

M

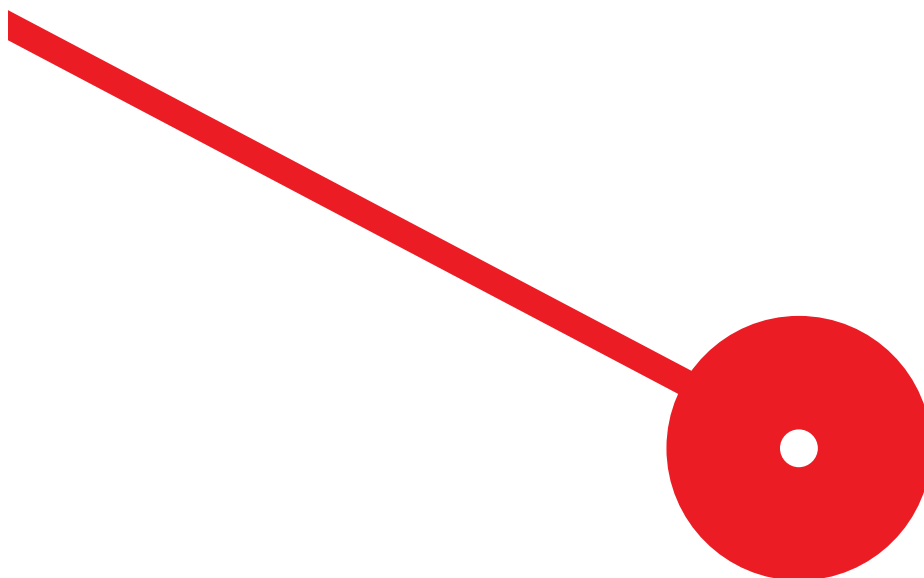
MESTRADO
Negócio Eletrónico

Percepção da Segurança da Informação no Mobile Commerce

António Pedreiras

10/2025

António Pedreiras. Percepção da Segurança da
Informação no mobile Commerce.
10/2025



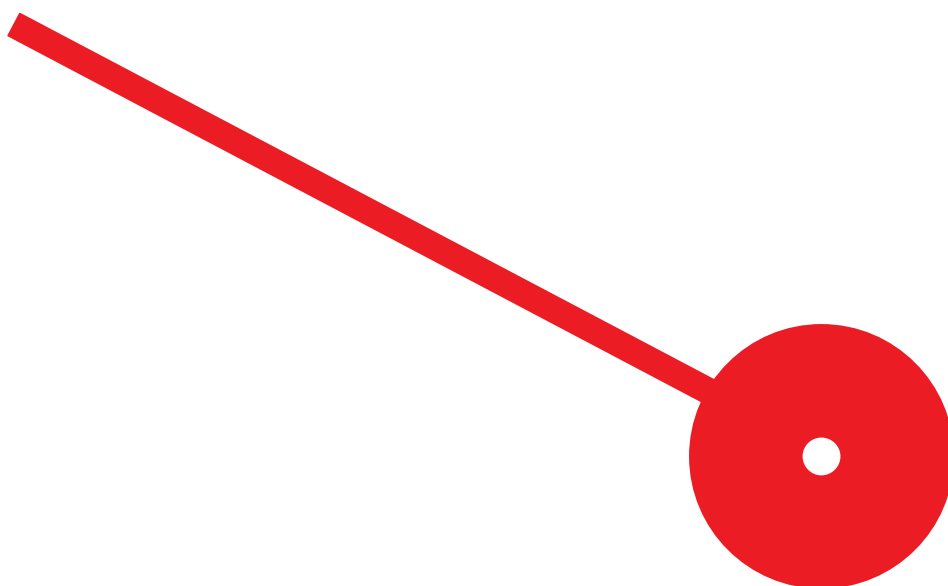
M

MESTRADO
Negócio Eletrónico

Percepção da Segurança da Informação no Mobile Commerce . João Coelho

**Dissertação de Mestrado apresentado ao Instituto Superior de
Contabilidade e Administração do Porto para a obtenção do
grau de Mestre em Negócio Eletrónico, sob orientação de
Professor Doutor Humberto Medrado e co-orientação do
Professor Doutor Agostinho Sousa Pinto**

António Pedreiras. Percepção da segurança da
informação no mobile commerce
10/2025



Dedicatória

Dedico este trabalho à minha mãe, Paula Pedreiras, pela força, amor e dedicação de uma vida inteira, e à minha namorada, Inês Bastos, pelo apoio incondicional e pela presença constante em todos os momentos.

A ambos, o meu mais profundo agradecimento por nunca deixarem que desistisse

Agradecimentos

A concretização deste trabalho não teria sido possível sem o apoio, incentivo e presença de várias pessoas que, de diferentes formas, contribuíram para esta etapa do meu percurso académico e pessoal.

Em primeiro lugar, expresso a minha profunda gratidão à minha namorada, Inês Bastos, pelo carinho, paciência e constante motivação ao longo de todo este processo. À minha mãe, Paula Pedreiras, agradeço por todo o amor, apoio incondicional e força que sempre me transmitiu.

Aos meus colegas e amigos Diogo Moura, Cláudio Cunha, Tiago Silva e Rui, deixo um sincero agradecimento pela amizade e companheirismo que se mantiveram desde o CTESP até este momento, tornando esta jornada mais leve e significativa.

Um reconhecimento especial ao co orientador Professor Doutor Agostinho, por todo o apoio e disponibilidade demonstrados ao longo destes sete anos de percurso académico, sempre com palavras de incentivo e sabedoria.

Por fim, deixo um profundo agradecimento ao meu orientador e amigo, Professor Humberto Medrado, pelo acompanhamento atento, pela orientação rigorosa e, acima de tudo, pela confiança, dedicação e empatia com que me guiou durante o desenvolvimento desta dissertação.

A todos, o meu mais sincero obrigado.

Resumo:

A rápida evolução das tecnologias móveis tem transformado o *mobile commerce* (*m-commerce*) num canal privilegiado de consumo digital, combinando conveniência e acessibilidade. Contudo, esta transição acarreta novos desafios no domínio **da** segurança da informação, especialmente no que respeita à forma como os utilizadores percebem e gerem os riscos associados às suas interações online. O presente estudo tem como objetivo analisar a percepção de segurança no m-commerce, explorando a relação entre o nível de literacia digital, as práticas de proteção adotadas e o grau de vulnerabilidade percebida. Para o efeito, foi utilizada uma metodologia de natureza quantitativa, com base num questionário aplicado a 44 participantes. As respostas foram tratadas através de análise descritiva e complementadas com a aplicação do Método de Mosler, o qual permitiu mensurar e classificar o risco associado a quatro dimensões: leitura das políticas de privacidade, práticas de segurança, atualização das palavras-passe e percepção de segurança das aplicações móveis face aos websites. Os resultados evidenciam que níveis mais elevados de conhecimento e de adoção de práticas seguras correspondem a riscos residuais ou muito baixos, enquanto comportamentos menos informados ou a ausência de medidas preventivas se associam a riscos elevados ou críticos. Verificou-se, ainda, uma tendência para maior confiança nas aplicações móveis em detrimento dos websites, nem sempre sustentada por critérios técnicos de segurança.

Em resumo, o fator humano permanece o principal vetor de vulnerabilidade no *m-commerce*, sendo determinante o reforço da literacia e da sensibilização digital dos utilizadores. O estudo contribui, assim, para uma compreensão mais abrangente da relação entre percepção, comportamento e risco, fornecendo evidências que poderão apoiar o desenvolvimento de estratégias de segurança mais eficazes e centradas no utilizador.

Palavras-chave: Comércio eletrónico; Mobile commerce; Segurança da informação; Literacia digital; Percepção de risco; Metodo Mosler; Malwares.

Abstract:

The rapid evolution of mobile technologies has transformed *mobile commerce* (*m-commerce*) into a key channel for digital consumption, combining convenience and accessibility. However, this transition also raises significant challenges in the field of information security, particularly regarding how users perceive and manage the risks associated with their online interactions. This study aims to analyse the perception of security in m-commerce, exploring the relationship between digital literacy, protective practices, and perceived vulnerability. A quantitative methodology was applied through an online questionnaire answered by 44 participants. The responses were analysed using descriptive statistics and complemented by the Mosler Method, which allowed the measurement and classification of risk across four dimensions: reading of privacy policies, security practices, password update frequency, and perceived security of mobile applications compared to websites. The results show that higher levels of digital literacy and consistent security habits are associated with residual or very low risk, while limited knowledge and lack of preventive measures correspond to high or critical risk. Participants demonstrated greater trust in mobile applications than in websites, although this perception does not always reflect stronger technical security standards.

In an overall, concluded that the human factor remains the primary source of vulnerability in *m-commerce*, highlighting the need to strengthen users' digital literacy and awareness. This research contributes to a broader understanding of the relationship between perception, behaviour, and risk, providing evidence to support the development of more effective and user-centred security strategies.

Key words: Electronic commerce; Mobile commerce; Information security; Digital literacy; Risk perception; Mosler Method; Malwares.

Índice geral

Capítulo I - Introdução	1
1 Introdução.....	2
Capítulo II – Estado da Arte	4
2 Estado da Arte	5
2.1.1 Caracterização do comércio eletrónico.....	5
2.1.2 Comércio Tradicional vs Comércio eletrónico.....	6
2.1.3 Barreiras na adoção do comércio eletrónico.....	7
2.2 Segmentos originados do comércio eletrónico.....	8
2.2.1 Modelos de negócio derivado do comércio eletrónico.....	9
2.2.1.1 M-Commerce.....	10
2.2.1.2 S-Commerce	10
2.2.1.3 T-commerce.....	11
2.2.1.4 Dropshipping	11
2.2.2 Vantagens e desvantagens do comércio eletrónico	12
2.3 Crescimento e expansão do comércio eletrónico	13
3 Caracterização do comércio eletrónico em Portugal	14
3.1 Perfil do utilizador de comércio eletrónico em Portugal.....	15
3.2 Tendências e perspetivas futuras do e-commerce em Portugal.....	18
4 O Mobile Commerce	20
4.1 Vantagens do m-commerce para o consumidor e para as empresas.....	21
4.2 Importância da segurança da informação no m-commerce	22
4.3 Desafios à segurança da informação no mobile commerce.....	23
4.4 Transformação do comportamento do consumidor	25
4.5 Identificação e avaliação dos riscos de segurança da informação no mobile commerce	26
4.6 Conceito de Risco e Método de Mosler	27

5	Considerações finais da revisão teorica.....	28
Capítulo III – Metodologia		30
6	Metodologia.....	31
6.1	Tipologia de Estudo.....	31
6.2	Revisão de literatura	31
6.2.1	Critérios de inclusão	32
6.2.2	Critérios de exclusão	32
6.2.3	Recolha de dados	32
6.3	Pesquisa quantitativa	33
6.3.1	Critérios de inclusão	33
6.3.2	Critérios de exclusão	33
6.3.3	Recolha de dados	33
7	Contextualização do questionário.....	34
8	Análise e discussão dos resultados	35
8.1	Caracterização da amostra	35
8.2	Análise dos dados	37
8.3	Testes.....	43
9	Aplicação do Método Mosler à análise de risco no M-commerce	46
9.1	Etapas para aplicação do Método Mosler.....	47
9.2	Análise de risco de variaveis	49
9.2.1	Práticas de segurança	49
9.2.2	Literatura da politica de privacidade	50
9.2.3	Atualização da palavra-chave.....	52
9.2.4	Perceção do maior risco associado ao uso de dispositivos móveis	53
9.2.5	Perceção de segurança das aplicações móveis face aos websites no navegador.....	55
9.3	Considerações finais da análise de risco.....	56

Capítulo IV – Conclusão	58
10 Conclusão	59
10.1 Síntese dos resultados	59
10.2 Implicações teóricas	60
10.3 Implicações práticas	60
10.4 Limitações do estudo	60
10.5 Recomendações para investigação futura.....	61
Referências bibliográficas.....	63
11 Referências Bibliográficas.....	64
Apêndices.....	67
12 Apêndices	68
12.1 Apêndice I – Questionário Aplicado	68
12.2 Formulas e estruturas de calculo utilizado	73
Anexos.....	75
13 Anexos.....	75
13.1 Anexo I – Escala Metodo de Mosler	75

Índice de Figuras

Ilustração 1 Percentagem de indivíduos residentes em Portugal que efetuaram compras através da Internet.....	14
Ilustração 2 Motivos para fazer compras online.....	17
Ilustração 3 Categorias com mais compras	18
Ilustração 4 Escala avaliação de risco	74
Ilustração 5 Escala de Pontuação Criterio F	75
Ilustração 6 Escala de pontuação criterio S	76
Ilustração 7 Escala de pontuação criterio P	76
Ilustração 8 Escala de pontuação critério E	76
Ilustração 9 Escala de pontuação critério A	76
Ilustração 10 Escala de pontuação critério V	77
Ilustração 11 Tabela de classificação Valor ER	78
Ilustração 12 Tabela calssificação classe de risco	78

Índice de Tabelas

Tabela 1 - Caracterização demográfica da amostra de inquiridos.....	36
Tabela 2 Conhecimento dos inquiridos sobre ameaças digitais e práticas de segurança no m-commerce	38
Tabela 3 Práticas preventivas de segurança dos inquiridos no contexto do m-commerce	41
Tabela 4 Perceção de segurança dos inquiridos relativamente ao uso de dispositivos móveis no m-commerce.....	42
Tabela 5 Frequência e principais motivos para a realização de compras online em dispositivos móveis	43
Tabela 6 Resultados da comparação das variáveis de segurança digital segundo o nível de escolaridade e idade dos inquiridos	46
Tabela 7 Classificação e Interpretação dos Níveis de Risco	49
Tabela 8 Atribuição das pontuações dos critérios do Método Mosler para a variável Práticas de Segurança	50
Tabela 9 Atribuição das pontuações dos critérios do Método Mosler para a variável Política de Privacidade	51
Tabela 10 Cálculo dos níveis de risco associados à Leitura da Política de Privacidade	52

Lista de abreviaturas

AI - Artificial Intelligence (Inteligência Artificial)

APP - Aplicação móvel

C2C - Consumer to Consumer

C2B - Consumer to Business

B2B - Business to Business

B2C - Business to Consumer

B2G - Business to Government

ER - Evolução do Risco

F - Função (critério do Método de Mosler)

S - Substituição (critério do Método de Mosler)

P - Profundidade (critério do Método de Mosler)

E - Extensão (critério do Método de Mosler)

A - Agressão (critério do Método de Mosler)

V - Vulnerabilidade (critério do Método de Mosler)

GDPR - General Data Protection Regulation (Regulamento Geral sobre a Proteção de Dados)

HTTP - Hypertext Transfer Protocol

MB WAY - Sistema de pagamento móvel português

M-Commerce - Mobile Commerce

RGPD - Regulamento Geral sobre a Proteção de Dados (versão em português do GDPR)

PCI DSS - Payment Card Industry Data Security Standard

S-Commerce - Social Commerce

T-Commerce - Television Commerce

PIN - Personal Identification Number

QR - Quick Response (Código QR)

URL - Uniform Resource Locator

Wi-Fi - Wireless Fidelity

UI - User Interface (Interface do Utilizador)

UX - User Experience (Experiência do Utilizador)

CAPÍTULO I - INTRODUÇÃO

1 Introdução

O rápido avanço das tecnologias de informação e comunicação, aliado à massificação do acesso a redes móveis, tem vindo a transformar profundamente os hábitos de consumo e as estratégias de negócio. Neste contexto, o mobile commerce (m-commerce) destaca-se como um canal com elevado potencial de alcance e conveniência, permitindo transações em qualquer lugar e a qualquer momento. Todavia, a própria portabilidade dos dispositivos móveis e a sua frequência de ligação a redes públicas ou de origem desconhecida expõem os utilizadores a riscos de segurança, como phishing, malware e interceptação de dados. A perceção destes riscos assume, por isso, um papel determinante na confiança do consumidor e, consequentemente, nas taxas de conversão e de fidelização das plataformas móveis.

Este estudo propõe-se a analisar a perceção de segurança dos consumidores no uso do m-commerce em Portugal, enquadrando-a no panorama nacional de penetração de dispositivos móveis e no crescimento acelerado das transações online após a pandemia de COVID-19. Para tal, foram definidos os seguintes objetivos:

- Caracterizar as principais ameaças à segurança da informação em dispositivos móveis utilizados para comércio eletrónico.
- Avaliar o nível de literacia digital e a familiaridade dos diferentes grupos etários com métodos de autenticação.
- Determinar o impacto dessa perceção de risco na intenção de compra e na fidelização dos utilizadores.
- Propor diretrizes para a otimização de mecanismos de segurança e de comunicação de alertas, de modo a reforçar a confiança do consumidor.

A recolha e análise de dados assenta num design misto, combinando revisão sistemática da literatura com um inquérito estruturado a utilizadores de m-commerce em Portugal. A aplicação do Método Mosler ao questionário permite validar a consistência interna das escalas e garantir a fiabilidade das medidas de perceção de segurança, bem como cruzar variáveis demográficas (idade, localidade, nível de habilitações) com padrões de utilização e de confiança.

A estrutura da dissertação organiza-se em seis capítulos. No Capítulo II, apresenta-se a revisão teórica sobre e-commerce, subsegmentos (m-commerce, s-commerce, dropshipping) e segurança da informação no contexto móvel. O Capítulo III descreve a metodologia adotada, em particular o desenho do inquérito, o pré-teste, o procedimento de validação pelo Método Moseley e a caracterização da amostra. Segue-se, no Capítulo IV, a análise dos resultados do inquérito e discussão dos principais achados. O Capítulo V aprofunda as implicações práticas, aborda as limitações do estudo e propõe linhas de investigação futura. Finalmente, o Capítulo VI sintetiza as conclusões, reformula as recomendações para empresas e decisores públicos e sugere orientações para futuras investigações.

