	17,7	30,6	25,4	14,2	5,2
2 – Sinto-me confiante na empresa por ser transparente quanto à segurança de dados.	0,9	3,0	4,3	19,0	28,9	25,9	18,1
3 – A empresa nunca me desilude.	4,3	19,8	21,1	32,8	13,8	4,7	3,4
4 – A empresa garante-me satisfação.	0,9	5,6	15,5	42,2	21,1	11,6	3,0
5 – A empresa seria honesta e sincera na resposta às minhas preocupações.	0,9	0,9	6,0	19,8	34,1	23,7	14,7
6 – Posso confiar na empresa para resolver um problema	0,4	2,6	7,3	30,6	32,8	19,4	6,9
7 – A empresa faria todos os esforços para me satisfazer.	0,4	0,9	5,2	31,0	33,6	19,8	9,1
8 – A empresa compensar-me-ia de alguma forma por um problema com a cibersegurança.	3,0	4,3	8,6	25,0	31,5	18,1	9,5

Tabela 22 - Variável Construto Confiança do Consumidor

Com base na informação obtida através da análise, decidiu-se manter todas as perguntas e respetivas respostas referentes à variável, uma vez que o nível de confiabilidade se revelou positivo e suficientemente robusto para sustentar a análise efetuada.

Estatísticas de item

	Média	Erro Desvio
1 – A empresa corresponde às minhas expectativas.	4,37	1,296
2 – Sinto-me confiante na empresa por ser transparente quanto à segurança de dados.	5,22	1,309
3 – A empresa nunca me desilude.	3,60	1,370
4 – A empresa garante-me satisfação.	4,24	1,163
5 – A empresa seria honesta e sincera na resposta às minhas preocupações.	5,15	1,209
6 – Posso confiar na empresa para resolver um problema.	4,78	1,153
7 – A empresa faria todos os esforços para me satisfazer.	4,92	1,106
8 – A empresa compensar-me-ia de alguma forma por um problema com a cibersegurança.	4,70	1,394

Tabela 23 - Variável Construto Confiança do Consumidor após Análise Descritiva

Estatísticas de escala

Média	Variância	Erro Desvio	N de itens
36,98	59,004	7,681	8

Tabela 24 - Estatísticas de Escala Confiança do Consumidor

O último construto analisado corresponde à variável Privacidade de Dados que, de um modo geral, apresentou uma distribuição semelhante à observada no construto anterior, Confiança do Consumidor. As segundas, quartas e quintas perguntas concentraram-se predominantemente no nível 4, com 26,7% e 31,0% das respostas, respetivamente. Por sua vez, as restantes perguntas obtiveram maior incidência no nível 5, com 28,8% e 25,9% das respostas.

Estes resultados permitem concluir que, embora exista uma posição de concordância moderada, os consumidores manifestam alguma preocupação relativamente à forma como os seus dados são partilhados e armazenados, sobretudo após tomarem conhecimento de que esses dados poderiam estar em risco.

Itens	Escala de Likert (percentagem)						
	1	2	3	4	5	6	7
1 – Considero que o tratamento dos meus dados pela empresa melhora a minha experiência enquanto consumidor.	2,2	3,0	12,9	24,1	28,0	18,5	11,2
2 – Considero que a empresa utiliza medidas de segurança adequadas	3,9	15,9	19,0	26,7	20,7	9,5	4,3
3 – A empresa informa-me da partilha dos meus dados com empresas terceiras.	3,9	6,0	8,6	24,1	25,9	22,0	9,5
4 – Considero que tenho controlo sobre os dados recolhidos pela empresa e como posso geri-los.	6,9	12,5	16,8	31,0	17,7	10,3	4,7
5 – Estou confortável em partilhar os meus dados com a empresa de modo a usufruir dos seus serviços.	8,2	15,5	17,2	23,7	19,8	11,2	4,3

Tabela 25 - Variável Construto Privacidade de Dados

À semelhança do que ocorreu com a variável anterior, uma vez que o nível de confiabilidade se encontrava dentro dos parâmetros recomendados (0,827), optou-se por manter todas as perguntas e respetivas respostas tal como foram inicialmente recolhidas.

Estatísticas de item

	Média	Erro Desvio
1 – Considero que o tratamento dos meus dados pela empresa melhora a minha experiência enquanto consumidor.	4,73	1,395
2 – Considero que a empresa utiliza medidas de segurança adequadas.	3,90	1,466
3 – A empresa informa-me da partilha dos meus dados com empresas terceiras.	4,66	1,498
4 – Considero que tenho controlo sobre os dados recolhidos pela empresa e como posso geri-los.	3,90	1,519
5 – Estou confortável em partilhar os meus dados com a empresa de modo a usufruir dos seus serviços.	3,82	1,595

Tabela 26 - Variável Construto Privacidade de Dados após Análise Descritiva

Estatísticas de escala

Média	Variância	Erro Desvio	N de itens
21,02	33,039	5,748	5

Tabela 27 - Estatísticas de Escala Privacidade de Dados

8.7. Análise das Correlações do Modelo Conceptual

Para possibilitar a análise das hipóteses e respetivas correlações, recorreu-se ao Teste do Coeficiente de Correlação de *Pearson*. Este teste permite avaliar a correlação entre variáveis com base no coeficiente denominado *r*, cujo valor varia entre -1 e +1. Quando o valor de *r* é igual a +1, a correlação é considerada perfeitamente positiva; quando é igual a 0, não há correlação; e quando é igual a -1, a correlação é perfeitamente negativa (Adler & Parmryd, 2010).

