Universidade do Minho

Escola de Economia e Gestão

João Afonso Cruz Loureiro

Evolução, impacto e mitigação do cibercrime no Setor Financeiro: uma revisão estruturada da literatura

Abril de 2026

Evolução, impacto e mitigação do cibercrime no Setor Financeiro: uma revisão estruturada da literatura

João Afonso Cruz Loureiro

UMinho ! 2026

Universidade do Minho

Escola de Economia e Gestão

João Afonso Cruz Loureiro

Evolução, impacto e mitigação do cibercrime no Setor Financeiro: uma revisão estruturada da literatura

Dissertação de Mestrado

Mestrado em Economia Industrial e da

Empresa

Trabalho efetuado sob a orientação de

Professora Doutora Maria Lurdes Castro Martins

abril de 2026

DECLARAÇÃO DE INTEGRIDADE

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

DECLARAÇÃO DE USO DE FERRAMENTAS DE INTELIGÊNCIA ARTIFICIAL (IA)

Declaro ter atuado com integridade na elaboração do presente trabalho académico e confirmo que não recorri a qualquer forma de utilização indevida de ferramentas de Inteligência Artificial (IA), nem à falsificação ou omissão de informações, fontes, dados, resultados ou processos em nenhuma das etapas conducentes à sua elaboração.

Declaro ainda que qualquer utilização de ferramentas de IA foi feita de forma transparente e responsável, encontrando-se devidamente assinalada/descrita no trabalho, e que procedi à verificação crítica da exatidão do conteúdo produzido com o seu apoio, assumindo integralmente a responsabilidade pelo que submeto.

Mais declaro que conheço e que respeitei o Código de Conduta Ética da Universidade do Minho, bem como as normas aplicáveis de integridade académica e de proteção de dados.

Direitos de Autor e Condições de Utilização do Trabalho por Terceiros

Este é um trabalho académico que pode ser utilizado por terceiros desde que respeitadas as regras e boas práticas internacionalmente aceites, no que concerne aos direitos de autor e direitos conexos. Assim, o presente trabalho pode ser utilizado nos termos previstos na licença abaixo indicada. Caso o utilizador necessite de permissão para poder fazer um uso do trabalho em condições não previstas no licenciamento indicado, deverá contactar o autor, através do RepositóriUM da Universidade do Minho.

Licença concedida aos utilizadores deste trabalho



Atribuição
CC BY

https://creativecommons.org/licenses/by/4.0/

Agradecimentos

A realização desta tese representa o culminar de uma etapa importante do meu percurso académico e pessoal, que não teria sido possível sem o apoio e a colaboração de várias pessoas e instituições.

Em primeiro lugar, expresso o meu sincero agradecimento à minha orientadora, Professora Maria Lurdes Castro Martins, pela orientação, disponibilidade, incentivo e pelos valiosos conhecimentos partilhados ao longo de todo este trabalho.

Agradeço também aos docentes e colegas que, de diferentes formas, contribuíram para a minha formação e para a concretização desta investigação.

Uma palavra de especial reconhecimento à minha família, pelo apoio incondicional, compreensão e confiança depositada em mim ao longo deste percurso. O seu encorajamento constante foi fundamental para superar os desafios encontrados.

Aos meus amigos, agradeço a amizade, a motivação e todos os momentos de apoio e companheirismo, que tornaram esta caminhada mais enriquecedora.
Por fim, agradeço a todos aqueles que, direta ou indiretamente, contribuíram para a realização desta tese e para a concretização deste objetivo.

A todos, o meu mais sincero obrigado.