2 Estado da Arte

A crescente digitalização da economia e a generalização do acesso à Internet móvel têm vindo a redefinir o modo como consumidores e empresas interagem, dando origem a novos modelos de negócio e a novas formas de transação comercial. Neste contexto, o mobile commerce (m-commerce) emergiu como uma extensão natural do comércio eletrónico tradicional, combinando conveniência, mobilidade e personalização. Contudo, esta evolução tecnológica trouxe também desafios significativos no domínio da segurança da informação, nomeadamente no que respeita à proteção de dados pessoais e à perceção de risco associada à utilização de plataformas móveis. O presente capítulo tem como objetivo revisar o enquadramento teórico e empírico do tema, explorando as principais contribuições científicas e os desenvolvimentos recentes na área do comércio eletrónico e móvel. Para tal, são abordados os conceitos fundamentais de e-commerce e m-commerce, a sua evolução histórica, os modelos de negócio associados, bem como os fatores que influenciam a adoção destas tecnologias por parte dos consumidores.

De seguida, são analisados os desafios de segurança e privacidade inerentes ao ambiente digital, com especial enfoque no contexto móvel, onde a portabilidade dos dispositivos e a multiplicidade de redes de acesso potenciam novas formas de vulnerabilidade. Por fim, discute-se a perceção de segurança e confiança do utilizador, relacionando-a com os comportamentos de compra e as práticas individuais de autoproteção, de modo a sustentar a base teórica que enquadra a investigação empírica apresentada nos capítulos seguintes.

2.1.1 Caracterização do comércio eletrónico

O comércio eletrónico (ou e-commerce) pode ser definido como qualquer transação comercial incluindo compra, venda, trocas de bens ou serviços realizada total ou parcialmente por meios eletrónicos, sobretudo através da Internet. Embora a sua forma mais reconhecida envolva lojas virtuais e pagamentos online, o conceito abrange igualmente processos de suporte, como sistemas de gestão de inventário, plataformas de CRM, marketing digital e logística integrada (Laudon & Traver, 2007).

As raízes do e-commerce remontam aos anos 1970, com a introdução do EDI (Electronic Data Interchange) e do EFT (Electronic Funds Transfer), que automatizaram a troca de documentos e valores entre empresas. Foi só com o surgimento da World Wide Web, em meados da década de 1990, que o comércio digital ganhou escala global, beneficiando da interface gráfica e do protocolo HTTP criado por Tim Berners-Lee (Segal, 1995). Desde

então, as vendas online registaram um crescimento exponencial, passando de nichos especializados para representarem hoje uma fatia significativa do retalho mundial.

Em Portugal, a adoção do e-commerce tem vindo a aumentar: dados recentes apontam para cerca de 44 % de penetração entre consumidores residenciais, ainda que abaixo da média europeia (72 %) (ANACOM, 2022). Este crescimento reflete não só o maior acesso a dispositivos conectados, mas também a diversificação dos meios de pagamento – da referência Multibanco e MB Way aos cartões de crédito/débito e carteiras digitais.

Do lado das empresas, o e-commerce transformou modelos de negócio tradicionais, permitindo a redução de custos fixos (como imóveis e stock), a segmentação precisa de públicos através de campanhas online e o acompanhamento em tempo real de métricas de performance. No entanto, esta disrupção trouxe também novos desafios, nomeadamente a necessidade de assegurar a segurança da informação em todas as fases do processo – desde a proteção de dados pessoais até à encriptação de transacções financeiras – e de otimizar a logística da “última milha” para satisfazer as expectativas de rapidez e fiabilidade dos clientes.

2.1.2 Comércio Tradicional vs Comércio eletrónico

O e-commerce caracteriza-se por vendas de bens ou serviços com o auxílio da Internet, já o comércio tradicional é caracterizado por ter obrigatoriamente como ponto de venda uma loja física. No e-commerce com o recurso à Internet os vendedores têm a capacidade de criar plataformas digitais, onde estes vendem os seus bens e serviços.

Assim, os clientes conseguem ter uma experiência de compra mais personalizada, podendo escolher como compram e pagam de acordo com as suas preferências e necessidades (Bornia, Donadel & Lorandi, 2006).

As diferenças entre os dois modelos podem ser analisadas segundo quatro dimensões principais: âmbito geográfico, aproximação entre produtor e consumidor final, conforto para o consumidor e segurança.

No que respeita ao âmbito geográfico, o mercado tradicional tem uma área de atuação condicionada territorialmente, ainda que isso não impeça consumidores de outras regiões de se deslocarem até ele. Já o mercado eletrónico ultrapassa esta barreira, permitindo que as empresas operem à escala global, sem que o consumidor tenha de se deslocar (Mistry & Dhavale, 2011). Esta interligação global contribui também para uma aproximação entre

produtor e consumidor final. Segundo Canetta, Cheikhrouhou e Glardon (2013), ao conectar vários elementos da cadeia de produção e distribuição, o e-commerce permite reduzir intermediários, o que tende a traduzir-se em preços mais competitivos.

O conforto para o consumidor é outro fator diferenciador. A ausência de restrições físicas e de horário torna a compra mais cómoda e acessível em qualquer momento. Em contraste, o comércio tradicional mantém-se relevante enquanto estrutura do mercado moderno, sobretudo no que diz respeito à distribuição de bens das indústrias para os consumidores (Parente, 2000; Hillmann, 2013).

Por último, a segurança é uma dimensão onde os dois modelos se distinguem claramente. No comércio tradicional, a transação decorre presencialmente, o que reduz a exposição a ameaças digitais. No e-commerce, por se apoiar em plataformas online e no tratamento de dados pessoais e financeiros, surgem riscos específicos — como fraude, roubo de identidade ou acesso indevido a informação — que exigem medidas adicionais de proteção, tema que será aprofundado nos capítulos seguintes.

2.1.3 Barreiras na adoção do comércio eletrónico

Apesar da rápida expansão do e-commerce, várias barreiras continuam a dificultar a sua adoção plena, tanto ao nível das empresas como dos consumidores. Em termos externos, a incompatibilidade de interfaces B2B, a fragmentação de padrões e as diferenças legislativas internacionais impõem custos adicionais de integração e conformidade (Van Toorn et al., 2006). A nível interno, muitas organizações revelam resistência à mudança e falta de competências digitais, subestimando o potencial da Internet para aumentar eficiência e alcance (Stockdale & Standing, 2004).

Para as pequenas e médias empresas (PME), as dificuldades na integração da cadeia de abastecimento tornam-se ainda mais evidentes: a perceção de que os custos iniciais de adaptação superam os benefícios imediatos leva a uma adoção tardia (Korchak & Rodman, 2001). A isto soma-se a identificação deficiente de vantagens, uma vez que sem incentivos claros — como reduções de preço ou melhorias de serviço — o apelo ao e-commerce fica reduzido. No plano do consumidor, as diferenças culturais e a desigualdade de literacia digital afetam a confiança: em Portugal, por exemplo, a elevada percentagem de utilizadores seniores e residentes em zonas rurais culmina numa menor predisposição para partilhar dados pessoais online, por receio de fraude ou de má experiência de compra. Adicionalmente, a perceção de insegurança no m-commerce

alimentada por notícias sobre ataques de phishing e malware em dispositivos móveis condiciona ainda mais a sua adoção, levando muitos utilizadores a preferir o canal presencial (Ferreira & Pitwak, 2009; Stockdale & Standing, 2004).

Finalmente, há barreiras de ordem prática: a logística da última milha, com custos elevados e prazos de entrega pouco fiáveis em certas regiões, e a falta de opções de pagamento digital universalmente aceites, nomeadamente para quem não dispõe de cartões de crédito, tornam a experiência online menos competitiva face ao comércio tradicional. Só ultrapassando estas barreiras através de formação em literacia digital, simplificação de processos B2B, reforço dos padrões de segurança e melhoria logística será possível potenciar todo o alcance e conveniência do e-commerce e do m-commerce em particular.

2.2 Segmentos originados do comércio eletrónico

Para conseguirmos caracterizar o e-commerce, também é necessário olhar quais os tipos de comércio eletrónico existentes, B2B ou business-to-business, B2C ou business to consumer, C2C ou consumer-to-consumer, C2B ou consumer-to-business, interbusiness e-commerce e non-business e-commerce. Segundo Turban, Lee, King & Chung (1999), os tipos de transações mais famosos são, B2C e B2B.

Inicialmente, o e-commerce era dominado por transações B2B, segundo Laudon & Traver (2007) este segmento é fundamental para a eficiência das operações comerciais entre empresas, simplificando processos de aquisição e reduzindo custos. Também podemos ver o comércio B2B como “qualquer transação efetuada entre organizações em que, pelo menos uma das seguintes atividades seja realizada por meios eletrónicos, sendo estas: produção, distribuição, comercialização, venda ou entrega” refere a World Trade Organization (2013, p. 13).

Concomitantemente, o comércio eletrónico B2C (Business-to-Consumer) também começou a ganhar tração, permitindo que as empresas vendessem diretamente aos consumidores. Adoção deste segmento de comércio eletrónico criou uma disrupção no paradigma e teve um impacto substancial nas práticas de compra dos indivíduos, oferecendo conveniência e uma variedade crescente de produtos e serviços ao alcance de um clique. “O comércio B2C é caracterizado por uma transação realizada entre uma organização e o seu consumidor final com a utilização da Internet.”, (Albertin, J. L.(2004)).

À medida que o e-commerce continuou a prosperar, novos modelos de negócios surgiram, incluindo o comércio eletrônico C2C (Consumer-to-Consumer), Jones & Leonard (2010) e Schneider (2010), consideram que este segmento é caracterizado por uma transação de bens ou serviços entre consumidores, tendo a possibilidade de estabelecer um intermediário para facilitar no processo de compra e venda por parte do consumidor, exemplificado pelo sucesso do eBay, que permitiu aos consumidores venderem produtos diretamente a outros consumidores, criando um mercado virtual global. O êxito deste tipo de comércio eletrônico depende da segurança oferecida pelas plataformas intermediárias aos seus utilizadores, já que é crucial haver confiança mútua entre eles.

Por último, o segmento B2G (Business-to-Government) está em ascensão, à medida que governos de todos os níveis procuram simplificar os seus processos de aquisição e reduzir custos (Laudon & Traver, 2007), abrindo oportunidades para empresas que oferecem serviços e produtos para o setor público.

2.2.1 Modelos de negócio derivado do comércio eletrônico

Com a popularização do *e-commerce*, o aumento da procura e da concorrência, levou as organizações a optarem por alguns modelos de e-commerce, com o objetivo de melhorar a sua eficiência e consequentemente a sua capacidade concorrencial (Oliveira et al., 2002).

São vários os tipos de *e-commerce* e modelos disponíveis para entrar neste mercado, para tal, é fundamental que cada indivíduo saiba classificar em que formato de negócio pretende investir. Alguns exemplos de modelos de comércio online são:

- M-Commerce;
- S-Commerce;
- T-Commerce;
- Dropshipping.

Importa notar que estes conceitos não se situam todos ao mesmo nível de análise. M-Commerce, S-Commerce e T-Commerce referem-se a canais ou plataformas de acesso ao comércio eletrônico — respetivamente, dispositivos móveis, redes sociais e televisão — enquanto o Dropshipping corresponde a um modelo de negócio baseado na logística e na gestão de stocks. Ainda assim, são aqui apresentados em conjunto por constituírem variantes ou desenvolvimentos relevantes do e-commerce.

2.2.1.1 M-Commerce

Com a globalização e difusão da Internet o ambiente de negócios tem vindo a sofrer numerosas alterações, sendo uma delas a crescente procura por mobilidade, permitindo assim ter acesso a qualquer recurso, informação ou serviços em qualquer lugar (Steendern, 2002).

Através destas mudanças, surge então o mobile commerce ou mais conhecido como M-Commerce. Este conceito é utilizado então quando para a realização de transações económicas é feita a utilização de dispositivos móveis, sendo este uma variante do e-commerce que para Seybold (2000) este conceito é o ato de realizar negociações via Internet. Assim, o M-commerce pode ser considerado como um subconjunto das negociações online, abrangendo diferentes modelos como B2C, B2B e C2C, na medida em que representa um canal de acesso que atravessa estes modelos e não um modelo de negócio próprio.

Este tipo de comércio engloba, todo o tipo de dispositivos de computação móvel utilizados para a realização de qualquer transação eletrónica, podendo as mesmas ser realizadas em qualquer lugar (Lyytinen K, 2001).

2.2.1.2 S-Commerce

O S-Commerce, ou Social Commerce, é um modelo de comércio realizado através das redes sociais, como Instagram, Facebook, entre outras (Turban et al., 2010).

Este modelo pode ser designado como um subgrupo do e-commerce que recorrer ao social media para a realização de compras ou vendas de produtos, inteiramente com recurso a serviços online (Turban, et al, 2010).

Este modelo de negócio utiliza o ponto chave de uma rede social, mas especificamente o relacionamento entre pessoas. Como tal, várias empresas estão a recorrer cada vez mais a este tipo de negócio, para captar assim mais clientes ou divulgar os seus produtos (Mendes, 2013).

O S-commerce, funciona através da publicação de experiências, avaliações e feedback dos produtos. Assim através destas informações as empresas passam a conhecer melhor o seu publico alvo, levando a um aumento e compreensão das preferências dos clientes em relação a qualquer marca, produto ou serviço (Turban et al., 2010). Dada a sua natureza assente no relacionamento entre utilizadores e na partilha de experiências, o S-

Commerce aproxima-se fortemente da lógica do C2C (Consumer-to-Consumer), já que muitas das transações ocorrem entre consumidores que avaliam, recomendam ou vendem produtos diretamente a outros consumidores.

2.2.1.3 T-commerce

São vários os estímulos ao comércio eletrónico, sendo um deles o T-Commerce, por outra palavras este é um novo subgrupo do e-commerce (Kim, Lee, & Leemand, 2004). Esta nova fonte de negócio, é uma ótima ferramenta para as empresas que desejam aumentar o seu volume de negócio, pois considerando a número de horas que as pessoas passam em frente a uma TV, temos então um grande número de consumidores que podem comprar qualquer produto a qualquer hora. Segundo Ghisi (2010), o T-commerce é baseado em 3 características:

- Apresentação;
- Forma de pagamento;
- Conteúdo associativo.

Para além destas 3 características apresenta ainda 4 modelo para o T-commerce:

- Canal de vendas: Canal que oferecer inúmeros produtos ou serviços;
- Relacionados à Programação: Aplicações que podem aparecer em programas televisivos;
- Publicidade interativa: Esta cria interatividade com os consumidores através de aplicações específicas;
- Outras iniciativas: Utilização o T-commerce para outros fins.

Em suma, a grande vantagem deste modelo é a capacidade de o telespectador um produto que esteja a ser publicitado através de uma propaganda televisiva.

2.2.1.4 Dropshipping

Segundo Cheong, Goh e Song (2015), o dropshipping ocorre quando o vendedor online não possui qualquer tipo de stocks, isto é, o vendedor quando recebe o pedido de compra, reencaminha este pedido diretamente aos fornecedores que por sua vez, irão preparar e enviar o produto ao consumidor final.

Para Zajac e Łódzki (2014), esta metodologia acaba por ser mais lucrativa na maioria das vezes, uma vez que o vendedor online terceiriza o processo de stocks e distribuição dos

produtos, deixando deste modo de ter este custo. Netessine et al. (2001), afirma que este modelo é completamente diferente do modelo utilizado no mercado tradicional, onde o comerciante armazena os stocks, onde algumas vezes este acaba por não ser dono do mesmo.

No dropshiping esta política de stocks e armazenamento é totalmente suportado pelo fornecedor. Este modelo só é possível devido a dois fatores, ao facto do consumidor que utiliza o e-commerce não consegue saber de onde o seu produto está a ser enviado e devido ao facto de este não esperar uma entrega imediata do produto.

Então com a junção destes dois fatores, foi possível desenvolver este modelo de forma eficiente e com custos reduzidos. A adoção deste modelo traz inúmeras vantagens, uma vez que os comerciantes eliminam todos os custos referentes aos stocks e ajudam novos empreendedores que pretendam entrar no mercado, pois não necessitam de um capital próprio para iniciar um negócio online (Rabinovich et al, 2008).

Para Cheong et al (2015), o dropshipping pode ser benéfico tanto para o comerciante como para o fornecedor, visto que através deste modelo ambos podem concentrar os seus esforços nas suas atividades principais. Nenhum modelo ou sistema é infalível, então não se poderia esperar o mesmo do dropshipping, pois mesmo trazendo tantas vantagens também pode ter algumas desvantagens. Rao et al. (2011), afirma que em alguns casos a qualidade do produto pode ser um problema, uma vez que a qualidade do produto está fora do alcance do comerciante, pois o produto nunca passa por este mesmo.

2.2.2 Vantagens e desvantagens do comércio eletrónico

O e-commerce, além de representar uma vantagem competitiva para as empresas que operam nele, oferece uma variedade de benefícios adicionais. Em primeiro lugar, reduz o tempo necessário para transações e garante a disponibilidade global de informações. Esse modelo de negócios encurta distâncias, diminui os custos operacionais e facilita trocas rápidas de informações sobre empresas e produtos, abrindo acesso a um mercado global e ampliando as opções de compra para os consumidores. Além disso, estabelece uma conexão mais direta com os consumidores ao manter constantemente atualizadas as informações sobre produtos e preços (Gunasekaran, 2002).

Segundo Albertin (2010), esse novo canal de vendas promove uma maior conectividade entre consumidores, empresas e fornecedores, criando novas oportunidades de negócios

anteriormente impossíveis. Também permite a customização de produtos ou serviços, levando a uma redução significativa no tempo de resposta aos consumidores. A criação de uma loja virtual é menos dispendiosa e mais rápida do que uma loja física, e sua manutenção é mais fácil, já que pode operar continuamente, 24 horas por dia, 7 dias por semana (Reedy & Schullo, 2007). A conveniência oferecida pelo e-commerce aos usuários é uma de suas maiores vantagens em relação ao comércio tradicional, pois permite realizar pesquisas e compras sem a necessidade de visitar fisicamente uma loja (Ferreira & Pitwak, 2009).

No entanto, algumas desvantagens também são identificáveis neste modelo de comércio. A principal delas é a questão da segurança, já que os clientes geralmente precisam fornecer uma série de dados pessoais, como números de cartão, o que pode gerar preocupação (Ferreira & Pitwak, 2009). Outro desafio é garantir condições adequadas de entrega e facilitar os métodos de pagamento, pois nem todos os clientes têm acesso a cartões para pagamentos online. O receio de problemas na entrega ou de produtos danificados, bem como as dificuldades de acesso à Internet em algumas regiões, também podem dificultar esse modelo de negócios (Turban et al., 1999; Trepper, 2000; Afuah & Tucci, 2001).