Correlações

	Confiança	Lealdade	WOM	Confiança consumidor	Privacidade
Confiança na PME	1	,538**	,629**	,700**	,600**
Lealdade		1	,678**	,724**	,661**
WOM			1	,764**	,660**
Confiança consumidor				1	,669**
Privacidade					1

**. A correlação é significativa no nível 0,01 (2 extremidades).

Tabela 28 - Correlação do Teste de Pearson

Assim, a tabela 28 apresenta as correlações entre as variáveis Confiança na PME, WOM, Confiança do Consumidor e Privacidade de Dados segundo o coeficiente de *Pearson*.

No caso da variável Confiança na PME apresenta correlações positivas com todas as restantes variáveis, sendo que as relações com uma correlação mais forte sejam com a Confiança do Consumidor com r=0,700, e a WOM, com r=0,629. A correlação com menos força, mas ainda positivamente correlacionada é a com a Lealdade, que assume um r=0,538.

A variável Lealdade também demonstra correlações positivas, sendo que a variável com correlação mais forte é a Confiança do Consumidor r=0,724, seguida de WOM r=0,678 e Privacidade com r=0,661.

O WOM apresenta uma relação positiva para com as variáveis Confiança do Consumidor r=0,764 e Privacidade com r=0,660.

A Confiança do Consumidor assume uma correlação positiva forte para com o WOM, como visto anteriormente, e com a Confiança na PME, vistos anteriormente. A Privacidade assume um r=0,669.

A última variável a ser analisada é a variável da Privacidade anteriormente correlacionada positivamente com as restantes variáveis sendo que a sua mais forte ligação é para com a Confiança do Consumidor com r=0,669.

De todas as correlações, a que se apresenta como a mais forte é a WOM com a Confiança do Consumidor com r=0,764.

Desta forma, podemos verificar se as hipóteses descritas ao longo deste estudo se podem confirmar.

A hipótese 1a, que afirma que "A perceção/conhecimento dos consumidores sobre as estratégias de cibersegurança adotadas pela empresa está positivamente correlacionada com a lealdade do consumidor", e a hipótese 1b, que afirma que "A confiança na PME está positivamente correlacionada com a lealdade do consumidor", podem ser analisadas através das mesmas correlações. De facto, é possível prever que a Confiança na PME influencia a Lealdade do Consumidor. A correlação de r=0,538 entre a Confiança na PME e a Lealdade sugere que, à medida que a Confiança na PME aumenta, a Lealdade do consumidor também cresce proporcionalmente.

Relativamente à hipótese 1c, que afirma que "A importância atribuída pelos consumidores à privacidade de dados está positivamente correlacionada com a lealdade do consumidor", a correlação observada entre a Privacidade e a Lealdade, com r=0,661, sustenta esta correlação

positiva. Assim, é possível concluir que os consumidores valorizam a forma como os seus dados são processados e armazenados. Quando uma empresa adota uma política mais robusta em termos de cibersegurança, os consumidores tendem a demonstrar maior Lealdade para com essa empresa. Em suma, a Privacidade tem uma influência positiva na Lealdade.

No que diz respeito à hipótese 1d, que postula que "A confiança do consumidor está positivamente correlacionada com a lealdade do consumidor", a correlação entre a Confiança do Consumidor e a Lealdade, apresentada na Tabela 28, revelou r=0,724, um dos coeficientes mais elevados entre todas as correlações analisadas. Este valor reforça a importância da confiança como uma variável determinante na Lealdade para com as PME, indicando que os consumidores que demonstram maior confiança numa empresa são também mais leais a ela.

Finalmente, a hipótese 2, que afirma que "A lealdade do consumidor está positivamente correlacionada com o WOM positivo", é confirmada pela correlação r=0,678, que valida esta hipótese. Este resultado sugere que as empresas que recebem melhores recomendações transmitem aos consumidores a sensação de que podem ser leais a estas empresas.

8.8. Teste T para Análise das Variáveis

Como o objetivo do estudo também passa por compreender a perceção dos consumidores relativamente às medidas de cibersegurança implementadas pelas PME, recorreu-se ao Teste T de amostras independentes para analisar esta relação.

Para tal, os participantes foram divididos em dois grupos: o Grupo 1, que representa os inquiridos que responderam "Sim" à pergunta *"*Está ciente das medidas que as empresas adotam para proteger os seus dados pessoais após a sua recolha?*"*, e o Grupo 2, correspondente às respostas "Não", à mesma pergunta.

Estatísticas de grupo

	Está ciente das medidas que as empresas adotam para proteger os seus dados pessoais após a sua recolha?	N	Média	Erro Desvio	Erro padrão da média
Confiança	1 (sim)	102	5,1289	0,83651	0,08283
	2 (não)	130	4,9758	0,72911	0,06395
Lealdade	1 (sim)	102	4,2230	1,14532	0,11340
	2 (não)	130	3,9788	1,16806	0,10245
WOM	1 (sim)	102	4,4902	1,06236	0,10519
	2 (não)	130	4,2577	1,11757	0,09802
Confiança consumidor	1 (sim)	102	4,7218	0,98675	0,09770
	2 (não)	130	4,5452	0,93529	0,08203
Privacidade	1 (sim)	102	4,4627	1,15286	0,11415
	2 (não)	130	4,0000	1,10951	0,09731

Tabela 29 - Teste T

De acordo com os resultados apresentados na Tabela 29, os consumidores do Grupo 1, que estão cientes das medidas de cibersegurança, demonstram uma perceção mais positiva relativamente às variáveis em análise (Confiança, Lealdade, WOM, Confiança do Consumidor e Privacidade). Em contraste, o Grupo 2, apesar de revelar um nível razoável de confiança e intenção de recomendação (WOM), apresenta valores mais baixos nas variáveis de Lealdade e, sobretudo, de Privacidade.