Resumo

O presente trabalho analisa a evolução, impacto e mitigação do cibercrime no setor financeiro nos anos 2020-2026. Nas últimas décadas, a digitalização intensiva do setor financeiro alterou profundamente a organização dos serviços bancários, dos pagamentos digitais e das infraestruturas de mercado, tornando a cibersegurança uma dimensão central da continuidade operacional das instituições, plataformas e infraestruturas críticas que compõem o ecossistema financeiro e, por essa via, da estabilidade do próprio setor e da confiança económica em contextos crescentemente dependentes da fiabilidade dos pagamentos, da intermediação financeira e do regular funcionamento dos mercados. Esta dissertação desenvolve uma revisão estruturada da literatura científica, apoiada por um procedimento de pesquisa, seleção e análise adaptado ao modelo PRISMA, com o objetivo de identificar os principais contributos da literatura sobre a evolução, o impacto e a mitigação do cibercrime no setor financeiro no período 2020–2026.

A investigação organiza a literatura em torno de quatro eixos analíticos: tipologias de ameaça, impactos económicos, respostas institucionais e regulatórias e mecanismos de resiliência digital. A análise assenta num corpus final de 70 artigos científicos, selecionados a partir do *Web of Science Core Collection* e da *Scopus*. Os resultados mostram, em primeiro lugar, que *phishing, smishing, ransomware*, fraude em pagamentos digitais, vulnerabilidades em ecossistemas *fintech* e dependências de terceiros críticos compõem um padrão de risco cada vez mais híbrido, interdependente e ecossistémico. Em segundo lugar, mostram que os efeitos do cibercrime ultrapassam a perda direta, incluindo custos operacionais, danos reputacionais, pressões de conformidade, custos de remediação e potenciais externalidades sistémicas. Em terceiro lugar, a literatura evidencia o reforço da resposta institucional e regulatória, com destaque para o DORA e para a crescente centralidade da resiliência operacional digital. Em quarto lugar, confirma que a mitigação eficaz depende da articulação entre governação, tecnologia, cultura organizacional e cooperação institucional.

A dissertação insere-se na área científica do Mestrado em Economia Industrial e de Empresa porque analisa o cibercrime no setor financeiro como variável que condiciona a eficiência, a competitividade, a governação e a estabilidade do setor financeiro contemporâneo.

Palavras-chave: cibercrime, ciberataque, cibersegurança, risco cibernético, setor financeiro, banca, instituição financeira, *fintech*, pagamentos digitais, banca móvel

Abstract

This study analyzes the evolution, impact, and mitigation of cybercrime in the financial sector from 2020 to 2026. Over the last decades, the intensive digitalization of the financial sector has *profoundly transformed banking services, digital payments, and market infrastructures, making cybersecurity* a *central dimension of the operational continuity of the institutions, platforms, and critical infrastructures that compose the financial ecosystem and*, consequently, *of the stability of the sector and the economic confidence that depends on the reliability of payments, financial* intermediation, *and the regular functioning of markets. This dissertation develops* a *structured review of the scientific literature, supported* by a *search, selection, and analysis procedure adapted from the* PRISMA *model, in order to identify the main contributions of the literature on the evolution, impact, and mitigation of cybercrime in the financial sector between* 2020 *and* 2026.

The study is organized around four analytical axes: threat typologies, economic impacts, institutional and regulatory responses, and digital resilience mechanisms. The analysis is based on a *final corpus of* 70 *scientific articles, selected from the Web of Science Core Collection and* Scopus. *The findings show, first, that phishing, smishing, ransomware, digital payment fraud, vulnerabilities in fintech ecosystems, and dependencies on critical third parties form an increasingly hybrid, interdependent, and ecosystem-based pattern of risk. Second, they show that the effects of cybercrime extend beyond direct losses to include operational costs*, reputational *damage, compliance pressures*, remediation *costs, and potential systemic externalities. Third, the literature highlights the strengthening of institutional and regulatory responses, particularly*

through DORA *and the growing centrality of digital operational resilience*. *Fourth*, *it confirms that effective mitigation depends on the articulation of governance*, *technology*, *organizational culture*, *and institutional cooperation*.

This dissertation is situated within the scientific field of the Master's in Industrial and Business Economics because it analyses cybercrime in the financial sector as a *variable that shapes efficiency*, *competitiveness*, *governance*, *and the stability of the* contemporary *financial sector*.