Complementando esta análise, a Comissão Europeia (2015) identificou os principais motivos que levam os clientes a optar por compras online, como a disponibilidade 24/7 das lojas, preços competitivos, acesso rápido a informações e ampla variedade de escolha.

Apontou, no entanto, algumas desvantagens, que incluem custos de devolução, dificuldades em obter reembolsos ou resolver problemas, tempos de entrega prolongados, confiança nos vendedores e nos próprios mercados online, além de barreiras nos métodos de pagamento para alguns clientes.

2.3 Crescimento e expansão do comércio eletrônico

À medida que avançamos no século XXI, o comércio eletrônico continua a crescer rapidamente, e as projeções de crescimento são otimistas. Tecnologias emergentes, como a Internet das Coisas (IoT) e a inteligência artificial, estão a reformar o método como as empresas abordam o e-commerce, personalizando ainda mais a experiência do cliente e melhorando a eficiência operacional.

Este panorama histórico e evolutivo do comércio eletrónico delineia claramente sua importância crescente na economia global.

Podemos dizer que o e-commerce passou por 4 etapas na sua evolução desde 2000. Nos últimos 20 anos, o e-commerce concentrou-se em ser cada vez mais conveniente, adaptando-se às mudanças nos comportamentos e expectativas dos consumidores. Passamos de um único computador estacionário por família para dispositivos móveis. A transformação digital levou-nos de uma interface de utilizador básica para lojas virtuais interativas que oferecem serviços semelhantes aos de um vendedor de uma loja física. A evolução do e-commerce concentrou-se em aprimorar a experiência tanto para os consumidores quanto para os vendedores.

Ainda, a Forbes, o e-commerce encontra-se num contante crescimento, sendo que o Covid-19 veio acelerar ainda mais este modelo de negócio.

3 Caracterização do comércio eletrónico em Portugal

A evolução do comércio eletrónico em Portugal tem sido notável. De acordo com o relatório da ANACOM, aproximadamente 44% dos portugueses já incorporaram o comércio eletrónico nas suas vidas diárias, refletindo a adesão significativa a esta prática. No entanto, é importante notar que Portugal permanece abaixo da média da União Europeia, que atinge uma taxa de utilização de 72% entre os consumidores (ANACOM, 2022), como se pode observar na Ilustração 1.

Destaque merece o facto de Portugal se destacar como o segundo país na Europa com o maior índice de compras em websites estrangeiros. A China surge como um protagonista central nesse contexto, representando a origem de quase metade das compras online realizadas por consumidores portugueses fora das fronteiras nacionais, seguida por Espanha, Reino Unido e Estados Unidos da América. Esta tendência denota a

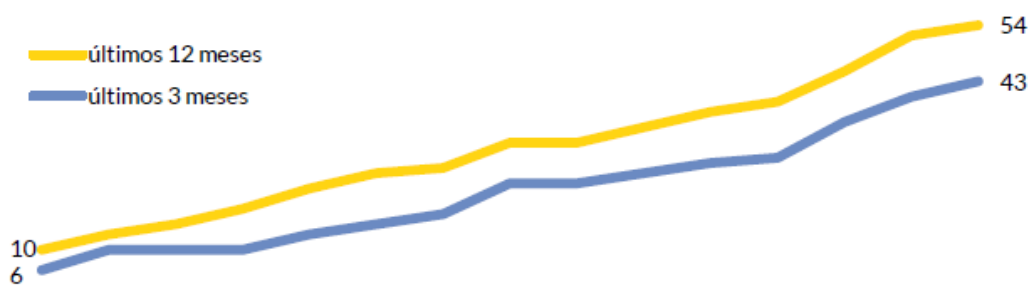


Ilustração 1 Percentagem de indivíduos residentes em Portugal que efetuaram compras através da Internet

predisposição dos consumidores portugueses para aceder a mercados internacionais e a preferência por uma ampla gama de produtos e oportunidades disponíveis através do comércio eletrónico.

No entanto, o comércio eletrónico em Portugal ainda enfrenta alguns desafios, segundo o relatório da AICEP Crescimento do comércio eletrónico em Portugal desenvolvido em 2020 “Os principais constrangimentos da evolução e do desenvolvimento do e-commerce em Portugal são:

- Elevada oferta de espaços comerciais com horários alargados;
- Dificuldade na entrega a tempo e horas das encomendas, principalmente no interior do país;
- Falta de escala e necessidade de alocar recursos a outras atividades, limitando a capacidade de investimento em inovação;
- Elevada iliteracia digital e financeira do consumidor nacional, representando um obstáculo ao desenvolvimento do e-commerce e ao aumento da utilização da Internet;
- Adoção tardia em Portugal dos meios de pagamento digital com elevada utilização a nível internacional, prejudicando a competitividade dos operadores nacionais;
- Desconfiança por parte dos consumidores na realização de pagamentos online;
- Consumidores nacionais não estão dispostos a pagar portes de envio;
- Consumidores nacionais compram fora de Portugal, uma vez que não há diversidade de oferta suficiente no país, além de ser geralmente mais barato comprar no estrangeiro;
- Dificuldade de captação e retenção de talento por parte das empresas nas áreas de engenharia, tecnologia e informática;”.

3.1 Perfil do utilizador de comércio eletrónico em Portugal

O perfil do consumidor em Portugal é diversificado e abrange várias faixas etárias, refletindo uma sociedade cada vez mais adaptada à utilização de tecnologias digitais. Como mencionado no relatório da ANACOM, os consumidores portugueses demonstram uma clara preferência por realizar compras online através de computadores, embora dispositivos móveis estejam a desempenhar um papel crescentemente relevante na jornada de compra.

Os métodos de pagamento preferenciais variam, o que indica uma vasta gama de opções disponíveis. A Referência Multibanco lidera as escolhas, seguida pelo Cartão de Crédito e Débito, Transferência, Paypal e MBWay (ANACOM, 2022). Esta diversidade reflete as preferências individuais dos consumidores e a conveniência de várias opções de pagamento, promovendo uma experiência de compra personalizada.

No que concerne às categorias de produtos mais adquiridos online pelos portugueses, o relatório da ANACOM destaca uma ampla variedade de opções. A eletrónica, incluindo dispositivos como smartphones, computadores e outros gadgets, ocupa o primeiro lugar. Seguem-se o vestuário, viagens, livros, artigos de beleza, alimentação, apostas e aplicações. Esta distribuição de preferências está em sintonia com as tendências globais, evidenciando a crescente utilização de plataformas online para aquisição de produtos de moda e tecnologia (ANACOM, 2022). Conforme relatado pelos CTT no “CTT e-commerce report 2022” e como se apresenta na Ilustração 2, é fundamental notar que as razões relacionadas com a conveniência continuam a ser dominantes na opção pela compra online.

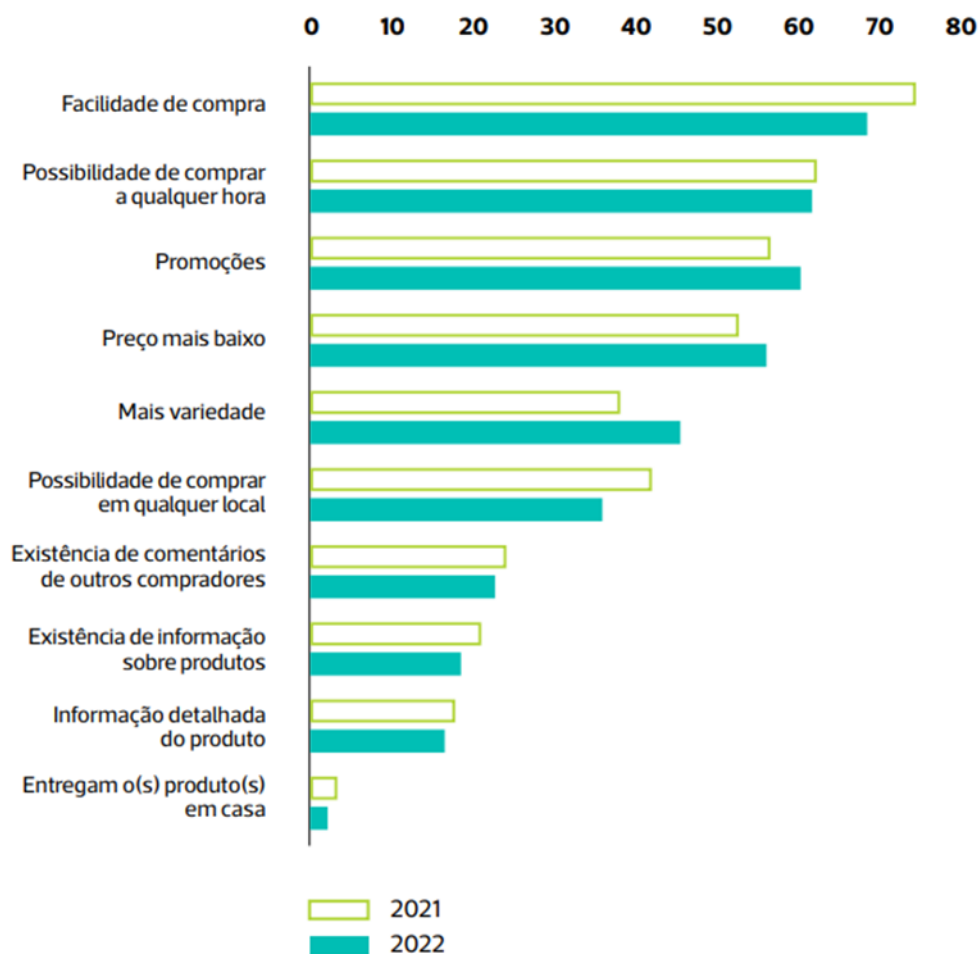


Ilustração 2 Motivos para fazer compras online

Fonte: CTT e-Commerce Report 2022

A facilidade de compra (68,2%) e a possibilidade de comprar a qualquer hora (61,4%) são fatores determinantes. Além disso, a encurtar distâncias, surgem razões relacionadas com o preço, como a existência de promoções (60%) e o preço online mais baixo (55,8%). Esses motivos contribuem para a crescente adesão dos consumidores portugueses ao comércio eletrónico e sublinham a importância da comodidade e da economia como impulsionadores deste mercado em constante evolução.

Agora abordando as categorias mais procuradas, os dados mais recentes (Ilustração 3) mostram que a categoria mais procurada entre os compradores online em Portugal é o Vestuário e Calçado, com uma impressionante taxa de 73% dos e-buyers a optarem por esta categoria, o que representa um aumento de 4,9 pontos percentuais em relação a 2021.

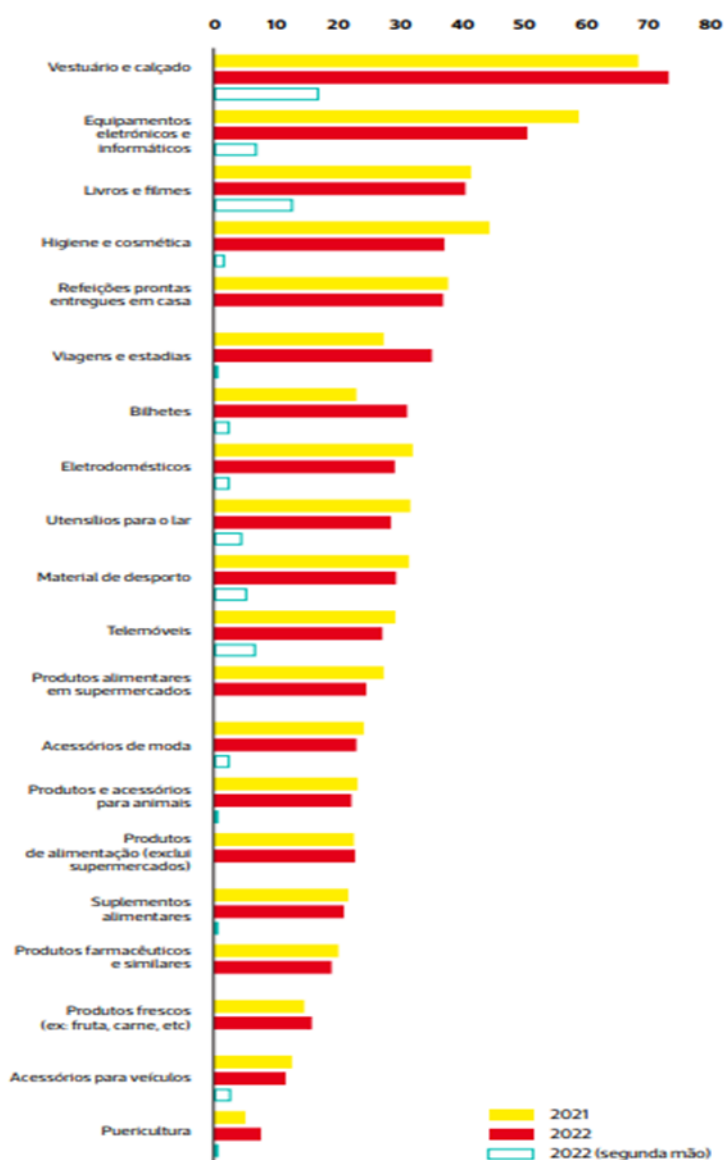


Ilustração 3 Categorias com mais compras

Fonte: CTT e-Commerce Report 2022

As categorias de Equipamentos Eletrónicos e Informáticos, Livros e Filmes, e Higiene e Cosmética surgem em seguida como opções populares entre os consumidores que recorrem ao comércio eletrónico. É relevante destacar que, devido ao crescimento constante deste mercado, as categorias de compras em segunda mão também ganharam destaque. Entre elas, as categorias de Vestuário e Calçado, Livros e Filmes, e Telemóveis são as mais notáveis, demonstrando uma mudança nas preferências dos consumidores em direção a produtos usados ou recondicionados.

3.2 Tendências e perspectivas futuras do e-commerce em Portugal

No panorama global, e-commerce está a testemunhar uma evolução contínua, impulsionada pelo avanço tecnológico e pela mudança nos hábitos de consumo.

Em Portugal, como parte integrante deste cenário dinâmico, observamos tendências semelhantes, mas também específicas, moldadas pelo contexto socioeconómico e pelas preferências dos consumidores locais. Uma tendência notável é a crescente adoção de dispositivos móveis para realizar compras online. Com a popularização dos smartphones e a melhoria da conectividade, os consumidores têm cada vez mais facilidade em realizar compras a qualquer hora e em qualquer lugar. Este aumento no uso de dispositivos móveis para compras online é corroborado por Carvalho et al. (2023), que destacam o crescimento significativo dessa tendência em Portugal.

Além disso, a personalização está a tornar-se uma característica-chave do e-commerce, à medida que as empresas procuram oferecer experiências de compra mais relevantes e envolventes. Tecnologias como a inteligência artificial e o machine learning permitem às empresas analisar o comportamento dos consumidores e oferecer recomendações personalizadas com base nos seus interesses e histórico de compras. A importância crescente dessas tecnologias no e-commerce é reforçada pelos achados de Carvalho et al. (2023), que evidenciam a personalização como um fator chave na melhoria da experiência de compra online.

No entanto, apesar das vantagens evidentes, o e-commerce também enfrenta desafios significativos, tanto para os consumidores como para as empresas. Um dos principais desafios é a questão da segurança dos dados pessoais e financeiros. Com o aumento das transações online, também aumentam os riscos de roubo de dados e fraudes. Carvalho et al. (2023) enfatizam a necessidade de implementação de medidas robustas de segurança, dada a prevalência de riscos de segurança no e-commerce.

Para as empresas, o principal desafio é destacar-se num mercado cada vez mais saturado e competitivo. Essa necessidade de adaptação às tendências digitais para manter a competitividade é evidenciada no estudo de Carvalho et al. (2023), que aborda a influência do e-commerce no comportamento do consumidor e nas operações empresariais.

Apesar dos desafios, o e-commerce continua a oferecer uma série de benefícios significativos para o quotidiano das pessoas. Além disso, Carvalho et al. (2023) confirmam os benefícios do e-commerce, como conveniência e acessibilidade, mas

também apontam para os impactos mais amplos, incluindo mudanças nas dinâmicas de mercado e na interação social.

No que diz respeito às empresas, o e-commerce pode alterar significativamente as dinâmicas do mercado, proporcionando novas oportunidades de crescimento e expansão, mas também introduzindo novos desafios e concorrência. Empresas tradicionais que não se adaptarem às mudanças no comportamento do consumidor e às tendências tecnológicas correm o risco de ficar para trás e perderem quota de mercado para concorrentes mais ágeis e inovadores. Por outro lado, as empresas que conseguirem capitalizar eficazmente as oportunidades oferecidas pelo e-commerce podem alcançar um sucesso significativo e posicionar-se para o crescimento futuro.

Em última análise, o e-commerce está a transformar profundamente a forma como as pessoas compram e vendem produtos e serviços, bem como as dinâmicas do mercado global. A sua adoção generalizada está a impulsionar a inovação e a mudança em diversos setores, desde o retalho até à logística, criando novas oportunidades e desafios para consumidores e empresas. À medida que o e-commerce continua a evoluir e a expandir-se, é fundamental que as partes interessadas, incluindo governos, empresas e consumidores, trabalhem em conjunto para abordar os desafios emergentes e maximizar os benefícios desta revolução digital.

4 O Mobile Commerce

O comércio móvel, também conhecido como mobile commerce ou m-commerce, emerge como uma vertente cada vez mais atrativa tanto a nível internacional como nacional. Este fenómeno impulsiona a adoção de estratégias empresariais, de marketing e de comunicação, visando a interação com o público-alvo através dos dispositivos móveis. O avanço tecnológico no domínio da informação e comunicação tem fomentado uma ampla utilização e inovação em métodos de compra. Isso conduz a uma rápida expansão de diversos canais de compra, proporcionando ao consumidor opções convenientes para adquirir produtos e serviços. O surgimento do mobile commerce é uma resposta natural à evolução tecnológica e à crescente integração de dispositivos móveis, como smartphones e tablets, no quotidiano.

Neste modelo de comércio, os dispositivos móveis são empregues para efetuar transações por meio de uma rede sem fios, permitindo aos utilizadores realizar operações sem

limitações geográficas, ao contrário dos utilizadores do comércio eletrónico tradicional (Büyükožkan, 2012).