Estes resultados sugerem que a ausência de informação sobre as práticas de cibersegurança pode afetar negativamente a perceção da proteção dos dados e a fidelização à empresa.

Ao comparar as médias através do Teste T, observa-se que não existem diferenças estatisticamente significativas entre os grupos na maioria das variáveis analisadas. No entanto, a variável Privacidade apresenta uma diferença significativa (p=0,002), indicando que os consumidores cientes das práticas de cibersegurança atribuem maior importância e confiança à proteção dos seus dados pessoais.

Esta diferença é expressiva (diferença média=0,46275), reforçando a ideia de que a comunicação eficaz das medidas de segurança adotadas pode contribuir para melhorar a perceção da privacidade e, consequentemente, a confiança global dos consumidores nas PME

Teste de amostras independentes

		teste-t para Igualdade de Médias				
		Sig. (2 extremidades)	Diferença média	Erro padrão de diferença	95% Intervalo de Confiança da Diferença	
					Inferior	Superior
Confiança	Variâncias iguais assumidas	0,138	0,15303	0,10292	-0,04976	0,35582
	Variâncias iguais não assumidas	0,145	0,15303	0,10464	-0,05330	0,35936
Lealdade	Variâncias iguais assumidas	0,112	0,24419	0,15319	-0,05764	0,54603
	Variâncias iguais não assumidas	0,112	0,24419	0,15283	-0,05700	0,54539
WOM	Variâncias iguais assumidas	0,109	0,23250	0,14466	-0,05253	0,51754
	Variâncias iguais não assumidas	0,107	0,23250	0,14378	-0,05084	0,51585
Confiança consumidor	Variâncias iguais assumidas	0,165	0,17662	0,12675	-0,07311	0,42636
	Variâncias iguais não assumidas	0,168	0,17662	0,12757	-0,07486	0,42810
Privacidade	Variâncias iguais assumidas	0,002	0,46275	0,14930	0,16857	0,75692
	Variâncias iguais não assumidas	0,002	0,46275	0,15000	0,16707	0,75842

Tabela 30 - Teste Amostras Independentes

9. Capítulo 9: Considerações Finais

9.1. Discussão de Resultados e Principais Conclusões

Em suma, o presente estudo teve como principal objetivo compreender se o investimento em cibersegurança por parte das PME influencia a perceção e consequente confiança dos consumidores. Face à crescente sofisticação dos ciberataques e ao baixo nível de literacia digital, as PME tornaram-se particularmente vulneráveis. Esta vulnerabilidade é agravada quando as políticas de cibersegurança não são compreendidas pelos consumidores e colaboradores, resultando na sua desvalorização e, por conseguinte, na fragilização da segurança organizacional.

Com base nos resultados obtidos, nomeadamente nas Tabelas 8 a 10, constatou-se que, embora os participantes demonstrem um conhecimento considerável sobre ciberataques e cibersegurança, persistem lacunas relativamente às medidas efetivamente adotadas pelas PME. Esta realidade pode evidenciar uma conjugação entre o desconhecimento dos consumidores e a reduzida transparência das políticas implementadas pelas empresas (Ali et al., 2024; Demirci & Yardan, 2023). Tais medidas, conforme evidenciado na Tabela 11, poderiam englobar a adoção de *software* mais robusto, o reforço de mecanismos de encriptação e a implementação de *firewalls* eficazes e devidamente configuradas (Alhasan et al., 2024; Alsharida et al., 2023; Ani et al., 2016). Estas iniciativas contribuem, não só para o reforço da segurança, como também para a promoção da literacia digital entre os consumidores (Ali et al., 2024).

Na análise da variável Confiança na PME, foi notório que a maioria dos inquiridos considera que as limitações financeiras constituem um entrave à adoção de boas práticas de cibersegurança. Esta limitação torna as PME mais suscetíveis a ciberataques (Saha & Anwar, 2024). A análise sugere que a implementação de determinadas estratégias pode reforçar a confiança dos consumidores. Entre estas destacam-se a transparência nas políticas de segurança, a formação contínua dos colaboradores, o controlo rigoroso do acesso à informação sensível e a promoção de boas práticas de proteção de dados (Balzano & Marzi, 2024; Alhasan et al., 2024; Ali et al., 2024).

A Lealdade do consumidor poderá ser seriamente comprometida na ausência de medidas eficazes de prevenção, pois a perceção de uma falha de segurança tende a abalar a confiança na organização. A ausência de conhecimento sobre estas políticas poderá justificar a indefinição de opinião por parte dos inquiridos, que pode também estar relacionada com a falta de experiências prévias. Neste contexto, a adoção de soluções como sistemas de armazenamento em nuvem, ações de sensibilização internas e a promoção da digitalização por parte dos gestores surge como

resposta pertinente (Alhasan et al., 2024; Hoong et al., 2024).

A análise do WOM revela-se essencial, uma vez que a perceção individual sobre uma marca ou produto, sobretudo influenciada por experiências pessoais ou relatos de outros consumidores, afeta significativamente a sua credibilidade. Os inquiridos demonstraram que, com algum receio, seriam capazes de recorrer a esta empresa, com o nível 4 e 5 de ambas as perguntas muito próximas. Entre as recomendações para as PME melhorarem a sua situação destaca-se a implementação de certificados de conformidade e selos de maturidade digital, que demonstram o compromisso da organização com práticas seguras e alinhadas com as normas legais em vigor (Wolford, 2025; Regulations, 2003; Commission, 2003).