Keywords*: cybercrime*, *cyber attack, cybersecurity cyber risk, financial sector, banking, financial institution, fintech, digital payment, mobile banking*

Índice

DECLARAÇÃO DE INTEGRIDADE i

Agradecimentos iii

Resumo iv

Abstract vi

Siglas e Abreviaturas xi

1. Introdução 1

2. Revisão da Literatura 4

2.1 Introdução 4

2.2 Cibersegurança: enquadramento conceptual e evolução do campo 4

2.3 O setor financeiro como espaço crítico de exposição ao risco cibernético 5

2.4 Evolução recente das ameaças no setor financeiro 7

2.5 Impactos do cibercrime: da perda direta à vulnerabilidade sistémica 8

2.6 Regulação, governação e resposta institucional 9

2.7 Resiliência digital como novo paradigma 10

2.8 Posicionamento da dissertação na literatura existente 11

2.9 Posicionamento da dissertação face às revisões estruturadas existentes 13

3. Metodologia 17

3.1 Enquadramento metodológico 17

3.2 Estratégia de pesquisa bibliográfica 18

3.3 Processo de seleção dos artigos 20

3.4 Critérios de inclusão e exclusão 21

3.5 Organização e tratamento dos resultados 22

3.6 Procedimentos de extração e análise dos dados 22

3.7 Composição do corpus analisado 23

3.8 Validação e controlo de qualidade 24
3.9 Limitações metodológicas 25
3.10 Síntese metodológica 25
4 Análise e Discussão dos Resultados 27
4.1 Introdução 27
4.2 Tipologias de ameaça no setor financeiro 28
4.2.1 Dados quantitativos do eixo das tipologias de ameaça 30
4.3 Impactos económicos do cibercrime financeiro 35
4.3.1 Dados quantitativos do eixo dos impactos económicos 37
4.4 Respostas institucionais e regulatórias 41
4.4.1 Dados quantitativos do eixo das respostas institucionais e regulatórias 43
4.5 Mecanismos de resiliência digital 48
4.5.1 Dados quantitativos do eixo dos mecanismos de resiliência digital 49
4.6 Síntese do capítulo 57
5 Conclusão 58
5.1 Introdução 58
5.2 Resposta à pergunta de investigação 58
5.3 Principais conclusões por eixo 59
5.6 Pistas para investigação futura 62
5.7 Conclusão final 63
Referências 63

Índice de tabelas

Tabela 1 – Distribuição dos artigos pelos eixos analíticos 23
Tabela 2 - Artigos que se enquadram no eixo das tipologias de ameaças 31
Tabela 3 - Artigos que se enquadram no eixo dos impactos económicos 39
Tabela 4 - Artigos que se enquadram no eixo das respostas institucionais e regulatórias 45
Tabela 5 - Artigos que se enquadram no eixo dos mecanismos de resiliência digital 51

Siglas e Abreviaturas

Sigla	Significado
IA	Inteligência Artificial
AI	Artificial Intelligence
PRISMA	Preferred Reporting Items for Systematic Reviews and Meta-Analyses
SLR	Systematic Literature Review
DORA	Digital Operational Resilience Act
NIS2	Network and Information Security Directive 2
TIC	Tecnologias de Informação e Comunicação
ICT	Information and Communication Technology
SWIFT	Society for Worldwide Interbank Financial Telecommunication
TS	Topic Search (Web of Science)
TITLE-ABS-KEY	Title, Abstract and Keywords (Scopus)
DOI	Digital Object Identifier
URL	Uniform Resource Locator
API	Application Programming Interface
ANN	Artificial Neural Network
CNN	Convolutional Neural Network
DNN	Deep Neural Network
RNN	Recurrent Neural Network
SGRU	Stacked Gated Recurrent Unit
AUC	Area Under the Curve
F1-score	Métrica F1
XAI	Explainable Artificial Intelligence
CBDC	Central Bank Digital Currency