Segundo Tiwari e Buse (2007, p. 33), o m-commerce é “qualquer operação que envolva a transferência de propriedade ou direitos de utilização de bens e serviços, que é iniciada e ou concluída utilizando o acesso móvel a redes mediadas por computador com a ajuda de um dispositivo electrónico”

Originado no início do século XXI, este desenvolvimento tecnológico transformou os dispositivos móveis em assistentes pessoais multifuncionais, tudo isto num único dispositivo. A conjugação de acesso à Internet de alta velocidade, interfaces intuitivas e aplicações específicas para transações comerciais desencadeou uma revolução no panorama do comércio.

A crescente popularidade do mobile commerce ao longo dos últimos anos deve-se sobretudo, mas não só, à realização de qualquer tipo de transação comercial a partir de um dispositivo móvel, mais comumente através de smartphones. Ruidong Zhang, Jim Q. Chen e Ca Jaejung Lee (2013) afirmam no seu artigo publicado no Journal of Computer Information Systems que “a popularidade do comércio móvel está diretamente relacionada com dois avanços tecnológicos”, quer pela evolução dos smartphones, que neste momento têm uma capacidade superior a alguns computadores, quer pelo avanço da qualidade da Internet, que neste momento já chegou ao 5G. Assim, pode-se constatar que o m-commerce é o e-commerce nas mãos dos consumidores.

Este segmento, m-commerce, envolve diversas atividades incluindo a compra de produtos, a contratação de serviços, pagamentos e outras transações realizadas por meio de aplicações ou sites otimizados para os diferentes dispositivos móveis.

4.1 Vantagens do m-commerce para o consumidor e para as empresas

Numa visão do consumidor, o mobile commerce proporciona conveniência, permitindo que se possam utilizar os diferentes serviços sem necessidade de estar num local físico. Além disso, oferece também uma experiência de compra personalizada e ágil, com recursos úteis e vantajosos na ótica do consumidor como é o caso das recomendações personalizadas, notificações de promoções e facilidade de navegação.

Já na visão das empresas, o m-commerce representa uma oportunidade de ampliar o alcance de seus produtos e serviços, essencialmente devido à recolha de dados e análises,

fornecendo insights valiosos sobre o comportamento do utilizador e possibilitando a criação de estratégias e abordagens de marketing melhoradas. Um exemplo destas estratégias seria a criação de anúncios personalizados consoante a localização do consumidor fornecida pelos smartphones o que poderá ser uma enorme vantagem para empresas de serviços físicos, os telemóveis constituem outro meio eficaz para a publicidade de produtos e serviços, com o segundo maior alcance potencial, a seguir à televisão (Zabala, 2000)

4.2 Importância da segurança da informação no m-commerce

No contexto global atual, a segurança da informação no m-commerce é um aspecto vital que necessita de atenção constante e inovação. As tendências emergentes em segurança da informação no m-commerce incluem a implementação de leis robustas de segurança cibernética, a necessidade de proteção de dados pessoais e a importância de sistemas de pagamento seguros.

Kashyap e Chaudhary (2023) destacam a importância de um quadro legal sólido para garantir a segurança no e-commerce, observando que a legislação adequada pode ajudar a prevenir fraudes online, proteger dados e fortalecer a confiança dos consumidores. Este princípio é igualmente aplicável ao m-commerce, onde transações e troca de informações ocorrem predominantemente em dispositivos móveis. As empresas enfrentam o desafio de garantir a segurança das transações e a proteção de dados em um ambiente cada vez mais móvel e conectado. Por exemplo, a implementação da Lei de Tecnologia da Informação de 2000 na Índia, conforme discutido por Kashyap e Chaudhary (2023), ilustra como um quadro jurídico pode fortalecer a segurança do e-commerce. Este exemplo pode ser extrapolado para o m-commerce, ressaltando a necessidade de leis específicas que abordem os desafios exclusivos desse setor.

Este exemplo pode ser extrapolado para o m-commerce, ressaltando a necessidade de leis específicas que abordem os desafios exclusivos desse setor. A segurança da informação no m-commerce afeta diretamente o cotidiano das pessoas. À medida que mais consumidores optam por fazer compras online através de dispositivos móveis, eles se expõem a riscos de segurança como fraudes, phishing e violações de dados. O impacto desses riscos não é apenas financeiro, mas também afeta a confiança do consumidor em relação às plataformas de m-commerce. Por outro lado, as empresas enfrentam o desafio de implementar sistemas de segurança robustos, ao mesmo tempo que garantem a

facilidade de uso e a conveniência que os usuários móveis esperam. A violação de dados, não só compromete a confidencialidade dos dados do cliente, mas também pode levar a perdas financeiras substanciais e danos à reputação da empresa.

Para as empresas, a segurança da informação no m-commerce é crítica, não apenas para proteger dados sensíveis, mas também para manter a confiança dos consumidores e cumprir as regulamentações legais. A adoção de padrões internacionais de segurança, como a ISO/IEC 27001, mencionada por Kashyap e Chaudhary (2023), é uma medida que as empresas podem tomar para fortalecer suas práticas de segurança. Além disso, as empresas devem estar cientes das leis locais e internacionais que regulamentam a proteção de dados e a segurança cibernética, adaptando suas políticas e práticas para estar em conformidade com essas normativas.

Em suma, importância da segurança da informação no m-commerce é multifacetada, impactando tanto os indivíduos quanto as empresas. Para os usuários, ela é sinônimo de confiança e segurança, enquanto para as empresas, representa um componente vital para a sustentabilidade e crescimento no cenário digital. À medida que o m-commerce continua a evoluir, a segurança da informação deve permanecer no centro das discussões, garantindo que a conveniência oferecida por esses serviços não seja ofuscada pelos riscos associados à sua utilização.

4.3 Desafios à segurança da informação no mobile commerce

O assunto segurança da informação emerge como um vetor crucial na área do e-commerce e consequentemente no modelo de negócio originado do mesmo m-commerce. A segurança da informação neste ramo contempla tanto a proteção das entidades empresariais quanto a salvaguarda dos direitos e privacidades dos consumidores.

A ubiquidade dos dispositivos móveis e a sua crescente utilização para transações comerciais trazem consigo um espectro alargado de desafios à segurança da informação, que, se não forem devidamente endereçados, podem comprometer a integridade, confidencialidade e disponibilidade dos dados, pilares fundamentais na construção de um ambiente digital seguro.

Um dos desafios prementes no segmento de m-commerce é a vulnerabilidade inerente aos dispositivos móveis. Estes aparelhos, frequentemente atualizados com novas aplicações e conectados a múltiplas redes, podem ser alvos fáceis para malwares e ataques de

phishing, sobretudo quando os utilizadores negligenciam atualizações de segurança ou descarregam aplicações de fontes não confiáveis. Além disso, a natureza portátil dos dispositivos móveis aumenta o risco de perda ou roubo físico, o que pode resultar em acessos não autorizados a informações sensíveis armazenadas no dispositivo.

No que toca à relação entre empresas e consumidores, a segurança da informação no m-commerce desempenha um papel duplamente significativo. Por um lado, falhas de segurança podem levar a violações de dados, expondo informações pessoais dos clientes e colocando em risco a sua privacidade e segurança financeira. Este cenário pode erodir a confiança do consumidor e afetar negativamente a reputação da empresa, resultando em perdas financeiras diretas e indiretas. Por outro lado, a adoção de medidas de segurança demasiado intrusivas ou onerosas pode impactar a experiência do utilizador, levando à perda de clientes para concorrentes que ofereçam soluções mais amigáveis ao utilizador.

A questão das cookies e dos pedidos de acesso aos dispositivos móveis constitui outro campo minado no que respeita à privacidade dos utilizadores e à segurança da informação. Cookies, frequentemente utilizadas para personalizar a experiência de navegação do utilizador, podem também ser empregues para rastrear o comportamento do utilizador de maneira invasiva, coletando informações sem o consentimento explícito deste. Adicionalmente, algumas aplicações móveis solicitam permissões que excedem as necessidades funcionais da aplicação, como o acesso a contactos, mensagens ou localização do dispositivo, aumentando assim o risco de violação de dados pessoais.

Exemplos reais de falhas de segurança em m-commerce não são difíceis de encontrar. Casos como o da Target, onde dados de milhões de cartões de crédito foram comprometidos, ilustram os riscos associados à insuficiência de medidas de segurança robustas. Além disso, a controvérsia em torno da aplicação TikTok, que levantou preocupações sobre a coleta e uso de dados de localização e clipboard em dispositivos móveis, destaca a importância da transparência e do consentimento no uso de dados pelos aplicativos.

Em suma, o impacto mais amplo dos desafios à segurança no segmento de m-commerce é multifacetado, abrangendo desde a proteção de dados pessoais e financeiros dos consumidores até à manutenção da confiança e lealdade do cliente. A implementação de práticas de segurança rigorosas, juntamente com uma abordagem equilibrada que respeite a privacidade e a experiência do utilizador, é fundamental para o desenvolvimento

sustentável do comércio móvel. A adoção de padrões de segurança reconhecidos internacionalmente, como o PCI DSS para transações com cartão de crédito, e o desenvolvimento de novas tecnologias de segurança, como a autenticação biométrica e a encriptação de ponta-a-ponta, são passos essenciais para mitigar os riscos associados ao m-commerce e para fomentar um ambiente digital mais seguro e confiável.

4.4 Transformação do comportamento do consumidor

À medida que o M-Commerce continua a expandir-se e a moldar o cenário comercial, é fundamental compreender o impacto que este setor tem no comportamento dos consumidores e na evolução dos modelos de negócios. Esta análise proporcionará uma visão clara das transformações que ocorreram à medida que os consumidores adotaram os dispositivos móveis para efetuar compras e como as empresas têm respondido a esta mudança.

Uma das mudanças mais notáveis resultantes da ascensão do M-Commerce é a transformação no comportamento do consumidor. Os consumidores estão agora mais inclinados a efetuar compras através de dispositivos móveis, seja por conveniência, variedade de escolha ou acessibilidade. Estudos recentes de Smith, J. (2020) demonstraram que os dispositivos móveis desempenham um papel significativo na pesquisa de produtos, comparação de preços e tomada de decisões de compra. Esta tendência afeta diretamente a forma como as empresas interagem com os seus clientes.

A ascensão do M-Commerce levou a uma rápida adaptação dos modelos de negócios. As empresas tiveram de reestruturar as suas estratégias para acomodar as preferências dos consumidores que agora valorizam a experiência móvel de compras. Isso inclui a otimização de sites e aplicativos para dispositivos móveis, bem como a implementação de funcionalidades específicas para melhorar a experiência do cliente (Khan, M. S., & Islam, S. H. 2021).. Além disso, a logística de entrega teve de ser revista, tornando-se mais ágil e eficiente para atender às expectativas de prazos de entrega mais curtos.

Num entanto, à medida que o M-Commerce continua a crescer, surgem desafios significativos, como a concorrência acirrada e a necessidade de manter a segurança das transações online (European Union. 2018). Neste contexto, as empresas devem explorar oportunidades estratégicas para se destacarem, como programas de fidelização, personalização de marketing e colaborações com empresas de tecnologia para desenvolver soluções inovadoras

4.5 Identificação e avaliação dos riscos de segurança da informação no mobile commerce

A segurança da informação emerge como uma preocupação crítica. Neste ponto, vamos examinar em detalhe os riscos de segurança associados ao M-Commerce e as implicações de ataques cibernéticos e roubo de dados para consumidores e empresas.

Riscos Emergentes no M-Commerce:

Muitos destes riscos não são exclusivos do m-commerce. Intrusões na infraestrutura das empresas, fraudes em transações ou violações de dados guardados em servidores são comuns a todo o comércio eletrónico. Existem, porém, alguns riscos que se tornam mais relevantes quando o canal é um dispositivo móvel. A ligação a redes Wi-Fi públicas é um bom exemplo, assim como a possibilidade de perda ou furto do aparelho enquanto tem sessões iniciadas. A isto soma-se ainda o chamado smishing (tentativas de phishing por SMS), a instalação de aplicações a partir de fontes não oficiais e o simples facto de o ecrã ser pequeno, o que leva muitas vezes o utilizador a ser menos cuidadoso do que seria num computador. Segundo a Verizon (2020), os ataques dirigidos a aplicações móveis e a sites de comércio eletrónico têm vindo a aumentar de forma significativa, e podem levar à exposição de dados sensíveis dos clientes, como informações de pagamento ou dados pessoais.

Ameaças à Privacidade:

A crescente quantidade de dados pessoais armazenados em dispositivos móveis torna-os alvos atrativos para criminosos cibernéticos. Roubo de identidade, phishing e malware direcionado são ameaças comuns que podem comprometer a privacidade dos consumidores (U.S. Federal Trade Commission 2021). Portanto, é fundamental que as empresas implementem medidas rigorosas de segurança para proteger as informações confidenciais dos seus clientes.

Implicações para as Empresas:

Os riscos de segurança no m-commerce têm consequências sérias para as empresas. Para além do impacto na reputação, podem enfrentar sanções legais e regulatórias quando não protegem de forma adequada os dados dos clientes que guardam nos seus sistemas. Esta responsabilidade diz respeito à informação que a empresa recolhe e trata, e não ao estado do dispositivo pessoal do cliente, que continua a ser responsabilidade deste. Ainda assim,

há muito que as empresas podem fazer para dificultar ataques que tenham origem do lado do utilizador, como reforçar a autenticação, sinalizar comportamentos pouco habituais ou limitar a duração das sessões. O que não podem é controlar se o cliente mantém o telemóvel atualizado, bem configurado ou utilizado com cuidado. É por isso que a aposta numa infraestrutura cibernética sólida continua a ser essencial.

Estratégias de Mitigação de Riscos:

Para mitigar os riscos de segurança no M-Commerce, as empresas devem adotar uma abordagem abrangente que inclui a criptografia de dados, a autenticação de dois fatores, a monitorização contínua de ameaças e a educação dos consumidores sobre práticas seguras. Além disso, é fundamental estar em conformidade com regulamentos de privacidade de dados, como o RGPD na União Europeia, para proteger os direitos dos consumidores.

4.6 Conceito de Risco e Método de Mosler

Na área da segurança da informação, o risco costuma ser definido como o cruzamento entre a probabilidade de um evento adverso acontecer e o impacto que esse evento pode ter sobre os ativos de uma organização ou de um utilizador (ISO 31000, 2018). Aven (2016) sublinha que avaliar o risco não se resume a identificar ameaças: é também necessário compreender as vulnerabilidades que podem facilitar a sua concretização e as consequências que daí podem resultar.

No caso do m-commerce, esta avaliação acaba por ser mais complexa, já que envolve diferentes tipos de fatores. Há, por um lado, questões tecnológicas, como as vulnerabilidades das aplicações e das redes móveis. Existem também fatores comportamentais, ligados às práticas de segurança dos utilizadores, e ainda fatores contextuais, como o nível de literacia digital. Entre as metodologias disponíveis para este tipo de análise, o Método de Mosler é uma das mais utilizadas no âmbito da segurança organizacional. Trata-se de um método de natureza mista, que assenta em seis critérios: Função, Substituição, Profundidade, Extensão, Agressão e Vulnerabilidade. Ao ponderar estes critérios, torna-se possível traduzir perceções qualitativas em valores numéricos, o que facilita a comparação entre diferentes ameaças e ajuda a definir prioridades de mitigação.

O Método de Mosler adequa-se particularmente bem a contextos onde existe elevada incerteza e uma escassez de dados quantitativos, o que se verifica precisamente no estudo da percepção de segurança no m-commerce. Uma vez que permite trabalhar com respostas qualitativas recolhidas através de inquéritos, atribuindo-lhes um peso analítico coerente, foi adotado como ferramenta central na componente empírica desta investigação.

5 Considerações finais da revisão teórica

A análise da literatura revela que o comércio eletrónico e os seus subsegmentos nomeadamente o m-commerce, o s-commerce e o dropshipping têm vindo a redefinir as dinâmicas entre empresas e consumidores. No que respeita aos resultados mais salientes, verifica-se que a personalização da experiência do utilizador, suportada por sistemas de recomendação baseados em inteligência artificial, tem contribuído para um aumento significativo do engagement e das taxas de conversão em plataformas de e-commerce. Paralelamente, modelos de negócio como o dropshipping permitem aos comerciantes uma redução substancial dos custos operacionais, ao dispensarem investimento em stock e logística, concentrando-se antes em estratégias de marketing e atendimento ao cliente. A expansão geográfica é outro resultado evidente: a eliminação de barreiras territoriais confere ao vendedor online acesso a um mercado global, ainda que este crescimento acarrete desafios logísticos acrescidos, sobretudo na “última milha” de entrega.

No contexto nacional, a adesão ao comércio eletrónico tem vindo a crescer de forma consistente, embora ainda aquém da média europeia, revelando um mercado com significativo potencial de expansão. Todavia, persistem constrangimentos, tais como a elevada iliteracia digital em certas faixas etárias, as dificuldades logísticas em regiões menos urbanizadas e a relutância em pagar portes de envio, fatores que condicionam a adoção plena e a confiança no canal digital.

No que diz respeito às percepções de segurança no m-commerce tema central do Capítulo V, os estudos apontam para receios significativos por parte dos utilizadores. A mobilidade dos dispositivos móveis eleva a exposição a ameaças como o phishing em aplicações, a interceção de dados em redes Wi-Fi públicas e a eventual violação de informações em caso de perda ou roubo do equipamento. Estes riscos influenciam diretamente o comportamento de compra: muitos consumidores optam por métodos de autenticação biométrica ou por carteiras digitais que garantam encriptação de ponta a ponta,

valorizando a transparência das comunicações de segurança (notificações push, alertas in-app) e a reputação das plataformas.

Não obstante estes ganhos, a literatura identifica várias limitações que importa considerar em profundidade. A diversidade de versões de sistemas operativos móveis e a proliferação de aplicações de origem incerta aumentam a vulnerabilidade dos utilizadores; a assimetria de literacia digital sobretudo entre gerações mais elevadas e residentes em zonas rurais condiciona a perceção de segurança e alimenta desconfianças. A escassez de estudos longitudinais que cruzem atitudes declaradas com métricas reais de fraude dificulta a avaliação objetiva da eficácia das medidas de proteção implementadas.