Quando a segurança é comprometida, a confiança é abalada, afetando negativamente o comportamento do consumidor. Para mitigar esta vulnerabilidade, as PME devem recorrer a especialistas em cibersegurança, gestores capacitados e adotar uma abordagem proativa de monitorização e análise digital (Adjei et al., 2009; Hoong et al., 2024). Segundo os dados obtidos relativamente a esta variável, esta manteve-se positiva, mesmo após um incidente de segurança e perante a forma como a empresa o geriu. Assim, a confiança assume um papel central na relação com a marca, influenciando diretamente a decisão de compra e a fidelização.

A preocupação com a Privacidade de Dados também foi salientada, apesar da confiança na atuação da empresa. Esta apreensão poderá ser minimizada através da implementação de medidas específicas de reforço da segurança da informação, nomeadamente a atualização regular de *software*, a aplicação da tríade CIA, com especial foco na confidencialidade, e a realização de cópias de segurança. A adoção do RGPD reforça a proteção contra o uso indevido de dados e contribui para o aumento da confiança dos consumidores (Ani et al., 2016; Bagies, 2024; Balzano & Marzi, 2024).

A análise dos dados do questionário revelou correlações significativas entre os construtos definidos no modelo conceptual. Confirmou-se que quanto maior o conhecimento dos consumidores sobre as práticas de cibersegurança da PME, maior é a valorização da proteção de dados. Os construtos analisados apresentaram correlações positivas com a Lealdade e o WOM, validando as hipóteses formuladas. A correlação mais forte ($r = 0{,}764$) foi observada entre a Confiança do Consumidor e o WOM, confirmando que a relação com o consumidor pode ser uma ferramenta estratégica de *marketing* e fidelização.

Os resultados da investigação evidenciam a necessidade de repensar a forma como as PME comunicam e gerem a sua cibersegurança. A realização de simulações de incidentes reais e da

modernização dos sistemas de informação revelam-se medidas essenciais para transmitir segurança e fiabilidade ao consumidor. Por outro lado, a inação, particularmente uma atuação reativa, pode comprometer gravemente o desempenho económico e a responsabilidade social destas empresas.

Assim, as PME que investem em medidas eficazes tendem a desenvolver relações mais sólidas e duradouras com os consumidores, contrastando com aquelas que adotam estratégias de risco. A investigação adotou uma abordagem dedutiva, enquadrada no *Realismo Crítico*, assumindo que as perceções dos consumidores são construídas socialmente. Neste contexto, a comunicação clara sobre práticas de segurança torna-se determinante para reforçar a confiança e a lealdade do consumidor, enquanto o uso de linguagem excessivamente técnica se revela uma barreira à compreensão, sublinhando a necessidade de promover literacia digital acessível.

A aceleração digital veio demonstrar que o investimento em cibersegurança não só reduz riscos, como também influencia positivamente a tomada de decisão do consumidor e o crescimento do negócio. A aplicação de medidas eficazes resulta num aumento da confiança, lealdade e recomendação (WOM), elementos fundamentais para a sustentabilidade das PME.

Através da Revisão de Literatura, foram identificados conceitos-chave, como a tríade CIA, a aplicação do RGPD, os impactos da engenharia social, e as definições de cibersegurança e ciberespaço. Constatou-se que a perceção dos consumidores relativamente à segurança digital, quando suportada por práticas claras e transparentes, tem um efeito direto na sua confiança, lealdade, intenção de recomendação e preocupação com a privacidade. Ficou patente que, para que uma PME seja verdadeiramente segura ao nível da cibersegurança, não basta investir em soluções tecnológicas. É essencial apostar na consciencialização e formação contínua de todos os intervenientes. As práticas devem ser adaptadas à realidade de cada organização, considerando o setor de atividade, o nível de literacia digital e os recursos disponíveis.

Conclui-se que a cibersegurança deve ser encarada como um investimento estratégico com impacto direto na confiança do consumidor, na lealdade e no desempenho financeiro. As PME devem ultrapassar abordagens reativas e integrar a segurança digital de forma preventiva e transversal ao seu modelo de negócio. Ao investir em cibersegurança, estão não só a proteger os seus ativos, como a reforçar a relação com os consumidores e a garantir a sustentabilidade a longo prazo.

9.2. Limitações do Estudo

Apesar das limitações inerentes à amostra utilizada na análise de dados, nomeadamente a predominância de indivíduos mais jovens, a utilização de uma amostragem por conveniência e a ausência de representação de todos os perfis de consumidores, reconhece-se que a perceção do consumidor pode variar consoante a sua experiência prévia com incidentes de cibersegurança. No entanto, os resultados obtidos reforçam que a necessidade de investimento na cibersegurança ultrapassa a dimensão digital, sendo também estratégica num mercado competitivo, constituindo uma oportunidade para as PME se destacarem positivamente.

Importa ressaltar que o estudo não permitiu estabelecer relações causais para além das correlações, o que permite dizer que, apesar da confiança e perceção de segurança estarem relacionadas, não é possível afirmar com certezas que uma causa diretamente a outra.

Adicionalmente, o questionário aplicado baseou-se numa situação hipotética de ciberataque, o que poderá não ter suscitado nos participantes as mesmas reações ou sentimentos que um caso real envolvendo uma empresa com a qual tenham contacto direto.

Tanto a cibersegurança como os ciberataques, bem como todos os aspetos inerentes a estes conceitos, são fenómenos relativamente recentes. Assim, importa referir que a informação apresentada no estudo corresponde ao estado de conhecimento disponível até à sua submissão, uma vez que a sua investigação e desenvolvimento é ainda corrente.