Sigla	Significado
P2P	Peer-to-Peer
PCI DSS	Payment Card Industry Data Security Standard
NIST	National Institute of Standards and Technology
ENISA	European Union Agency for Cybersecurity
ECB	European Central Bank
BIS	Bank for International Settlements
FMI	Fundo Monetário Internacional
GFSR	Global Financial Stability Report
GDPR	General Data Protection Regulation
IEEE	Institute of Electrical and Electronics Engineers
ACM	Association for Computing Machinery
EU	European Union
UE	União Europeia
UK	United Kingdom
US	United States
EUA	Estados Unidos da América
USD	United States Dollar
IBM	International Business Machines

1. Introdução

Nas últimas duas décadas, a transformação digital do setor financeiro reconfigurou profundamente a prestação de serviços bancários, os sistemas de pagamento, a mediação financeira e as infraestruturas de mercado. A aceleração do *digital banking*, das *fintech*, dos pagamentos móveis, da automatização analítica e da interligação entre plataformas aumentou a eficiência, a conveniência e a capacidade de escala das instituições, mas tornou igualmente a segurança digital um fator central da continuidade operacional do ecossistema financeiro, da confiança do mercado e da estabilidade do próprio setor financeiro em economias crescentemente dependentes da integridade das transações e da disponibilidade dos serviços.

Esta exposição acrescida ao risco não resulta apenas da crescente sofisticação tecnológica das instituições financeiras. Decorre, sobretudo, da densidade relacional do ecossistema em que estas operam, marcado por interdependências entre bancos, seguradoras, processadores de pagamento, prestadores de serviços TIC, fornecedores *cloud*, operadores de mercado e utilizadores finais. Num contexto desta natureza, uma vulnerabilidade localizada pode propagar efeitos para lá da entidade inicialmente afetada, ampliando os custos operacionais, reputacionais e regulatórios do incidente.

A relevância do problema torna-se particularmente evidente quando é dada relevância na literatura a episódios de ataque ao *Bangladesh Bank* via *SWIFT*, grandes violações de dados em entidades financeiras, esquemas de *phishing* dirigidos a clientes bancários, fraude em pagamentos digitais e disrupções operacionais associadas a dependências tecnológicas críticas. Estes casos mostram que o cibercrime financeiro não representa apenas uma ameaça técnica: trata-se de um fenómeno com implicações económicas, organizacionais, jurídicas e estratégicas, capaz de afetar simultaneamente instituições individuais e a confiança sistémica no funcionamento do setor.

A presente dissertação insere-se na área científica do Mestrado em Economia Industrial e de Empresa porque analisa o cibercrime no setor financeiro, que é uma variável que condiciona a eficiência organizacional, a governação, a inovação, a regulação e a competitividade no setor financeiro. A questão da cibersegurança é aqui tratada não como domínio periférico de suporte tecnológico, mas como componente estruturante da economia digital contemporânea e da capacidade das instituições para criar valor em ambientes de elevada interdependência e incerteza.

O objetivo principal da investigação consiste em analisar o cibercrime no setor financeiro entre 2020 e 2026 com base na literatura científica recente, procurando identificar as principais tipologias de ameaça, compreender os seus impactos económicos, examinar as respostas institucionais e regulatórias e discutir os mecanismos de resiliência digital propostos ou observados no período em análise.

De forma mais específica, a dissertação procura responder à seguinte questão de investigação: o que revela a literatura científica recente sobre a evolução, o impacto e a mitigação do cibercrime no setor financeiro entre 2020 e 2026? A resposta a esta questão é desenvolvida a partir de quatro eixos analíticos: tipologias de ameaça, impactos económicos, respostas institucionais e regulatórias e mecanismos de resiliência digital, que funcionam como estrutura de leitura e de integração dos resultados.