A partir destas lacunas, propõem-se três linhas de investigação futura que se mostrem simultaneamente pragmáticas e adaptadas à realidade portuguesa. Em primeiro lugar, um estudo comparativo da eficácia dos diferentes métodos de autenticação móvel (PIN, biometria, multifator) junto de grupos etários e geográficos distintos, avaliando não só a segurança técnica, mas também a perceção de confiança. Em segundo lugar, uma avaliação do impacto do e-commerce em zonas rurais, centrada nos custos logísticos de distribuição e no grau de literacia digital dos consumidores, de forma a fundamentar políticas públicas e incentivos para operadores regionais. Por fim, recomenda-se uma investigação aprofundada sobre o papel das redes sociais enquanto canais de retenção e fidelização de clientes e não apenas de conversão, explorando métricas de engagement, satisfação e lealdade em micro e pequenas empresas.

A adoção destas direções de investigação permitirá não só suprir lacunas identificadas na presente revisão teórica, mas também gerar insights empiricamente validados e ajustados aos rápidos desenvolvimentos tecnológicos do comércio digital em Portugal, contribuindo para uma visão mais completa e orientada para a perceção de segurança no m-commerce.

CAPÍTULO III – METODOLOGIA

6 Metodologia

Este estudo tem como objetivo e compreender a segurança da informação no contexto do mobile commerce (m-commerce), com foco na percepção dos usuários sobre os riscos associados à utilização de dispositivos móveis para transações comerciais. A metodologia foi desenvolvida para integrar uma revisão de literatura abrangente e a aplicação de questionários, de modo a recolher dados primários que sustentem a análise das práticas e percepções de segurança entre os usuários de m-commerce. A seguir, detalha-se o tipo de estudo, as fontes de dados, os critérios de inclusão e exclusão, o procedimento de recolha de dados e as técnicas de análise empregadas.

6.1 Tipologia de Estudo

O presente estudo caracteriza-se como uma pesquisa mista, composta por duas fases principais: uma revisão de literatura integrativa e uma pesquisa quantitativa descritiva. Esta abordagem mista permite uma análise aprofundada do tema, combinando a síntese de conhecimentos teóricos e empíricos existentes com a coleta e análise de dados primários. A revisão de literatura foi realizada com o objetivo de sintetizar o estado atual do conhecimento sobre a segurança da informação no m-commerce, identificando ameaças, práticas de segurança e lacunas existentes. Este tipo de revisão é particularmente adequado para integrar estudos teóricos e empíricos, oferecendo uma visão ampla e crítica do tema.

Na segunda fase, foi conduzida uma pesquisa quantitativa descritiva por meio de questionários estruturados. Esta abordagem foi escolhida para explorar a percepção e o comportamento dos consumidores em relação à segurança no m-commerce, permitindo a coleta de dados em larga escala e a análise de padrões e tendências entre os utilizadores.

6.2 Revisão de literatura

A revisão de literatura foi realizada através de uma busca sistemática em bases de dados acadêmicas renomadas, que garantem o acesso a estudos de alta qualidade e relevância para o tema investigado. Nas principais fontes utilizadas incluímos Bases de dados Acadêmicas e Relatórios de organizações.

Para assegurar a qualidade e relevância dos estudos selecionados na revisão de literatura e a adequação da amostra na pesquisa quantitativa, foram estabelecidos critérios rigorosos de inclusão e exclusão.

6.2.1 Critérios de inclusão

Apenas estudos publicados entre 2000 e 2024 foram considerados e estudos que abordam diretamente:

- Ameaças e vulnerabilidades no m-commerce: Incluindo malwares móveis, ataques de phishing, e interceptação de dados.
- Protocolos de segurança e criptografia: Análises sobre a implementação de medidas de segurança, como autenticação multifatorial e encriptação de dados.
- Impacto de legislações.

Somente estudos com metodologia clara e rigor científico foram incluídos, assegurando a validade e confiabilidade dos dados. Publicações em inglês e português foram consideradas, permitindo uma cobertura internacional sem perder de vista o contexto local.

6.2.2 Critérios de exclusão

Estudos que não focam diretamente no m-commerce ou que discutem segurança em contextos amplos de e-commerce sem especificidades para o móvel foram excluídos. Documentos como blogs, artigos de opinião e editoriais que não passaram por revisão acadêmica não foram considerados. Estudos excessivamente técnicos que não discutem as implicações práticas ou de negócios da segurança no m-commerce foram excluídos, a menos que contribuíssem para a compreensão geral dos problemas enfrentados. Artigos que apresentassem conteúdo significativamente similar a outros já incluídos foram excluídos para evitar redundância.

6.2.3 Recolha de dados

A revisão de literatura foi conduzida de forma sistemática, garantindo uma análise abrangente e crítica dos estudos existentes sobre a segurança da informação no m-commerce. Esta revisão foi realizada em várias etapas bem definidas. Em primeiro lugar, foram definidas palavras-chave abrangentes para guiar a pesquisa bibliográfica. Entre estas palavras-chave incluem-se termos como: "Segurança no mobile commerce", "Ameaças à segurança em dispositivos móveis", "E-commerce", "Proteção de dados pessoais em aplicações móveis". Estas palavras-chave foram combinadas utilizando operadores booleanos (AND, OR, NOT) com o intuito de refinar as buscas e garantir a recuperação de estudos altamente relevantes.

Posteriormente, a pesquisa foi conduzida em bases de dados previamente selecionadas. Foram aplicados filtros de data e tipo de documento para otimizar os resultados da pesquisa. Cada estudo recuperado foi inicialmente avaliado através dos seus títulos e resumos, com o objetivo de identificar aqueles que estavam alinhados com os objetivos da pesquisa. Os artigos considerados relevantes foram, então, lidos na íntegra para confirmar a sua adequação ao estudo. Foi desenvolvida uma ficha de avaliação destinada a registar informações importantes de cada estudo, como os objetivos, a metodologia e as limitações. Esta abordagem permitiu uma análise detalhada e rigorosa, essencial para fundamentar adequadamente a investigação em questão.

6.3 Pesquisa quantitativa

A pesquisa quantitativa foi realizada através de questionários estruturados aplicados a uma amostra diversificada de indivíduos. A escolha de questionários permite a recolha de dados quantificáveis sobre a percepção dos utilizadores sobre os riscos associados ao m-commerce no requisito segurança de informação.

6.3.1 Critérios de inclusão

- Participantes com idade mínima de 18 anos, garantindo a inclusão de indivíduos com capacidade legal para realizar transações online.
- Indivíduos que utilizaram dispositivos móveis para compras online ou serviços de m-commerce pelo menos uma vez nos últimos seis meses.
- Inclusão de participantes de diferentes faixas etárias, gêneros, níveis educacionais e regiões geográficas, assegurando a representatividade da amostra.

6.3.2 Critérios de exclusão

- Indivíduos que nunca utilizaram dispositivos móveis para transações comerciais foram excluídos, pois não contribuiriam para a análise do comportamento e percepção de utilizadores.
- Respostas incompletas ou incoerentes serão excluídas para garantir a integridade dos dados para análise.

6.3.3 Recolha de dados

A pesquisa quantitativa foi conduzida através da aplicação de questionários estruturados, Google Forms, seguindo um procedimento bem definido. Em primeiro lugar, o

questionário foi elaborado com base numa revisão da literatura existente e nos objetivos específicos da pesquisa. As questões foram desenhadas para abordar três áreas principais: a consciencialização sobre segurança, os comportamentos de segurança e a perceção de risco. Na secção de consciencialização sobre segurança, as perguntas visavam avaliar o nível de conhecimento dos utilizadores sobre as ameaças à segurança. Na parte dedicada aos comportamentos de segurança, as questões procuravam identificar as práticas de segurança adotadas pelos utilizadores ao utilizarem dispositivos móveis para transações online. Por último, a secção de perceção de risco incluía perguntas destinadas a medir como os utilizadores percecionam os riscos associados ao uso de dispositivos móveis para compras online. O questionário foi submetido a uma revisão e validação por parte de especialistas em segurança da informação e metodologias de pesquisa, de modo a garantir a sua clareza e relevância.

Relativamente à amostragem, será uma amostragem por conveniência. Os participantes serão selecionados com base na sua disponibilidade e vontade de participar no estudo. A amostra será composta por indivíduos de diversas idades, géneros, níveis educacionais e experiências com m-commerce, assegurando assim uma representação diversificada. O questionário será distribuído por meio de plataformas online, como partilha de link do Formulário Google através de e-mails e redes sociais maioritariamente. Esta abordagem facilitará a participação dos inquiridos e permitira a recolha de dados em larga escala. A recolha de dados decorrerá durante um período de 2 meses. As respostas obtidas serão armazenadas de forma segura.

7 Contextualização do questionário

O questionário desenvolvido aborda questões que se relacionam diretamente com três eixos principais identificados na revisão de literatura. Em primeiro lugar, o crescimento e benefícios do m-commerce, que, como apontado por Carvalho et al. (2023), tem vindo a ser impulsionado pela crescente utilização dos dispositivos móveis, oferecendo aos consumidores uma forma prática e acessível de realizar compras. Este crescimento, no entanto, vem acompanhado de uma maior exposição a riscos, pelo que se faz necessário avaliar de que forma os utilizadores lidam com esses riscos. Em segundo lugar, a preocupação com a segurança e a proteção de dados pessoais, uma questão central no m-commerce, conforme sublinhado por Kashyap e Chaudhary (2023), que indicam que a segurança dos dados pessoais é uma das maiores preocupações dos consumidores. Por

fim, o papel da confiança na adoção de novas tecnologias, que, de acordo com Laudon & Traver (2007), é um fator determinante para a adesão ao m-commerce, dado que a confiança do consumidor é diretamente afetada pela percepção de riscos associados à utilização de plataformas digitais. Neste contexto, o questionário desenvolvido pretende identificar não só as ameaças de segurança mais comuns percebidas pelos utilizadores, como o phishing, o malware móvel e a fraude em transações, mas também explorar como essas preocupações influenciam as práticas de segurança adotadas pelos consumidores. Através das respostas, é possível também compreender a percepção de risco dos utilizadores, ou seja, como eles avaliam o nível de segurança das transações realizadas em dispositivos móveis e o impacto de experiências negativas. Foi selecionado o Método Mosler para estruturar a análise dos dados, uma vez que possibilita identificar os riscos e classificar esses riscos com recurso a critérios bem definidos.

8 Análise e discussão dos resultados

O presente capítulo apresenta a análise e interpretação dos dados obtidos a partir do questionário aplicado, com o objetivo de compreender as percepções e comportamentos dos utilizadores relativamente à segurança da informação no m-commerce. A análise procura identificar padrões de resposta, relações entre variáveis e níveis de risco associados às práticas de utilização de dispositivos móveis em contextos de compra digital. Inicialmente, são descritas as características gerais da amostra e as tendências observadas nas respostas. Seguidamente, procede-se à aplicação do Método de Mosler, que permite mensurar e classificar os riscos de acordo com critérios específicos, transformando percepções subjetivas em indicadores quantitativos de vulnerabilidade.

A abordagem possibilita uma leitura mais rigorosa e comparativa dos resultados, permitindo compreender de que forma fatores como o nível de literacia digital, as práticas de segurança e a percepção de confiança influenciam o comportamento dos utilizadores no contexto do comércio eletrónico móvel.

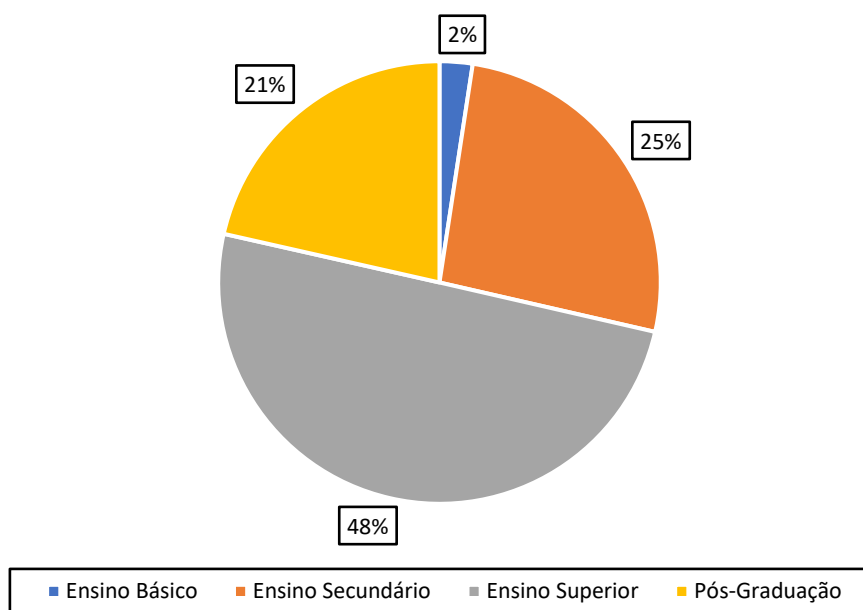
8.1 Caracterização da amostra

Amostra deste estudo é constituída por 44 inquiridos, de forma a fazer uma caracterização mais geral da amostra serão apresentados e analisados os resultados obtidos através das respostas ao questionário.

A caracterização demográfica desta amostra (Tabela 1), 59% dos inquiridos foram do sexo masculino e aproximadamente metade da amostra (45,5%) situava-se entre os 18-34 anos. Relativamente ao nível de escolaridade, obtivemos que 25% dos inquiridos teria apenas concluído o ensino secundário, enquanto que 47,7% dos inquiridos teria o grau correspondente ao ensino superior e 20,5% apresentava pelo menos uma pós-graduação.

	Número de Inquiridos (n=44)	Percentagem de Inquiridos (%)
Idade		
18-34 anos	20	45,5
35-44 anos	10	22,7
45-54 anos	8	18,2
55-64 anos	5	11,4
≥65 anos	1	2,3
Género		
Masculino	26	59
Feminino	16	36,4
Não divulgado	2	4,6
Nível de Escolaridade		
Ensino Básico	1	2,3
Ensino Secundário	11	25
Ensino Superior	21	47,7
Pós-Graduação	9	20,5

Tabela 1 - Caracterização demográfica da amostra de inquiridos



8.2 Análise dos dados

Foi questionado a todos os participantes, qual o seu conhecimento acerca dos tipos de ameaça, segundo a análise da Tabela 2 relacionando com os dados obtidos no inquérito, face ao conhecimento sobre os diferentes tipos de ameaças no m-commerce (Tabela 2), obtivemos que o roubo de identidade foi a modalidade mais conhecida entre a nossa amostra, com 81,8% dos inquiridos a responder positivamente. Contrariamente, a interceção de dados foi a modalidade com menor percentagem de conhecimento (56,8%).

	Número de Inquiridos (n=44)	Percentagem de Inquiridos (%)
Tipo de Ameaça		
Malware Móvel		
Com conhecimento	32	72,7
Sem conhecimento	12	27,3
Phishing		
Com conhecimento	34	77,3
Sem conhecimento	10	22,7
Interseção de Dados		
Com conhecimento	25	56,8
Sem conhecimento	19	43,2
Fraude em Transações		
Com conhecimento	32	72,7
Sem conhecimento	12	27,3
Roubo de Identidade		
Com conhecimento	36	81,8
Sem conhecimento	8	18,2
Práticas de Segurança		
Conhecimento muito alto	1	2,3
Conhecimento alto	8	18,2
Conhecimento médio	23	52,3
Conhecimento baixo	9	20,5
Conhecimento muito baixo	3	6,8

Tabela 2 Conhecimento dos inquiridos sobre ameaças digitais e práticas de segurança no m-commerce

No que diz respeito às práticas de segurança, obtivemos que aproximadamente metade da nossa amostra (52,3%) considera que apresenta um conhecimento médio sobre estas, enquanto que 27,3% dos inquiridos referem que apresentam um conhecimento baixo ou muito baixo.

Nas práticas preventivas de segurança (Tabela 3), constatamos que uma grande parte dos nossos inquiridos raramente revê a política de privacidade dos sites onde realiza compras (34,1%), contrastando com a pequena percentagem de inquiridos que frequentemente revê estas políticas (13,6%). Relativamente à utilização de palavras passe, observamos

que a maioria dos inquiridos nunca ou muito raramente as atualiza (61,4%). Além disso, quando questionados sobre a utilização de diferentes palavras-passe em diferentes lojas online, apenas 22,7% dos inquiridos responderam que o faziam sempre, e 27,3% dos inquiridos responderam que o faziam frequentemente. Quanto aos métodos de armazenamento de palavras-passe, obtivemos resultados variados, sendo que a preferência dos nossos inquiridos foi armazenamento em aplicação de gestão de palavras-passe (36,4%) e armazenamento no dispositivo (27,3%).

Quando questionados com questões acerca da uma experiencia negativas num serviço e quais as suas consequencias, a probabilidade de abandonar um site na ausência de certificado de segurança, cerca de 47,7% dos inquiridos respondeu que apresentava uma probabilidade muito alta. Em relação à confiança no serviço online após uma experiência negativa de segurança, 43,2% dos nossos inquiridos responderam que isso reduziria significativamente a confiança nesse mesmo serviço.