Um outro aspeto ainda a considerar prende-se com a necessidade de retirar algumas perguntas de alguns construtos, como o WOM, de forma a alcançar um nível de confiabilidade estatística mais elevado. Tal pode ter comprometido a profundidade da análise teórica e prática.

Por último, importa reconhecer que a cibersegurança é uma área em expansão, o que com o tempo, pode significar ataques mais sofisticados e diversificados, exigindo das PME mais soluções. No entanto, a valorização crescente da cibersegurança na conjuntura internacional poderá representar novas oportunidade para as PME, tanto ao nível de maiores vantagens competitivas, como no acesso a apoios financeiros e incentivos a nível nacional e internacional.

9.3. Sugestões para Investigação Futura

Para investigações futuras, seria pertinente incluir participantes com diferentes níveis de literacia digital e pertencentes a distintos contextos socioeconómicos, de modo a captar diferentes perceções e comportamentos face à cibersegurança. Esta abordagem permitiria uma compreensão mais diversificada de como diferentes consumidores valorizam as práticas de cibersegurança adotadas pelas PME.

A realização de entrevistas qualitativas poderá constituir um fator relevante para a compreensão dos fatores de influência na Confiança do Consumidor, em especial o modo como estes lidam emocionalmente com incidentes de segurança.

Para além disso, analisar casos de ataques reais a PME poderá ter *insights* valiosos sofre o impacto desses acontecimentos na confiança e lealdade dos consumidores e sobre como acontece a recuperação da credibilidade da empresa.

É, ainda, recomendado a inclusão de variáveis mais especificas associadas ao setor de atividade das PME, permitindo comprar a perceção de risco, nível de exigência dos consumidores e estratégias adotadas. A comparação entre empresas de maior ou menor dimensão poderá revelar diferenças no modo como estas comunicam e gerem a cibersegurança, conduzindo a uma melhor adaptação das estratégias à sua realidade.

10. Referências Bibliográficas

Adjei, M. T., Noble, S. M., & Noble, C. H. (2009). The influence of C2C communications in online brand communities on customer purchase behavior. *Journal of the Academy of Marketing Science*, *38*(5), 634–653. https://doi.org/10.1007/s11747-009-0178-5

Adler, J., & Parmryd, I. (2010). Quantifying colocalization by correlation: The Pearson correlation coefficient is superior to the Mander's overlap coefficient. *Cytometry Part A*, *77A*(8), 733–742. https://doi.org/10.1002/cyto.a.20896

Alexandrov, A., Lilly, B., & Babakus, E. (2013). The effects of social- and self-motives on the intentions to share positive and negative word of mouth. *Journal of the Academy of Marketing Science*, *41*(5), 531–546. https://doi.org/10.1007/s11747-012-0323-4

Alhasan, W., Wannous, M., Abualkishik, A., Al Nasar, M. R., Ali, L., & Al-Zoubi, H. (2024). An in-depth examination of cybersecurity: Unveiling contemporary trends and recent advancements in the world of cyber threats. *2024 2nd International Conference on Cyber Resilience (ICCR)*, 1–11. https://doi.org/10.1109/iccr61006.2024.10533062

Ali, A., Overboe, C., Mohottalalage, T., & Mailewa, A. B. (2024). *The human factor in cybersecurity: Understanding psychology, training efficacy, and error reduction strategies*.

Ali, A., Shah, M., Foster, M., & Alraja, M. N. (2025). Cybercrime resilience in the era of advanced technologies: Evidence from the financial sector of a developing country. *Computers*, *14*(2), 38. https://doi.org/10.3390/computers14020038

Alsharida, R. A., Al-rimy, B. A. S., Al-Emran, M., & Zainal, A. (2023). A systematic review of multi perspectives on human cybersecurity behavior. *Technology in Society*, *73*(102258), 102258. https://doi.org/10.1016/j.techsoc.2023.102258

Alyami, A., Sammon, D., Neville, K., & Mahony, C. (2023). The critical success factors for security education, training and awareness (SETA) program effectiveness: A lifecycle model. *Information Technology & People, 36*(8), 94–125. https://doi.org/10.1108/itp-07-2022-0515

Ani, U. P. D., He, H. (Mary), & Tiwari, A. (2016). Review of cybersecurity issues in industrial critical infrastructure: Manufacturing in perspective. *Journal of Cyber Security Technology*, *1*(1), 32–74. https://doi.org/10.1080/23742917.2016.1252211

Bagies, T. (2024). Classifying software security requirements into confidentiality, integrity, and availability using machine learning approaches. *PeerJ Computer Science*, *10*(e2554), e2554. https://doi.org/10.7717/peerj-cs.2554

Balzano, M., & Marzi, G. (2024). At the cybersecurity frontier: Key strategies and persistent challenges for business leaders. *Strategic Change*, *34*(2), 181–192. https://doi.org/10.1002/jsc.2622

Bendler, D., & Felderer, M. (2023). Competency models for information security and cybersecurity professionals: Analysis of existing work and a new model. *ACM Transactions on Computing Education*, *23*(2), 1–33.