Embora estes quatro eixos orientem a interpretação global do estudo, a dissertação não os utiliza de forma mecânica em todos os capítulos. O Capítulo 2 desenvolve uma revisão da literatura de natureza conceptual e progressiva; o Capítulo 3 explicita as opções metodológicas, o processo de seleção do corpus e a lógica de análise; o Capítulo 4 mobiliza diretamente os quatro eixos na discussão dos resultados; e o Capítulo 5 sintetiza as conclusões, as implicações para o setor e as principais direções de aprofundamento futuro.

A dissertação encontra-se, assim, organizada em cinco capítulos. O primeiro apresenta o enquadramento do problema, a relevância do tema, o objetivo da investigação e a questão orientadora. O segundo capítulo revê criticamente a literatura sobre cibersegurança, risco financeiro digital, regulação e resiliência. O terceiro capítulo descreve o desenho metodológico e os procedimentos de seleção e análise dos artigos. O quarto capítulo discute os resultados à luz dos quatro eixos analíticos definidos. Por fim, o quinto capítulo reúne as conclusões da investigação, as implicações práticas e as limitações e perspetivas de investigação futura.

2. Revisão da Literatura

2.1 Introdução

A digitalização da economia transformou profundamente a forma como indivíduos, empresas e instituições financeiras operam, comunicam e realizam transações. No setor financeiro, esta transformação assumiu particular intensidade, dada a combinação entre forte pressão por eficiência, crescente expectativa de conveniência por parte dos utilizadores e rápida integração de infraestruturas digitais, plataformas móveis, serviços baseados em dados e ecossistemas *fintech*. É neste contexto que a literatura recente passou a tratar o cibercrime financeiro não como desvio marginal da inovação, mas como consequência estrutural da reorganização digital do setor.

A presente revisão da literatura tem como objetivo enquadrar teoricamente a investigação e clarificar o lugar da dissertação no debate recente sobre cibercrime no setor financeiro. Em vez de reproduzir uma enumeração descritiva de estudos, o capítulo organiza a discussão de forma temática e cumulativa, articulando conceitos, resultados empíricos e tendências de investigação. Pretende-se, assim, construir um quadro interpretativo capaz de sustentar a análise posterior, identificar os principais consensos e tensões da literatura e justificar a opção pelos quatro eixos analíticos que estruturam a dissertação.

2.2 Cibersegurança: enquadramento conceptual e evolução do campo

A cibersegurança consolidou-se, nas últimas décadas, como uma área central de investigação e de intervenção prática, acompanhando a crescente digitalização das sociedades e das economias. Inicialmente associada sobretudo à proteção de sistemas informáticos, redes e bases de dados, a cibersegurança passou progressivamente a ser entendida de forma mais ampla, abrangendo a proteção de infraestruturas críticas, cadeias de fornecimento digitais, plataformas de comunicação, identidades eletrónicas e processos organizacionais. Esta evolução reflete o reconhecimento de que os riscos digitais não se limitam ao plano técnico, mas têm também implicações

económicas, sociais, organizacionais e políticas (Uddin et al., 2020; Annarelli et al., 2020).

A literatura contemporânea tende a conceptualizar a cibersegurança como um domínio multidisciplinar, no qual coexistem abordagens oriundas da ciência da computação, da gestão, da economia, do direito e das relações internacionais. Esta multidisciplinaridade tornou-se especialmente relevante à medida que os incidentes cibernéticos passaram a afetar não apenas a integridade e confidencialidade de dados, mas também a continuidade operacional de organizações, a reputação institucional, a confiança dos consumidores e, em alguns casos, a estabilidade de mercados inteiros. Assim, a cibersegurança deixou de poder ser tratada apenas como uma função técnica de proteção e passou a ser integrada em modelos mais amplos de gestão do risco e de governação organizacional (Dasgupta et al., 2022; Gatzert & Schubert, 2022; Cojocaru, 2025).