	Número de Inquiridos (n=44)	Percentagem de Inquiridos (%)
Leitura da Política de Privacidade		
Sempre	2	4,5
Frequentemente	6	13,6
Ocasionalmente	12	27,3
Raramente	15	34,1
Nunca	9	20,5
Atualização de Palavras-Passe		
Mensalmente	1	2,3
A cada 3 meses	4	9,1
A cada 6 meses	5	11,4
Anualmente	7	15,9
Nunca/Muito raramente	27	61,4
Utilização de diferentes Palavras-Passe		
Sempre	10	22,7
Frequentemente	12	27,3
Ocasionalmente	9	20,5
Raramente	9	20,5
Nunca	4	9,1
Métodos de Armazenamento de Palavras-Passe		
Anotação em agenda	1	2,3
Aplicação de gestão de palavras-passe	16	36,4
Armazenamento no dispositivo	12	27,3
Memorização	5	11,2
Anotação em local físico (ex: papel)	9	20,5
Aplicação de gestão de palavras-passe + memorização	1	2,3
Probabilidade de abandonar um site na ausência de Certificado de Segurança		

Muito alta	21	47,7
Alta	13	29,5
Moderada	5	11,4
Baixa	2	2,5
Muito baixa	3	6,8
Confiança no serviço online após uma experiência negativa de segurança		
Perderia totalmente a confiança	15	34,1
Reduziria significativamente a confiança	19	43,2
Reduziria um pouco a confiança	6	13,6
Não afetaria muito a confiança	4	9,1

Tabela 3 Práticas preventivas de segurança dos inquiridos no contexto do m-commerce

Relativamente à percepção de segurança do utilizador comum face ao uso de dispositivos móveis (Tabela 4), constatamos que 38,6% dos inquiridos considera seguro realizar transações em dispositivos móveis, enquanto que 13,6% considera-o inseguro. Quando questionados sobre qual consideravam ser o maior risco associado ao uso destes dispositivos, a opção mais escolhida foi a “perda de dinheiro em transações fraudulentas” (29,5%). Ainda, verificamos que cerca de 31,8% dos inquiridos considerou que as aplicações móveis são mais seguras face aos websites em navegador, contrastando com os 6,8% que consideraram o oposto.

	Número de Inquiridos (n=44)	Percentagem de Inquiridos (%)
Nível de segurança em transações em dispositivos móveis		
Muito seguro	1	2,3
Seguro	17	38,6
Neutro	18	40,9
Inseguro	6	13,6
Muito inseguro	2	4,5
Percepção do maior risco associado ao uso de dispositivos móveis		
Downloads de Malware	2	4,5
Perda de dinheiro em transações fraudulentas	13	29,5
Roubo de informações pessoais	8	20,5
Uso indevido dos saldos do cartão de crédito	20	25,5
Percepção de segurança das aplicações móveis face aos websites no navegador		
As aplicações móveis são mais seguras	14	31,8
Os websites no navegador são mais seguros	3	6,8
Ambas igualmente seguras	13	29,5
Nenhuma é segura	4	9,1
Sem opinião	10	22,7

Tabela 4 Percepção de segurança dos inquiridos relativamente ao uso de dispositivos móveis no m-commerce

Dentro da nossa amostra, obtivemos que 27,3% dos inquiridos realiza compras online em dispositivos móveis semanalmente, e a mesma percentagem mensalmente. Apenas 9,1% da amostra refere raramente realizar este tipo de compras online. Os principais motivos para a realização de compras online num dispositivo móvel prendem-se com a conveniência em 45,5% dos casos e com a rapidez em 40,9% dos casos, como se pode verificar na Tabela 5.

	<i>Número de Inquiridos (n=44)</i>	<i>Percentagem de Inquiridos (%)</i>
Frequência de realização de compras		
Compras online em dispositivo móvel		
Diariamente	3	6,8
Semanalmente	12	27,3
Mensalmente	12	27,3
Ocasionalmente	13	29,5
Raramente	4	9,1
Principais motivos para realizar compras online num dispositivo móvel		
Conveniência	20	45,5
Rapidez	18	40,9
Conveniência e rapidez	1	2,3
Promoções e descontos exclusivos	13	9,1
Conveniência e rapidez fora da residência	1	2,3

Tabela 5 Frequência e principais motivos para a realização de compras online em dispositivos móveis

8.3 Testes

Quando comparadas as diferentes variáveis face ao nível de escolaridade (Comparação de diferentes variáveis face à escolaridade), obtiveram-se resultados estatisticamente significativos para conhecimento sobre ameaças no m-commerce ($p=0,000$), conhecimento sobre práticas de segurança no m-commerce ($p=0,009$), leitura da política de privacidade ($p=0,028$) e perceção de segurança das aplicações móveis face aos websites ($p=0,000$). Portanto, verificou-se que os inquiridos com menor nível de escolaridade apresentaram tendencialmente menor conhecimento sobre ameaças no m-commerce. Por sua vez, aqueles que apresentavam níveis de escolaridade mais elevados, apresentaram níveis mais elevados de conhecimento sobre práticas de segurança no m-commerce. Adicionalmente, também é possível verificar que os inquiridos mais instruídos academicamente apresentaram frequências de revisão da política de privacidade mais elevadas. Finalmente, verificamos que pessoas que consideram as

aplicações móveis inseguras ou muito inseguras face aos websites em navegador apresentam menor grau de escolaridade. Para os restantes parâmetros listados na Tabela 6 não se verificaram diferenças estatisticamente significativas entre grupos. De forma global, estes resultados permitem concluir que a escolaridade e a idade se assumem como variáveis determinantes no nível de literacia digital em segurança no m-commerce. A escolaridade revelou estar diretamente associada não apenas ao grau de conhecimento sobre ameaças e práticas de segurança, mas também à maior consciência crítica, refletida na leitura mais frequente das políticas de privacidade e numa perceção de risco mais ajustada. Por outro lado, a idade demonstrou impacto sobretudo no conhecimento sobre práticas de segurança, revelando um desfasamento geracional: os participantes mais jovens apresentam, em média, níveis de conhecimento mais consistentes, enquanto os mais velhos evidenciam fragilidades neste campo. Importa ainda salientar que, relativamente a práticas concretas de segurança como a atualização periódica das palavras-passe ou a utilização de combinações diferenciadas não se observaram diferenças estatisticamente significativas entre os grupos. Tal sugere que, independentemente da idade ou escolaridade, os comportamentos efetivos de gestão de passwords permanecem relativamente homogéneos, contrastando com as diferenças verificadas ao nível da perceção e do conhecimento.

	<i>Ensino Básico</i> (n=1)	<i>Ensino Secundário</i> (n=11)	<i>Ensino Superior</i> (n=21)	<i>Mestrado</i> (n=2)	<i>Pós-Graduação</i> (n=9)	<i>p^a</i>
Conhecimento sobre Ameaças no m-commerce						0,000 b
<i>Conhecimento de ≥1</i>	0	10	21	2	9	
<i>Sem conhecimento</i>	1	1	0	0	0	
Conhecimento sobre práticas de Segurança no m-commerce						0,009 b
<i>Muito alto</i>	0	1	3	0	4	
<i>Alto</i>	0	5	2	1	1	
<i>Médio</i>	0	3	15	1	4	
<i>Baixo</i>	0	0	1	0	0	
<i>Muito baixo</i>	1	2	0	0	0	
Leitura da Política de Privacidade						0,028 b
<i>Sempre</i>	0	0	1	1	4	
<i>Frequentemente</i>	0	5	2	0	1	
<i>Ocasionalmente</i>	0	1	9	0	2	
<i>Raramente</i>	0	4	9	1	1	
<i>Nunca</i>	1	1	0	0	1	
Atualização de Palavras-Passe						0,455 b

<i>Mensalmente</i>	0	0	1	0	3
<i>A cada 3 meses</i>	0	0	4	0	1
<i>A cada 6 meses</i>	0	2	3	1	1
<i>Anualmente</i>	0	1	0	0	0
<i>Nunca/Muito raramente</i>	1	8	13	1	4
Utilização de diferentes Palavras-Passe					0,353 b
<i>Sempre</i>	0	1	7	1	3
<i>Frequentemente</i>	0	3	1	0	0
<i>Ocasionalmente</i>	1	3	5	0	0
<i>Raramente</i>	0	2	4	1	2
<i>Nunca</i>	0	2	4	0	4
Confiança no serviço online após uma experiência negativa de segurança					0,483 b
<i>Perderia totalmente a confiança</i>	1	7	5	1	1
<i>Reduziria significativamente e a confiança</i>	1	3	9	1	6

Tabela 6 Resultados da comparação das variáveis de segurança digital segundo o nível de escolaridade e idade dos inquiridos

9 Aplicação do Método Mosler à análise de risco no M-commerce

Após a análise estatística descritiva e inferencial dos dados recolhidos através dos questionários, procedeu-se à mensuração do risco com base no Método Mosler, de modo a avaliar a probabilidade e o impacto dos principais riscos associados à segurança da informação no m-commerce. Esta etapa permitiu transformar as percepções recolhidas

junto dos utilizadores em indicadores quantitativos e comparáveis, capazes de apoiar decisões estratégicas de mitigação de riscos tanto para empresas como para utilizadores finais.

O Método Mosler é amplamente reconhecido na área da gestão de segurança organizacional, sendo utilizado para avaliar e priorizar riscos com base em dois parâmetros fundamentais: impacto e probabilidade. No contexto desta investigação, a sua aplicação assume especial relevância, uma vez que o estudo tem natureza exploratória e descritiva, enquadrando-se metodologicamente nas recomendações de utilização deste método em ambientes caracterizados por elevada incerteza e baixa disponibilidade de dados quantitativos. Assim, a adoção do Método Mosler justifica-se pela sua capacidade de converter perceções subjetivas em resultados mensuráveis, permitindo uma leitura objetiva do risco a partir de respostas qualitativas obtidas nos questionários.

Importa sublinhar que o ineditismo da aplicação do Método Mosler neste trabalho não reside na criação de uma nova ferramenta, mas na forma como este é recontextualizado e adaptado ao estudo da segurança da informação no m-commerce — um domínio onde as análises de risco ainda são incipientes ou frequentemente limitadas a abordagens puramente estatísticas. Deste modo, a dissertação não apenas aplica uma metodologia consolidada, mas amplia a sua utilidade ao introduzir uma perspetiva comportamental e percecional dos utilizadores, contribuindo com novo conhecimento para a área.

9.1 Etapas para aplicação do Método Mosler

A aplicação prática do Método de Mosler foi operacionalizada através de uma folha de cálculo em Microsoft Excel, estruturada em duas fases principais, “Tratamento de Dados” e “Evolução do Risco”. Este processo permitiu quantificar e comparar o nível de exposição a diferentes categorias de risco associadas ao uso do m-commerce, com base nas perceções recolhidas junto dos participantes do inquérito.

1. Preenchimento e Mensuração Inicial dos Critérios

Numa primeira etapa, cada risco identificado a partir das respostas ao questionário foi avaliado individualmente segundo os seis critérios fundamentais definidos por Mosler:

- Função (F) – avalia o impacto do risco sobre as atividades essenciais ou recursos críticos do sistema;

- Substituição (S) – mede a dificuldade ou impossibilidade de substituição dos ativos afetados;
- Profundidade (P) – avalia a extensão das consequências internas e reputacionais resultantes do evento;
- Extensão (E) – mede o alcance dos danos sobre outros processos, utilizadores ou stakeholders;
- Agressão (A) – estima a probabilidade de ocorrência ou intensidade do ataque;
- Vulnerabilidade (V) – avalia o grau de exposição e o impacto económico e operacional decorrente do risco.

Cada critério foi pontuado numa escala de 1 (mínimo) a 5 (máximo), de acordo com a percepção associada. As pontuações resultantes foram introduzidas na folha de cálculo, permitindo criar uma base de dados estruturada para a análise quantitativa subsequente.

2. Cálculo e Classificação dos Riscos

Numa segunda fase, os valores inseridos foram processados para calcular a Evolução do Risco (ER), que integra a importância do ativo, o dano potencial e a probabilidade de ocorrência. Foram aplicadas as seguintes fórmulas propostas por Mosler:

- Magnitude do Risco (C) = Importância do Sucesso (I) + Danos Causados (D)
- Probabilidade de Ocorrência (Pb) = Agressão × Vulnerabilidade
- Evolução do Risco (ER) = C × Pb

O valor final de ER reflete o nível de criticidade de cada risco identificado, permitindo classificá-lo de forma hierarquizada.

Para uniformizar essa classificação, foi definida a escala apresentada na Tabela 7 (Classificação e Interpretação dos Níveis de Risco).

Intervalo ER	Nível de Risco	Interpretação
$ER \leq 10$	Muito Baixo	Riscos Residuais
$10 < ER \leq 50$	Baixo	Riscos de impacto limitado e facilmente mitigáveis
$50 < ER \leq 200$	Moderado	Riscos controláveis e de baixa probabilidade
$200 < ER \leq 600$	Elevado	Riscos com potencial de dano relevante e alargado
$ER > 600$	Muito Elevado	Riscos severos com impacto direto e imediato

Tabela 7 Classificação e Interpretação dos Níveis de Risco

9.2 Análise de risco de variáveis

9.2.1 Práticas de segurança

A variável Práticas de Segurança avalia o grau de conhecimento que os utilizadores afirmam possuir sobre comportamentos e medidas de proteção aplicáveis ao contexto do m-commerce. Este conhecimento compreende noções relativas a segurança de dados, identificação de riscos, utilização de redes seguras, gestão de palavras-passe e reconhecimento de situações de potencial fraude digital. Assim, quanto menor o nível de conhecimento reportado, maior é o risco de exposição e de vulnerabilidade durante a utilização de plataformas de comércio móvel. As pontuações atribuídas a cada critério do Método de Mosler para esta variável estão apresentadas na Tabela 8.

Cálculo Riscos Práticas de segurança					
Frequencia	I = F×S	D = P×E	C = I+D	PB = A×V	ER = C×PB
Conhecimento muito alto	1	1	2	1	2
Conhecimento alto	4	2	6	4	24
Conhecimento médio	9	6	15	9	135
Conhecimento baixo	16	12	28	16	448
Conhecimento muito baixo	25	20	45	25	1125

Tabela 8 Cálculo dos níveis de risco associados às Práticas de Segurança

Práticas de Segurança	Respostas	Percentual	Nota de 1 a 5 sera atribuída a partir da mensuração dos seis critérios
-----------------------	-----------	------------	--

			F	S	P	E	A	V
Conhecimento muito alto	1	2,3	1	1	1	1	1	1
Conhecimento alto	8	18,2	2	2	2	1	2	2
Conhecimento médio	23	52,3	3	3	3	2	3	3
Conhecimento baixo	9	20,5	4	4	4	3	4	4
Conhecimento muito baixo	3	6,8	5	5	5	4	5	5

Os resultados acima, na tabela, evidenciam uma relação inversa entre o nível de conhecimento e o risco de segurança. De acordo com a escala de classificação apresentada na Tabela Classificação e Interpretação dos Níveis de Risco (ponto 9.4.1), observa-se que o perfil de conhecimento muito alto apresenta um risco residual (ER=2), enquanto o conhecimento alto corresponde a risco muito baixo (ER=24).

O conhecimento médio enquadra-se no nível de risco moderado (ER=135), ao passo que os perfis de conhecimento baixo e muito baixo se situam nos patamares de risco elevado (ER=448) e crítico (ER=1125), respetivamente.

Esta distribuição evidencia uma relação inversa entre o nível de literacia em segurança e o grau de exposição ao risco, confirmando que utilizadores com menor domínio de práticas seguras se encontram significativamente mais vulneráveis no contexto do m-commerce.

9.2.2 Literatura da política de privacidade

A variável Leitura da Política de Privacidade avalia um comportamento de natureza preventiva, relacionado com o grau de atenção e consciência que o utilizador dedica à proteção dos seus dados pessoais durante o uso de plataformas de m-commerce. A leitura prévia das políticas de privacidade constitui uma prática essencial para a compreensão das permissões concedidas, dos dados recolhidos e das condições de partilha com terceiros. Assim, quanto menor for a frequência dessa leitura, maior se torna o risco associado, uma vez que o utilizador revela menor literacia digital e maior vulnerabilidade a ameaças relacionadas com a segurança da informação. A Tabela 9 apresenta a pontuação atribuída a cada critério do Método de Mosler para esta variável.

Leitura da Política de Privacidade	Respostas	Percentual	Nota atribuída a partir da mensuração dos seis critérios...de 1 a 5 será a nota					
			F	S	P	E	A	V
Sempre	2	4,5	1	1	1	1	1	1
Frequentemente	6	13,6	2	2	2	1	2	2
Ocasionalmente	12	27,3	3	3	3	2	3	3

Raramente	15	34,1	4	4	4	3	4	4
Nunca	9	20,5	5	5	5	4	5	5

Os resultados obtidos demonstram uma progressão linear do risco à medida que diminui a frequência de leitura das políticas de privacidade. O valor de ER = 2 no perfil “Sempre” representa um risco residual, enquanto os perfis “Raramente” (ER = 448) e “Nunca” (ER

Tabela 9 Atribuição das pontuações dos critérios do Método Mosler para a variável Política de Privacidade

= 1125) atingem níveis de risco elevados e muito elevados, respetivamente. Este comportamento traduz uma clara vulnerabilidade do utilizador que tende a aceitar condições de uso sem a devida leitura ou compreensão das implicações legais e de segurança. De forma a obter uma visão global, foi ainda calculado o ER ponderado, de acordo com o peso percentual de cada grupo de respondentes, resultando num valor médio de 423,6, o que classifica esta variável globalmente como risco elevado.

Os resultados obtidos demonstram uma progressão linear do risco à medida que diminui a frequência de leitura das políticas de privacidade. O valor de ER = 2 no perfil “Sempre” representa um risco residual, enquanto os perfis “Raramente” (ER = 448) e “Nunca” (ER = 1125) atingem níveis de risco elevados e muito elevados, respetivamente. Este comportamento traduz uma clara vulnerabilidade do utilizador que tende a aceitar condições de uso sem a devida leitura ou compreensão das implicações legais e de segurança. De forma a obter uma visão global, foi ainda calculado o ER ponderado, de acordo com o peso percentual de cada grupo de respondentes, resultando num valor médio de 423,6, o que classifica esta variável globalmente como risco elevado.

A predominância dos perfis “Raramente” e “Nunca” entre os inquiridos reforça a necessidade de intervenção educativa e formativa, tanto ao nível empresarial como individual, no sentido de promover uma cultura digital mais informada e responsável. A Tabela 10 apresenta os níveis de risco calculados para esta variável.

Para concluir, análise demonstra que a maioria dos utilizadores adota uma postura de baixa vigilância relativamente à proteção dos seus dados pessoais. Tal comportamento, ainda que comum, potencia a exposição a ataques de phishing, acessos não autorizados e utilização indevida de dados por entidades terceiras. Verifica-se, assim, que a literacia digital e a perceção de risco estão intrinsecamente associadas à atenção dispensada às políticas de privacidade, sendo esta uma das dimensões mais críticas na prevenção de incidentes de segurança.