https://doi.org/10.1145/3573205
Bonett, D. G., & Wright, T. A. (2015). Cronbach's alpha reliability: Interval estimation, hypothesis testing, and sample size planning. *Journal of Organizational Behavior*, *36*(1), 3–15. https://doi.org/10.1002/job.1960
Certificação de maturidade digital. (2022). Portugal Digital. https://portugaldigital.gov.pt/avaliar-a-maturidade-digital-e-certificar-a-sua-empresa/certificacao-de-maturidade-digital/
Chaudhuri, A., & Holbrook, M. B. (2001). The Chain of Effects from Brand Trust and Brand Affect to Brand Performance: The Role of Brand Loyalty. *Journal of Marketing*, *65*(2), 81–93. https://doi.org/10.1509/jmkg.65.2.81.18255
Ciberdefesa. (2018). Consilium. https://www.consilium.europa.eu/pt/policies/cyber-defence/
CNCS - glossário. (2024). CNCS. https://www.cncs.gov.pt/pt/glossario/#linhasobservacao
Commission. (2003). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32003H0361
Coutinho, C. P. (2020). *Metodologia de investigaçao em ciencias sociais e humanas : teoria e prática* (2 edição). Almedina.
Dalal, R. S., Howard, D. J., Bennett, R. J., Posey, C., Zaccaro, S. J., & Brummel, B. J. (2021). Organizational science and cybersecurity: Abundant opportunities for research at the interface. *Journal of Business and Psychology*, *37*(1). https://doi.org/10.1007/s10869-021-09732-9
Delgado-Ballester, E. (2004). Applicability of a brand trust scale across product categories. *European Journal of Marketing*, *38*(5/6), 573–592. https://doi.org/10.1108/03090560410529222
Demirci, H. F., & Yardan, E. D. (2023). Data management in the digital health environment scale development study*. *BMC Health Services Research*, *23*(1). https://doi.org/10.1186/s12913-023-10205-3
ENISA Threat Landscape 2024. (2024). *European Union Agency for Cybersecurity*. https://doi.org/10.2824/0710888
Fallatah, W., Kävrestad, J., & Furnell, S. (2024). Establishing a model for the user acceptance of cybersecurity training. *Future Internet*, *16*(8), 294. https://doi.org/10.3390/fi16080294
Fedele, A., & Roner, C. (2021). Dangerous games: A literature review on cybersecurity investments. *Journal of Economic Surveys*, *36*(1), 157–187. https://doi.org/10.1111/joes.12456
Fernandez de Arroyabe, J. C., Arroyabe, M. F., Fernandez, I., & Arranz, C. F. A. (2023). Cybersecurity resilience in smes. A machine learning approach. *Journal of Computer Information Systems*, *64*(6), 711–727. https://doi.org/10.1080/08874417.2023.2248925
Geneste, L., & Galvin, P. (2013). Trust and knowledge acquisition by small and medium-sized firms in weak client–firm exchange relationships. *International Small Business Journal: Researching Entrepreneurship*, *33*(3), 277–298. https://doi.org/10.1177/0266242613497379
Glaser, K. (2016). News from the pragmatics classroom: Contrasting the inductive and the deductive approach in the teaching of pragmatic competence. *Intercultural Pragmatics*, *13*(4), 529–561. https://doi.org/10.1515/ip-2016-0023

Goel, S. (2011). Cyberwarfare. *Communications of the ACM*, *54*(8), 132–140. https://doi.org/10.1145/1978542.1978569

Haudi, Handayani, W., Musnaini, Suyoto, Y., Prasetio, T., Pitaloka, E., Wijoyo, H., Yonata, H., Koho, I., & Cahyono, Y. (2022). The effect of social media marketing on brand trust, brand equity and brand loyalty. *Journal of Data and Network Science*, *6*(3). https://doi.org/10.5267/j.ijdns.2022.1.015

Heinberg, M., Ozkaya, H. E., & Taube, M. (2015). A brand built on sand: Is acquiring a local brand in an emerging market an ill-advised strategy for foreign companies? *Journal of the Academy of Marketing Science*, *44*(5), 586–607. https://doi.org/10.1007/s11747-015-0452-7

Hoong, Y., Rezania, D., & Baker, R. (2024). When traditional SME managers encounter cybersecurity: Discourse analysis of opportunities and dilemmas in meeting the demands. *Technology in Society*, *78*. https://doi.org/10.1016/j.techsoc.2024.102650

Hu, X. (2018). Methodological implications of critical realism for entrepreneurship research. *Journal of Critical Realism*, *17*(2), 118–139. https://doi.org/10.1080/14767430.2018.1454705

Lim, W. M. (2024). What Is Quantitative research? an Overview and Guidelines. *Australasian Marketing Journal (AMJ)*, *1*(1). Sagepub. https://doi.org/10.1177/14413582241264622

McMullan, R. (2005). A multiple-item scale for measuring customer loyalty development. *Journal of Services Marketing* , *19*(7). https://doi.org/10.1108/08876040510625972

McMullan, R., & Gilmore, A. (2003). The conceptual development of customer loyalty measurement: A proposed scale. *Journal of Targeting, Measurement and Analysis for Marketing*, *11*(3), 230–243. https://doi.org/10.1057/palgrave.jt.5740080

Michelena, Á., Aveleira-Mata, J., Jove, E., Bayón-Gutiérrez, M., Novais, P., Romero, O. F., Calvo-Rolle, J. L., & Aláiz-Moretón, H. (2023). A novel intelligent approach for Man-In-The-Middle attacks detection over IoT environments based on MQTT. *Expert Systems*, *41*(2). https://doi.org/10.1111/exsy.13263

Morales-Sáenz, F. I., Medina-Quintero, J. M., & Reyna-Castillo, M. (2024). Beyond data protection: Exploring the convergence between cybersecurity and sustainable development in business. *Sustainability*, *16*(14), 5884. https://doi.org/10.3390/su16145884

Ning, H., Ye, X., Bouras, M. A., Wei, D., & Daneshmand, M. (2018). General Cyberspace: Cyberspace and Cyber-Enabled Spaces. *IEEE Internet of Things Journal*, *5*(3), 1843–1856. https://doi.org/10.1109/jiot.2018.2815535

Oliver, R. L. (1999). Whence Consumer Loyalty? *Journal of Marketing*, *63*(Special Issue 1999), 33. https://doi.org/10.2307/1252099

Overill, R. E. (1999). Denial of service attacks: Threats and methodologies. *Journal of Financial Crime*, *6*(4), 351–351. https://doi.org/10.1108/eb025906

Parsaei, A. (2024). Awareness and social engineering-based cyberattacks. *International Journal of Reliability, Risk and Safety: Theory and Application*, *7*(1), 31–36. https://doi.org/10.22034/IJRRS.2024.7.1.4

Pescaroli, G., Velazquez, O., Alcántara-Ayala, I., Galasso, C., Kostkova, P., & Alexander, D. (2020).

A Likert Scale-Based Model for Benchmarking Operational Capacity, Organizational Resilience, and Disaster Risk Reduction. *International Journal of Disaster Risk Science*, *11*(3), 404–409. https://doi.org/10.1007/s13753-020-00276-9

Prasad, S., Gupta, I. C., & Totala, N. K. (2017). Social media usage, electronic word of mouth and purchase-decision involvement. *Asia-Pacific Journal of Business Administration*, *9*(2), 134–145. https://doi.org/10.1108/apjba-06-2016-0063

Rawindaran, N., Jayal, A., Prakash, E., & Hewage, C. (2023). Perspective of small and medium enterprise (sme's) and their relationship with government in overcoming cybersecurity challenges and barriers in wales. *International Journal of Information Management Data Insights*, *3*(2), 100191. https://doi.org/10.1016/j.jjimei.2023.100191

Regulamento de utilização da marca nacional selos de maturidade digital. (2021). Imprensa Nacional - Casa Da Moeda.

Regulations. (2003). https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679

Rieder, A., Chakraborty, S., Goyal, S., & Berndt, D. J. (2024). A critical realist approach to agent-based modeling: Unlocking prediction in non-positivist paradigms. *Journal of Information Technology*, *0*(0). https://doi.org/10.1177/02683962241280657

Saha, B., & Anwar, Z. (2024). A Review of Cybersecurity Challenges in Small Business: The Imperative for a Future Governance Framework. *Journal of Information Security*, *15*(01), 24–39. https://doi.org/10.4236/jis.2024.151003

Selo de cibersegurança. (2025). Certificação de Maturidade Digital. https://selosmaturidadedigital.incm.pt/SMD/Cybersecurity

Sirdeshmukh, D., Singh, J., & Sabol, B. (2002). Consumer trust, value, and loyalty in relational exchanges. *Journal of Marketing*, *66*(1), 15–37. https://doi.org/10.1509/jmkg.66.1.15.18449

Smith, H. (2023). The geopolitics of cyberspace and the European Union's changing identity. *Journal of European Integration*, *45*(8), 1219–1234. https://doi.org/10.1080/07036337.2023.2277329

Veiga, P. (2024). *Cibersegurança* (1st ed.). Fundação Francisco Manuel Dos Santos.

Wolford, B. (2025). *What is GDPR, the EU's new data protection law?* GDPR.eu. https://gdpr.eu/what-is-gdpr/

Yague-Guillen, M. J., Munuera-Aleman, J. L., & Delgado-Ballester, E. (2003). Development and Validation of a Brand Trust Scale. *International Journal of Market Research*, *45*(1), 1–18. https://doi.org/10.1177/147078530304500103

11. Anexo – Formulário do Questionário

Este questionário faz parte de um estudo académico desenvolvido no âmbito da minha dissertação de Mestrado em Gestão e Negócios da Universidade do Minho. O objetivo principal deste estudo é analisar o impacto das estratégias de cibersegurança na confiança do consumidor, com um foco particular nas práticas adotadas por Pequenas e Médias Empresas (PMEs).

A sua colaboração é fundamental para compreender como as PMEs implementam estratégias de cibersegurança e de que forma essas práticas influenciam a confiança dos consumidores nos serviços prestados. As informações recolhidas serão tratadas de forma confidencial e utilizadas exclusivamente para fins académicos.

O questionário é totalmente anónimo e o tempo estimado para o seu preenchimento é de cerca de 5 minutos. A sua participação é voluntária e, em caso de dúvidas ou necessidade de esclarecimentos, estou à disposição para qualquer contacto através do endereço eletrónico pg53252@alunos.uminho.pt.

Agradeço antecipadamente pela sua colaboração e pelo tempo dispensado na resposta ao presente questionário.

Declaro que aceito participar no estudo apresentado

-Sim

-Não

Perguntas sobre o perfil dos inquiridos

- Idade
- Género
- Nacionalidade
- Nível de escolaridade (concluído)
- Ocupação/Profissão
- Concelho de Residência

Perguntas sobre a consciencialização da cibersegurança

Uma Pequena e Média Empresa (PME) é uma empresa que emprega menos de 250 colaboradores e com um volume de negócios anual não superior a 50 milhões de euros (European Commission, 2024).

A cibersegurança é um conjunto de medidas e ações de prevenção e análise com o intuito de proteger as informações e pessoas no ciberespaço (*CNCS - Glossário*, 2024).

Um ciberataque é um ataque contra um ou vários sistemas, com o intuito de prejudicar a segurança das tecnologias de informação e roubar ou danificar dados pessoais ou de organizações (*CNCS - Glossário*, 2024).