Cálculo do Risco - Leitura da Política de Privacidade					
Frequencia	I = F×S	D = P×E	C = I+D	PB = A×V	ER = C×PB
Sempre	1	1	2	1	2
Frequentemente	4	2	6	4	24
Ocasionalmente	9	6	15	9	135
Raramente	16	12	28	16	448
Nunca	25	20	45	25	1125

Tabela 10 Cálculo dos níveis de risco associados à Leitura da Política de Privacidade

9.2.3 Atualização da palavra-chave

A variável Atualização da Palavra-Passe mede o comportamento preventivo dos utilizadores relativamente à renovação periódica das credenciais de acesso às plataformas de m-commerce. Esta prática constitui uma das medidas fundamentais de segurança, uma vez que a substituição regular de palavras-passe reduz significativamente o risco de intrusão, roubo de dados e utilização indevida de contas pessoais. As pontuações atribuídas a cada critério do Método de Mosler para esta variável podem ser consultadas na Tabela 11.

Atualização da Palavra Chave	Respostas	Percentual	Nota de 1 a 5 sera atribuída a partir da mensuração dos seis critérios					
			F	S	P	E	A	V
Mensalmente	1	2,3	1	1	1	1	1	1
A cada 3 meses	4	9,1	2	2	2	2	1	2
A cada 6 meses	5	11,4	3	3	3	2	3	3
Atualmente	7	15,9	4	4	4	3	4	4
Nunca/Muito raramente	27	61,4	5	5	5	4	5	5

Tabela 11 Atribuição das pontuações dos critérios do Método Mosler para a variável Atualização da Palavra Chave

Os resultados demonstram uma correlação inversa entre a frequência de atualização das palavras-passe e o risco de segurança. Os utilizadores que atualizam as suas credenciais mensalmente ou trimestralmente apresentam níveis de risco muito baixos (ER = 2 a 16), enquanto aqueles que nunca ou raramente o fazem revelam risco extremo (ER = 1125).

A distribuição dos inquiridos evidencia uma concentração expressiva nas categorias de maior risco, o que reforça a necessidade de campanhas educativas sobre a importância da renovação periódica das credenciais e da adoção de boas práticas, como o uso de autenticação multifator.

O comportamento predominante de desatualização das senhas sugere uma falsa percepção de segurança: muitos utilizadores consideram que a ausência de incidentes passados equivale à inexistência de risco, ignorando a exposição prolongada que credenciais

antigas representam. De acordo com esta escala na tabela Classificação e Interpretação dos Níveis de Risco (Ponto 9.4.1), a maioria dos utilizadores inquiridos insere-se nas categorias “Elevado” e “Muito Elevado”, demonstrando a urgência de medidas pedagógicas e tecnológicas para mitigar este fator de vulnerabilidade. Os valores calculados para cada perfil de utilizador encontram-se na Tabela 12.

Cálculo Riscos Atualização Palavra Chave					
Frequencia	I = F×S	D = P×E	C = I+D	PB = A×V	ER = C×PB
Mensalmente	1	1	2	1	2
A cada 3 meses	4	4	8	2	16
A cada 6 meses	9	6	15	9	135
Atualmente	16	12	28	16	448
Nunca/Muito raramente	25	20	45	25	1125

Tabela 12 Cálculo dos níveis de risco associados a Riscos Atualização palavra chave

9.2.4 Percepção do maior risco associado ao uso de dispositivos móveis

A variável Percepção do Maior Risco Associado ao Uso de Dispositivos Móveis visa compreender quais as ameaças que os utilizadores consideram mais relevantes quando utilizam dispositivos móveis. A percepção de risco é um fator determinante na adoção de comportamentos seguros.

Os resultados obtidos no questionário indicam que a principal preocupação dos inquiridos é a perda de dinheiro em transações fraudulentas (29,5%), seguida do uso indevido dos saldos do cartão de crédito (25,5%) e do roubo de informações pessoais (20,5%). Apenas 4,5% mencionaram os downloads de malware como risco principal. Estes dados revelam que os utilizadores associam a segurança no m-commerce sobretudo a aspetos financeiros e menos a fatores técnicos de cibersegurança, demonstrando uma percepção prática e

orientada para o impacto imediato. A pontuação atribuída a cada risco identificado, segundo os critérios do Método de Mosler, está apresentada na Tabela 13.

Percepção do maior risco associado ao uso de dispositivos móveis	Respostas	Percentual	Nota de 1 a 5 será atribuída a partir da mensuração dos seis critérios					
			F	S	P	E	A	V
Downloads de Malwaree	2	2,3	2	2	2	1	2	2
Perda de dinheiro em transações fraudulentas	13	9,1	5	5	5	4	5	5
Roubo de informações pessoais	8	11,4	4	4	4	3	4	4
Uso indevido dos saldos do cartão de crédito	20	15,9	5	4	5	4	5	5

Tabela 13 Atribuição das pontuações dos critérios do Método Mosler para a variável Percepção do maior risco associado ao uso de dispositivos móveis

A análise dos resultados demonstra uma clara hierarquização da percepção de risco entre os inquiridos.

Os valores mais elevados de Evolução do Risco (ER) foram registados nas categorias “Perda de dinheiro em transações fraudulentas” (ER=1125) e “Uso indevido dos saldos do cartão de crédito” (ER=1000), o que confirma a predominância da preocupação financeira como principal fonte de insegurança no m-commerce.

O “Roubo de informações pessoais” apresenta um risco moderado (ER=448), refletindo uma consciência parcial sobre o impacto da violação de dados pessoais, mas ainda abaixo da percepção associada à perda de capital. Por outro lado, o “Download de malware” obteve o menor nível de risco (ER=24), o que indica uma baixa percepção de ameaça técnica entre os utilizadores. Os valores calculados para cada categoria de risco podem ser consultados na Tabela 14.

Cálculo Riscos Percepção do maior risco associado ao uso de dispositivos móveis					
Frequência	I = F×S	D = P×E	C = I+D	PB = A×V	ER = C×PB
Downloads de Malwaree	4	2	6	4	24
Perda de dinheiro em transações fraudulentas	25	20	45	25	1125
Roubo de informações pessoais	16	12	28	16	448
Uso indevido dos saldos do cartão de crédito	20	20	40	25	1000

Tabela 14 Cálculo dos níveis de risco associados a Percepção do maior risco associado ao uso de dispositivos móveis

Este padrão sugere que a maioria dos utilizadores possui uma percepção reativa e não preventiva: só reconhecem como grave o risco que tem consequências financeiras diretas

e imediatas, desvalorizando vulnerabilidades técnicas que podem ser a origem de ataques mais complexos.

9.2.5 Percepção de segurança das aplicações móveis face aos websites no navegador

Os dados indicam que 31,8 % dos inquiridos consideram que as aplicações móveis são mais seguras do que os websites no navegador, enquanto 29,5 % acreditam que ambos são igualmente seguros. Apenas 6,8 % dos participantes atribuem maior segurança aos websites, e 9,1 % afirmam que nenhuma das opções é segura, sendo ainda 22,7 % os que não têm opinião definida.

Estes resultados revelam uma percepção mista, mas com tendência para uma maior confiança nas aplicações móveis, provavelmente associada à sensação de controlo e à familiaridade com interfaces próprias de bancos, retalho ou serviços digitais. A pontuação atribuída a cada critério do Método de Mosler para esta variável encontra-se na Tabela 15.

Percepção da segurança das aplicações em dispositivos móveis face aos websites no navegador	Respostas	Percentual	Nota de 1 a 5 sera atribuída a partir da mensuração dos seis critérios					
			F	S	P	E	A	V
As aplicações móveis são mais seguras	14	31,8	1	1	1	1	1	1
Os websites no navegador são mais seguros	3	6,8	2	2	2	2	2	2
Ambas igualmente seguras	13	29,5	3	3	3	3	3	3
Nenhuma é segura	4	9,1	5	5	5	4	5	5
Sem opinião	10	22,7	4	4	4	3	4	4

Tabela 15 Atribuição das pontuações dos critérios do Método Mosler para a variável Percepção da segurança das aplicações em dispositivos móveis face aos websites no navegador

Análise evidencia uma tendência inversa entre confiança e risco percebido: à medida que aumenta a sensação de segurança, o valor de Evolução do Risco (ER) diminui significativamente. A Tabela 16 consolida os valores calculados para esta variável.

Percepção de segurança das aplicações móveis face aos websites no navegador					
Frequencia	I = F×S	D = P×E	C = I+D	PB = A×V	ER = C×PB
As aplicações móveis são mais seguras	1	1	2	1	2
Os websites no navegador são mais seguros	4	4	8	4	32
Ambas igualmente seguras	9	9	18	9	162
Nenhuma é segura	25	20	45	25	1125
Sem opinião	16	12	28	16	448

Tabela 16 Cálculo dos níveis de risco associados a Percepção de segurança das aplicações em dispositivos móveis face aos websites no navegador

Os utilizadores que confiam nas aplicações móveis apresentam risco residual ($ER = 2$), enquanto os que não reconhecem segurança em nenhuma das opções demonstram risco crítico ($ER = 1125$), refletindo um nível elevado de incerteza e percepção de vulnerabilidade. De forma intermédia, os que não possuem uma opinião definida apresentam risco elevado ($ER = 448$), sugerindo que a indefinição ou ausência de percepção de risco constitui, por si só, um fator de vulnerabilidade comportamental

Em síntese, esta variável confirma que a percepção subjetiva de segurança influencia diretamente a exposição ao risco no contexto do m-commerce. A confiança nas aplicações móveis está associada a menor vulnerabilidade percebida, enquanto a indefinição ou desconfiança total potencia a exposição a ameaças reais, reforçando a importância de estratégias de sensibilização e educação digital que aproximem a percepção do utilizador da realidade técnica da segurança online.

9.3 Considerações finais da análise de risco

A aplicação do Método de Mosler neste estudo permitiu transformar percepções subjetivas de segurança digital em indicadores quantitativos de risco, proporcionando uma leitura mais sistemática da forma como os utilizadores compreendem e gerem a segurança no contexto do m-commerce. As quatro variáveis analisadas, Leitura da Política de Privacidade, Práticas de Segurança, Atualização da Palavra-Passe e Percepção de Segurança das Aplicações Móveis face aos Websites, estas foram selecionadas por representarem dimensões complementares da literacia digital e comportamental, capazes de refletir tanto o grau de conhecimento como a atitude preventiva dos indivíduos perante potenciais ameaças.

Os resultados obtidos demonstram que a percepção de segurança e o comportamento do utilizador estão profundamente interligados.

Variáveis como a leitura das políticas de privacidade e a atualização periódica das palavras-passe evidenciam que a ausência de práticas de segurança consistentes se traduz em níveis de risco mais elevados, enquanto o aumento da literacia e da sensibilização contribui para uma redução significativa da exposição a incidentes.

De igual modo, a percepção de que as aplicações móveis são mais seguras do que os websites traduz uma confiança seletiva, frequentemente sustentada na familiaridade com

estas plataformas e não necessariamente na robustez técnica das medidas de segurança implementadas.

A classificação dos riscos, segundo a escala definida anteriormente, e já referida, tabela de classificação e interpretação dos níveis de risco (ponto 9.4.1), confirma a existência de três patamares distintos de vulnerabilidade:

1. riscos residuais ou muito baixos, associados a comportamentos informados e coerentes;
2. riscos moderados a elevados, relacionados com práticas intermitentes ou percepções neutras;
3. riscos críticos, observados nos grupos de utilizadores que demonstram ausência de confiança ou desconhecimento das práticas de proteção digital.

Esta gradação reforça que o fator humano continua a ser o elemento mais determinante na gestão da segurança da informação em dispositivos móveis, independentemente da sofisticação das tecnologias de defesa implementadas.

A seleção das variáveis revelou-se adequada para captar diferentes dimensões do risco — cognitiva, comportamental e percecionada — permitindo uma visão global e integrada do fenómeno.

Os resultados obtidos não só validam a relevância das práticas individuais de segurança, como evidenciam a necessidade de estratégias educativas orientadas para a consciencialização digital, de forma a alinhar a percepção dos utilizadores com os riscos efetivos e promover uma utilização mais informada das plataformas móveis.

Mais do que uma avaliação quantitativa, o capítulo demonstra que a segurança digital é, antes de tudo, uma construção cultural e comportamental, dependente da forma como os utilizadores interpretam, valorizam e integram as práticas de proteção no seu quotidiano.

Assim, compreender o risco não se resume a medi-lo, mas a reconhecer que a verdadeira resiliência digital resulta da combinação entre conhecimento, percepção e ação, estes fatores em conjunto definem o grau de maturidade de uma sociedade digitalmente segura.

10 Conclusão

Este capítulo encerra a dissertação, estabelecendo a ligação entre os resultados obtidos, os objetivos inicialmente definidos e a questão de investigação que orientou o estudo:

“De que forma a percepção de segurança da informação influencia o comportamento dos utilizadores no mobile commerce (m-commerce)?”

A partir da revisão da literatura, do enquadramento teórico e da análise empírica efetuada com recurso ao Método de Mosler, apresentam-se de seguida as principais conclusões. O capítulo contempla uma síntese dos resultados, as implicações teóricas e práticas, as limitações identificadas no processo e algumas recomendações para futuros trabalhos. Termina com uma reflexão final sobre o contributo do estudo para o conhecimento e para a prática no domínio da segurança digital e do comportamento dos utilizadores.

10.1 Síntese dos resultados

A análise dos dados permitiu constatar que a percepção de segurança exerce uma influência direta sobre o modo como os utilizadores interagem com plataformas de m-commerce. Verificou-se que uma parte considerável dos inquiridos possui um nível médio de conhecimento em matéria de segurança digital, revelando ainda práticas de proteção inconsistentes. Essa realidade traduz-se em diferentes graus de exposição a riscos, nomeadamente perdas financeiras, phishing ou violação de dados pessoais.

Os resultados demonstram que os utilizadores com maior consciência e melhores práticas de segurança tais como, a leitura das políticas de privacidade, a alteração periódica das palavras-passe ou a utilização de mecanismos de autenticação reforçada — apresentam níveis de risco muito baixos, segundo o Método de Mosler. Pelo contrário, comportamentos mais negligentes associam-se a riscos elevados ou muito elevados, o que confirma a relação entre o grau de conhecimento e o nível de vulnerabilidade digital.

Em termos gerais, observou-se ainda uma percepção de segurança moderada nas transações móveis, com destaque para o receio de fraudes e da exposição de dados pessoais. Estes resultados corroboram a ideia de que a segurança percebida continua a ser um dos fatores centrais para a adoção e continuidade de uso das plataformas de m-commerce.

10.2 Implicações teóricas

No plano teórico, o estudo reforça a relevância da segurança da informação enquanto elemento estruturante da experiência digital e da confiança do utilizador. A aplicação do Método de Mosler revelou-se particularmente adequada para traduzir percepções subjetivas em indicadores mensuráveis, permitindo avaliar o risco percebido de forma sistemática e comparável. A investigação confirma ainda que a percepção de segurança resulta da interação entre fatores comportamentais, tecnológicos e contextuais, evidenciando a importância de uma abordagem multidimensional. Assim, o trabalho contribui para o avanço da literatura ao propor um modelo de avaliação do risco percebido aplicável em diferentes contextos organizacionais e académicos.

10.3 Implicações práticas

Do ponto de vista prático, os resultados oferecem orientações úteis para organizações e entidades que operam no domínio do comércio eletrónico móvel.

Destaca-se, em particular, a necessidade de:

1. Comunicar de forma clara e acessível as políticas de privacidade e segurança;
2. Adotar mecanismos técnicos robustos de proteção da informação, como a autenticação multifator ou a encriptação de dados;
3. E reforçar a literacia digital dos utilizadores, promovendo comportamentos de prevenção e responsabilidade digital.

O modelo de risco utilizado neste estudo pode ainda servir como instrumento de diagnóstico interno, ajudando as organizações a identificar vulnerabilidades e a definir estratégias de mitigação de forma mais direcionada e eficiente.

10.4 Limitações do estudo

Entre as limitações identificadas, destaca-se a dimensão da amostra, composta por 44 respondentes, o que restringe a capacidade de generalização dos resultados. Acresce o facto de o estudo ter sido desenvolvido no contexto português, não refletindo eventuais diferenças culturais ou tecnológicas de outros mercados.

Outro aspeto a considerar prende-se com a ausência de métodos estatísticos avançados de validação, substituídos pela validação interna supervisionada pelo orientador,

assegurando a coerência e a fiabilidade dos dados tratados. Apesar destas limitações, a aplicação rigorosa do Método de Mosler confere consistência e legitimidade às conclusões apresentadas.

10.5 Recomendações para investigação futura

Em síntese, o estudo confirma que a perceção de segurança da informação constitui um fator determinante para o desenvolvimento e consolidação do m-commerce. A aplicação do Método de Mosler mostrou-se eficaz para quantificar perceções e identificar riscos, permitindo compreender de forma estruturada como o comportamento e o conhecimento dos utilizadores influenciam a sua exposição digital. Os resultados obtidos reforçam a ideia de que a confiança digital depende tanto de medidas técnicas como de atitudes comportamentais, sendo necessário um esforço conjunto entre empresas, utilizadores e instituições públicas para promover ambientes digitais mais seguros e transparentes.

Apesar dos contributos alcançados, este trabalho abre espaço para diversas linhas de investigação futura, nomeadamente:

- Validação do Método de Mosler noutros contextos e populações, aplicando o mesmo enquadramento metodológico a diferentes grupos etários, sectores de atividade e realidades geográficas, de forma a avaliar a consistência e a adaptabilidade do modelo à realidade portuguesa.
- Realização de estudos longitudinais que analisem a evolução da perceção de segurança e do nível de literacia digital ao longo do tempo, permitindo compreender o impacto de campanhas de sensibilização, alterações legislativas ou inovações tecnológicas.
- Integração de variáveis de natureza psicológica e social, como a confiança nas instituições, a influência social ou a experiência prévia com fraudes, de modo a aprofundar a compreensão dos fatores que moldam o comportamento do utilizador no ambiente digital.
- Análise do papel das organizações e das políticas públicas na construção da confiança digital, avaliando a eficácia de mecanismos como a autenticação multifator, as certificações de segurança ou os selos de conformidade em privacidade e proteção de dados.

- Aplicação do método em outros domínios digitais, como o e-banking ou as plataformas de e-government, em que a perceção de risco e a confiança do utilizador assumem relevância semelhante à observada no m-commerce.