- Antes da definição apresentada, tinha conhecimento sobre o conceito de "cibersegurança"? (resposta escolha múltipla “Sim” ou “Não”)
- Antes da definição apresentada, tinha conhecimento sobre o conceito de "ciberataque"? (resposta escolha múltipla “Sim” ou “Não”)
- Está ciente das medidas que as empresas adotam para proteger os seus dados pessoais após a sua recolha? (resposta escolha múltipla “Sim” ou “Não”)
- Na sua opinião, qual deve ser a ação das empresas para proteger os dados dos utilizadores contra ciberataques?
    - Investir em ferramentas de cibersegurança
    - Realizar *backups* regulares de dados críticos
    - Implementar políticas que limitem o acesso a dados sensíveis
    - Monitorizar redes e sistemas da empresa de forma contínua para prevenir ameaças
    - Realizar formações constantes a todos os colaboradores
    - Realizar avaliações de risco regulares para identificar novas ameaças
    - Outra opção

Perguntas direcionadas com os construtos definidos

As seguintes questões visam compreender como os consumidores reagem a ataques informáticos e como as práticas de cibersegurança de uma Pequena e Média Empresa (PME)

podem afetar a sua confiança e lealdade. O cenário fictício a ser analisado é o seguinte:

A empresa “Jorge”, uma PME bem estabelecida no mercado nacional, sofreu recentemente um ciberataque que bloqueou o acesso aos vários sistemas da empresa.

Imediatamente após a deteção da ameaça, a equipa de cibersegurança da empresa ativou o protocolo de resposta a incidentes e comunicou aos consumidores o ocorrido.

Apesar de todos os esforços para controlar os danos e reforçar a segurança, as reações dos consumidores foram mistas. Alguns perderam completamente a confiança na empresa, considerando o ataque inaceitável, enquanto outros apreciaram a forma transparente como a empresa comunicou o sucedido. No entanto, uma outra parte, embora não vissem a sua confiança afetada, preferiam não ter sido informados sobre o ataque.

Perguntas sobre a Confiança na PME

Enquanto consumidor fictício da empresa, por favor, assinale a opção que considerar a correta com base no cenário apresentado sobre a confiança na empresa. Utilize a escala de 1 a 7, onde 1 significa "Discordo Totalmente " e 7 significa "Concordo Totalmente ".

1. Considero que as PME enfrentam mais dificuldades em termos de acesso a financiamento e recursos adequados para cibersegurança em comparação com empresas de maior dimensão.
2. Considero que, apesar do incidente de cibersegurança, continuo a confiar nesta empresa.
3. Considero que posso contar com esta empresa para proteger os meus dados enquanto consumidor.
4. Considero que a empresa reagiu de forma honesta após o ciberataque, o que reforçou a minha confiança.
5. Considero que, após o ataque, continuo a sentir segurança para utilizar os serviços da empresa.
6. Considero que me sentiria melhor se a empresa investisse mais em práticas de cibersegurança.
7. Considero que o investimento em cibersegurança é um fator importante para a minha felicidade com a empresa.

8. Considero que sentiria maior confiança face à empresa se esta não tivesse exposto o ataque.

Perguntas sobre a Lealdade

Enquanto consumidor fictício da empresa, por favor, assinale a opção que considerar a correta com base no cenário apresentado sobre a lealdade na empresa. Utilize a escala de 1 a 7, onde 1 significa "Discordo Totalmente " e 7 significa "Concordo Totalmente ".

1. Gosto de comprar nesta empresa em qualquer altura.
2. Na minha próxima compra, escolherei esta empresa.
3. Nos próximos meses, comprarei frequentemente nesta empresa.
4. Nos próximos meses, comprarei mais nesta empresa do que nos seus concorrentes, mesmo se soubesse que a sua segurança de dados não foi afetada.

Perguntas sobre o WOM

Enquanto consumidor fictício da empresa, por favor, assinale a opção que considerar a correta com base no cenário apresentado sobre sua recomendação da empresa. Utilize a escala de 1 a 7, onde 1 significa "Discordo Totalmente " e 7 significa "Concordo Totalmente ".

1. Considero dizer coisas positivas sobre a empresa após o ciberataque.
2. Considero que a minha experiência pós-ataque influenciaria a minha decisão de recomendar esta empresa a outros consumidores.
3. Considero recomendar a empresa a alguém que peça o meu conselho.

Perguntas sobre Confiança do Consumidor

Enquanto consumidor fictício da empresa, por favor, assinale a opção que considerar a correta com base no cenário apresentado sobre a sua confiança. Utilize a escala de 1 a 7, onde 1 significa "Discordo Totalmente " e 7 significa "Concordo Totalmente ".

1. A empresa corresponde às minhas expectativas.
2. Sinto-me confiante na empresa por ser transparente quanto à segurança de dados.
3. A empresa nunca me desilude.
4. A empresa garante-me satisfação.
5. A empresa seria honesta e sincera na resposta às minhas preocupações.
6. Posso confiar na empresa para resolver um problema.
7. A empresa faria todos os esforços para me satisfazer.
8. A empresa compensar-me-ia de alguma forma por um problema com a cibersegurança.

Perguntas sobre Privacidade de Dados

Enquanto consumidor fictício da empresa, por favor, assinale a opção que considerar a correta com base no cenário apresentado sobre a privacidade de dados da empresa. Utilize a escala de 1 a 7, onde 1 significa "Discordo Totalmente " e 7 significa "Concordo Totalmente ".

1. Considero que o tratamento dos meus dados pela empresa melhora a minha experiência enquanto consumidor.
2. Considero que a empresa utiliza medidas de segurança adequadas.
3. A empresa informa-me da partilha dos meus dados com empresas terceiras.
4. Considero que tenho controlo sobre os dados recolhidos pela empresa e como posso geri-los.
5. Estou confortável em partilhar os meus dados com a empresa de modo a usufruir dos seus serviços.

Fim do questionário