Com este trabalho, procurou-se não apenas contribuir para o avanço do conhecimento académico, mas também oferecer um referencial prático de avaliação do risco percebido, que possa apoiar futuras investigações e políticas de segurança digital, em especial no contexto português.

REFERÊNCIAS BIBLIOGRÁFICAS

11 Referências Bibliográficas

- Albertin, A. L. (1999). Comércio Eletrônico: modelo, aspectos e contribuições de sua aplicação. São Paulo: Atlas 15 p.
- Albertin, J. L. (2004). Comércio eletrônico: modelo, aspetos e contribuições de sua aplicação, 5ª Ed. São Paulo: Atlas.
- Albertin, A. L. (2010). Comercio Eletrônico: modelo, aspectos e contribuições de sua aplicação. 6. Ed. São Paulo: Atlas.
- ANACOM. (2022). O comércio eletrônico em Portugal e na União Europeia em 2022 - segmento residencial e empresarial. Wwww.anacom.pt. <https://www.anacom.pt/render.jsp?contentId=1737244>
- Arbex, G. (2021). E-commerce global pode movimentar US\$ 3,4 trilhões em 2025. Forbes Brasil. Disponível em: <https://forbes.com.br/forbes-tech/2021/01/e-commerce-globalpode-movimentar-us-34-tri-em-2025-retailtechs-americanas-brf-muito-mais/>
- Aven, T. (2016). Risk assessment and risk management: Review of recent advances on their foundation. European Journal of Operational Research, 253(1), 1-13. <https://doi.org/10.1016/j.ejor.2015.12.023>
- Bornia, A. C.; Donadel, C. M.; A., Lorandi J. (2006). A logística do comércio eletrônico do B2C (business to consumer). 29º Encontro Nacional de Engenharia da Produção. Salvador, 2006.
- Büyüközkan, G. (2012). Determining the mobile commerce user requirements using an analytic approach. Computer Standards & Interfaces, 31(1), 144–152. <https://doi.org/10.1016/j.csi.2007.11.006>
- Carvalho, S., Carvalho, J. V., Silva, J. C., Casquilho, M., & Santos, G. (2023). The use of ICT in today's society from the perspective of citizens and businesses: Security risks and their influence on the quality of life of the Portuguese population. International Journal for Quality Research, 17(3). <http://ijqr.net/journal/v17-n3/11.pdf>

Comissão Europeia. (2015). Trends in European eCommerce in the EU 2015. Disponível em: <https://ec.europa.eu/digital-single-market/en/downloadscoreboard-reports>.

European Union. (2018). General Data Protection Regulation (GDPR). Retrieved from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679>.

Ferreira & Pitwak. (2009). A Evolução do Retalho de Artigos Desportivos On-line no Século XXI – Projecto Sport Zone On-line (Dissertação de Mestrado não editada, Programa de Mestrado em Gestão). ISCTE - Instituto Universitário de Lisboa, Lisboa.

Gunasekaran, A. M. (2002). Ecommerce and its impact on operations management. *International Journal of Production Economics*, 75(1-2), 185-197, doi: 10.1016/S0925-5273(01)00191-8

Hillmann, R. (2013). Administração de vendas, varejo e serviços; Curitiba; InterSaberes; 2013.

ISO 31000 (2018). Risk management — Guidelines. International Organization for Standardization, Geneva.

Jones, K., and Leonard, L. N. K. (2010). Consumer-to-Consumer e-Commerce: Research in Information Systems Journals. *Journal of Internet Commerce* v.9 (3- 4), pp 186–207.

Kashyap, A. K., & Chaudhary, M. (2023). Cyber security laws and safety in e-commerce in India. *Law and Safety*, 2(89), 207–217. <https://doi.org/10.32631/pb.2023.2.19>.

Khan, M. S., & Islam, S. H. (2021). Cybersecurity in Mobile Commerce: Vulnerabilities, Threats, and Countermeasures. In: 2021 IEEE 15th International Conference on Anti-counterfeiting, Security, and Identification (ASID), Xiamen, China.

Laudon, K. C., & Traver, C. G. (2007). E-commerce: Business, Technology, Society. Pearson.

- Parente, Juracy. (2000). Varejo no Brasil. São Paulo. Atlas, 2000.
- Reedy, J., Schullo, S. (2007). Marketing eletrônico: integrando recursos eletrônicos no processo de marketing. Cengage Learning.
- Tiwari, R., & Buse, S. (2007). The Mobile Commerce Prospects: A Strategic Analysis of Opportunities in the Banking Sector. Hamburg University Press, Hamburg, 33.
- World Trade Organization. (2013). E-commerce in developing countries: Opportunities and challenges for small and medium-sized enterprises. Obtido de https://www.wto.org/english/res_e/booksp_e/ecom_brochure_e.pdf.
- Zhang, R., Chen, J. Q., & Lee, C. J. (2013). Mobile commerce and consumer privacy concerns. Journal of Computer Information Systems, 53(4), 31-38.

12 Apêndices

12.1 Apêndice I – Questionário Aplicado

Questionário sobre Segurança em m-Commerce

Instruções: Por favor, responda às seguintes perguntas com base na sua experiência com compras online e serviços de m-commerce. Todas as respostas são confidenciais e serão utilizadas apenas para fins de investigação.

1. Informações Pessoais

1. Idade:

- ☐ 18-24
- ☐ 25-34
- ☐ 35-44
- ☐ 45-54
- ☐ 55-64
- ☐ 65 ou mais

2. Género:

- ☐ Masculino
- ☐ Feminino
- ☐ Prefiro não divulgar

3. Nível de Escolaridade:

- ☐ Ensino Básico
- ☐ Ensino Secundário
- ☐ Ensino Superior Incompleto
- ☐ Ensino Superior Completo
- ☐ Pós-Graduação
- ☐ Outro (especifique): _____

4. Região Geográfica:

- ☐ Norte

- ☐ Centro
- ☐ Lisboa e Vale do Tejo
- ☐ Alentejo
- ☐ Algarve
- ☐ Açores
- ☐ Madeira

2. Conscientização sobre Segurança

5. Já ouviu falar das seguintes ameaças de segurança em m-commerce? (Marque todas as que se aplicam)

- Malware móvel
- Phishing
- Intercepção de dados
- Fraude em transações
- Roubo de identidade
- Outras (especifique): _____
- Não estou ciente de nenhuma destas ameaças

6. Qual é o seu nível de conhecimento sobre práticas de segurança para compras online?

- ☐ Muito baixo
- ☐ Baixo
- ☐ Médio
- ☐ Alto
- ☐ Muito alto

3. Comportamentos de Segurança

7. Quais das seguintes práticas de segurança você adota ao realizar compras online em dispositivos móveis? (Marque todas as que se aplicam)

- Uso de autenticação multifatorial
- Verificação do certificado de segurança do site
- Evitação de redes Wi-Fi públicas para transações
- Uso de aplicativos de segurança (antivírus, firewall)

- Atualização regular do sistema operativo e aplicativos
- Monitoramento das transações bancárias
- Outras práticas (especifique): _____
- Não adoto nenhuma destas práticas

8. Você costuma rever a política de privacidade dos sites onde realiza compras?

- ☐ Sempre
- ☐ Frequentemente
- ☐ Ocasionalmente
- ☐ Raramente
- ☐ Nunca

Com que frequência atualiza as palavras-passe das suas contas em plataformas de m-commerce?

- ☐ Mensalmente
- ☐ A cada 3 meses
- ☐ A cada 6 meses
- ☐ Anualmente
- ☐ Nunca ou muito raramente

Utiliza diferentes palavras-passe para diferentes contas de m-commerce?

- ☐ Sempre
- ☐ Frequentemente
- ☐ Ocasionalmente
- ☐ Raramente
- ☐ Nunca

Que métodos utiliza para armazenar ou lembrar-se das suas palavras-passe?

- ☐ Aplicações de gestão de palavras-passe
- ☐ Escritas num local físico (caderno, papel)
- ☐ Memorização
- ☐ Armazenadas no navegador
- ☐ Outro (especifique): _____

4. Percepção de Risco

9. Qual é a sua percepção sobre o nível de segurança das transações realizadas em dispositivos móveis?

- ☐ Muito inseguro
- ☐ Inseguro
- ☐ Neutro
- ☐ Seguro
- ☐ Muito seguro

10. Qual é a probabilidade de abandonar um site de compras online se perceber que ele não tem um certificado de segurança?

- ☐ Muito alta
- ☐ Alta
- ☐ Moderada
- ☐ Baixa
- ☐ Muito baixa

11. Quão preocupante você considera os seguintes riscos associados ao m-commerce? (Avalie de 1 a 5, sendo 1 = Nada preocupante e 5 = Extremamente preocupante)

- Malware móvel: [1] [2] [3] [4] [5]
- Phishing: [1] [2] [3] [4] [5]
- Interceptação de dados: [1] [2] [3] [4] [5]
- Fraude em transações: [1] [2] [3] [4] [5]
- Roubo de identidade: [1] [2] [3] [4] [5]

Se tivesse uma experiência negativa de segurança (ex.: roubo de dados), como isso afectaria a sua confiança no m-commerce?

- ☐ Perderia totalmente a confiança
- ☐ Reduziria significativamente a confiança
- ☐ Reduziria um pouco a confiança
- ☐ Não afectaria muito a minha confiança

- ☐ Não afectaria em nada a minha confiança

Qual considera ser o maior risco ao realizar compras em dispositivos móveis?

- ☐ Roubo de informações pessoais
- ☐ Uso indevido dos dados do cartão de crédito
- ☐ Perda de dinheiro em transações fraudulentas
- ☐ Downloads de malware
- ☐ Outro (especifique): _____

Qual é a sua percepção sobre a segurança das aplicações móveis de grandes empresas comparada com websites no navegador?

- ☐ As aplicações móveis são mais seguras
- ☐ Os websites no navegador são mais seguros
- ☐ Ambas são igualmente seguras
- ☐ Nenhuma delas é segura
- ☐ Não tenho opinião formada

5. Experiência com m-Commerce

12. Com que frequência você realiza compras online usando dispositivos móveis?

- ☐ Diariamente
- ☐ Semanalmente
- ☐ Mensalmente
- ☐ Ocasionalmente
- ☐ Raramente

Qual é o principal motivo que o leva a utilizar dispositivos móveis para compras online?

- ☐ Conveniência
- ☐ Rapidez
- ☐ Promoções e descontos exclusivos
- ☐ Facilidade de pagamento
- ☐ Outro (especifique): _____

Já teve alguma experiência negativa ao realizar compras através de dispositivos móveis?

- ☐ Sim, mais de uma vez
- ☐ Sim, uma vez
- ☐ Não, nunca tive
- ☐ Não sei ou não me lembro

Com que frequência compara preços entre diferentes plataformas antes de concluir uma compra num dispositivo móvel?

- ☐ Sempre
- ☐ Frequentemente
- ☐ Ocasionalmente
- ☐ Raramente
- ☐ Nunca

6. Comentários Adicionais

14. Se tiver alguma outra observação ou comentário sobre segurança em m-commerce, por favor, partilhe abaixo:

- _____

Obrigado por participar na nossa pesquisa! As suas respostas são muito importantes para o nosso estudo.

12.2 Formulas e estruturas de calculo utilizado

| **Calculos**

Magnitude do Risco (C) dado por **I** mportância do Sucesso (I) + **D** anos causados (D)

I (FxS)	1
D (Px E)	1

Probabilidade de Ocorrência (Pb), dado por **A** gressão x **V**ulnerabilidade

PB	1
----	---

Evolução do Risco (ER), dado pela Magnitude do Risco x Probabilidade

ER	2
----	---

Escala:	Pontuação:
Muito Alta	05
Alta	04
Normal	03
Baixa	02
Muito Baixa	01

Ilustração 4 Escala avaliação de risco

13 Anexos

13.1 Anexo I – Escala Metodo de Mosler

O método Mosler é uma metodologia científica, dividida em quatro fases, assim distribuídas:

1. Definição do risco (bem e o dano)
2. Análise do risco (seis critérios)
3. Evolução do risco
4. Classe do risco

A análise de risco é realizada através da mensuração de seis critérios.

Os critérios são:

- Critério da Função (F) – projeta as consequências ou danos que podem alterar a atividade principal da empresa, caso o risco se concretize, na seguinte pontuação:

Escola:	Pontuação:
Muito Gravemente	05
Gravemente	04
Medianamente	03
Levemente	02
Muito Levemente	01

Ilustração 5 Escala de Pontuação Criterio F

- Critério da Substituição (S) – avalia qual o impacto da concretização da ameaça sobre os bens, ou seja, a dificuldade em substituir os bens atingidos. Sua escala de pontuação é:

Escala:	Pontuação:
Muito Difícilmente	05
Difícilmente	04
Sem Muitas Dificuldades	03
Facilmente	02
Muito Facilmente	01

Ilustração 6 Escala de pontuação critério S

- Critério da Profundidade (P) – Caso o risco se concretize, mede a perturbação interna e os efeitos psicológicos que o risco poderá causar para a imagem da empresa. Possui a seguinte tabela de pontuação:

Escala:	Pontuação:
Perturbações Muito Graves	05
Perturbações Graves	04
Perturbações Limitadas	03
Perturbações Leves	02
Perturbações Muito Leves	01

Ilustração 7 Escala de pontuação critério P

- Critério da Extensão (E) – mede o alcance e a extensão que o dano causaria à empresa, caso se concretizasse. Possui a seguinte escala de pontuação:

Escala:	Pontuação:
De caráter Internacional	05
De caráter Nacional	04
De caráter Regional	03
De caráter Local	02
De caráter Individual	01

Ilustração 8 Escala de pontuação critério E

- Critério de Agressão (A) – Mede a possibilidade de o risco vir a ocorrer, de acordo com as características conjunturais e físicas da empresa onde a avaliação está sendo realizada. A tabela de avaliação é:

Escala:	Pontuação:
Muito Alta	05
Alta	04
Normal	03
Baixa	02
Muito Baixa	01

Ilustração 9 Escala de pontuação critério A

- Critério de Vulnerabilidade (V) – Baseado no item anterior (critério de agressão), o critério da vulnerabilidade avalia o impacto financeiro caso o risco se concretize. Sua tabela de avaliação é a seguinte:

Escala:	Pontuação:
Muito Alta	05
Alta	04
Normal	03
Baixa	02
Muito Baixa	01

Ilustração 10 Escala de pontuação critério V

Para cada uma destes critérios, o gestor deve pontuar, de acordo com o cenário existente e sua experiência profissional. Sempre lembrando da necessidade da participação de outros integrantes da empresa para auxiliarem na avaliação desta pontuação.

3. Evolução do risco:

Agora veremos a Evolução do Risco, que é a quantificação do risco. Isto é feito calculando-se a magnitude do risco, representado pela letra “C”.

O valor da magnitude do risco (C) é encontrado através da soma da Importância do Sucesso (I) e dos Danos Causados (D).

Então, a fórmula fica: $C = I + D$, onde:

$$I = F \times S \text{ (Função x Substituição)}$$

$$D = P \times E \text{ (Profunda x Extensão)}$$

Desse modo a Magnitude do risco fica assim representada:

$$C = I (F \times S) + D (P \times E)$$

A próxima etapa será calcular a Probabilidade de Ocorrência (Pb), que será encontrada através da multiplicação da Agressão pela Vulnerabilidade, ficando assim representado:

$$Pb = A \times V \text{ (Agressão x Substituição)}$$

Agora poderemos calcular a Evolução do Risco (ER) que é a multiplicação dos dois resultados encontrados anteriormente, o C x Pb (Magnitude do Risco x Probabilidade).

$$ER = C \times Pb$$

Com o resultado desta multiplicação encontramos o valor da Evolução do Risco, agora, a partir deste resultado, vamos classificar o risco.

5. Classe do risco

A classificação do risco nada mais é do que pegarmos o resultado do ER (Evolução do risco) e compará-lo com a tabela abaixo, classificando, dessa forma, o risco analisado.

De acordo com esta tabela a classificação pode ser:

Valor do ER	Classe do Risco
2 – 250	Muito Baixo
251 – 500	Pequeno
501 – 750	Normal
751 – 1.000	Grande
1.001 – 1.250	Elevado

Ilustração 11 Tabela de classificação Valor ER

A classificação do risco, de acordo com a análise realizada, dará subsídios para que o gestor possa priorizar as ações de segurança na empresa.

Este método pode ser representado através de uma grade que representa toda a metodologia, como vemos na figura abaixo:

Risco	F	S	P	E	A	V	I F x S	D P x E	C I+D	Pb A x V	ER C x Pb	CLASSE
ASSALTO	3	2	4	3	3	4	6	12	18	12	216	MUITO BAIXO

Ilustração 12 Tabela classificação classe de risco

Apenas como exemplo, inseri alguns números na grade a fim de demonstrar sua utilização e o resultado alcançado.

É, sem dúvida, um método simples e que é usado há muito tempo na segurança patrimonial e empresarial, porém este método é subjetivo e seu resultado dependerá do grau de conhecimento do gestor e dos demais membros da empresa que colaboraram com a análise.

PARAMETRIZAÇÃO

Apesar de esta metodologia ser usada amplamente na Europa, temos algumas dificuldades na sua aplicação, principalmente por apresentar como resultado conclusivo uma avaliação de que o risco pode ser muito baixo, pequeno, normal, grande ou elevado, ou seja, não é mensurável, o que dificulta a sua aceitação por parte dos empresários.

A partir destas dificuldades é que o professor Antonio Celso Ribeiro Brasileiro, criou a parametrização, que nada mais é do que transformar o resultado da classe do risco em percentual, ou seja, em probabilidade numérica, como ocorre com o método estatístico, o que facilita nosso entendimento e principalmente, a visualização do risco.

Além disso, ele substituiu o critério de agressão por probabilidade e de vulnerabilidade por impacto financeiro, permanecendo as mesmas tabelas de gradação.

Estas alterações no método Mosler ficaram conhecidas como método Brasileiro, devido à iniciativa do professor, porém hoje em dia ele usa uma metodologia própria dentro de um processo que segue o modelo sugerido pela ISO 31000.

Para fazer a parametrização é necessário pegar o resultado da análise da Evolução do Risco (ER) e classificá-lo na tabela de Pb, que é dividida em cinco níveis relativos à variação de faixa, que neste caso é de 20% (4% para cada faixa).