Um dos aspetos mais importantes da evolução recente da literatura é a passagem de uma visão centrada na prevenção para uma lógica mais abrangente de resiliência. Se, numa fase anterior, o enfoque recaía sobretudo na criação de barreiras defensivas e mecanismos de controlo de acesso, hoje é cada vez mais frequente a defesa de modelos orientados para a capacidade de resistir, detetar, responder e recuperar face a incidentes. Esta mudança decorre do reconhecimento de que, num ambiente digital altamente complexo e interconectado, a eliminação completa do risco é impraticável.

Consequentemente, a literatura passou a valorizar a adaptabilidade organizacional, a aprendizagem com incidentes e a preparação para cenários de disrupção (Annarelli et al., 2020; van der Kleij et al., 2021; Vandezande, 2024).

2.3 O setor financeiro como espaço crítico de exposição ao risco cibernético

Entre todos os setores económicos, o setor financeiro surge recorrentemente na literatura como um dos mais expostos e mais sensíveis ao risco cibernético. Tal deve-se a um conjunto de características estruturais. Em primeiro lugar, trata-se

de um setor com elevado grau de digitalização, no qual grande parte da atividade depende de sistemas eletrónicos de pagamento, plataformas bancárias *online*, aplicações móveis, redes interbancárias, serviços de *cloud* e integração com prestadores tecnológicos externos. Em segundo lugar, a informação tratada por estas instituições possui elevado valor económico e estratégico, tornando-as alvos particularmente atrativos para agentes maliciosos. Em terceiro lugar, o funcionamento do setor depende fortemente da confiança dos utilizadores, o que significa que incidentes cibernéticos podem ter efeitos reputacionais e sistémicos desproporcionados em relação ao dano técnico imediato (Uddin et al., 2020; Uddin et al., 2023; Aldasoro et al., 2022).

A literatura também sublinha a elevada interdependência do ecossistema financeiro. Bancos, seguradoras, processadores de pagamentos, *fintech*, operadores de mercado e prestadores de serviços TIC estão hoje ligados por relações tecnológicas e operacionais cada vez mais densas. Esta interdependência implica que uma falha num único ponto da cadeia possa propagar-se com rapidez e gerar efeitos em cascata. Assim, o setor financeiro distingue-se de outros setores não apenas pelo valor dos ativos digitais que concentra, mas também pela possibilidade de transformação de incidentes individuais em eventos com alcance sistémico. Esta leitura aproxima o risco cibernético de categorias tradicionalmente associadas à supervisão macroprudencial, como contágio, interligação e vulnerabilidade estrutural (Aldasoro et al., 2022; Vandezande, 2024; Krishna et al., 2023).

Neste contexto, o cibercrime financeiro deve ser entendido como um fenómeno que atua simultaneamente sobre o plano microeconómico e macroeconómico. Ao nível das instituições individuais, os ataques podem causar perdas diretas, interrupção de serviços, roubo de informação e custos de recuperação. Ao nível do sistema, podem comprometer a confiança dos utilizadores, afetar canais de pagamento, interromper infraestruturas críticas e aumentar a perceção de instabilidade nos mercados. A literatura recente tem vindo, por isso, a insistir que a análise do cibercrime financeiro não pode restringir-se à lógica da segurança

informática clássica, exigindo uma leitura integrada que combine risco operacional, economia da confiança, regulação e estabilidade financeira (Uddin et al., 2020; Gatzert & Schubert, 2022; Aldasoro et al., 2022).

2.4 Evolução recente das ameaças no setor financeiro

A literatura sobre o período mais recente evidencia uma transformação significativa na natureza das ameaças cibernéticas dirigidas ao setor financeiro. Os ataques tornaram-se mais frequentes, mais diversificados e mais difíceis de detetar, acompanhando a crescente complexidade das infraestruturas digitais utilizadas pelas instituições. Entre as ameaças mais estudadas destacam-se o *phishing* e outras formas de engenharia social, a fraude em pagamentos digitais, os ataques a aplicações móveis, o *malware*, os ataques a cadeias de fornecimento e a exploração de vulnerabilidades em plataformas e APIs (Jain et al., 2023; Javaheri et al., 2024; Mustapha et al., 2023).

O destaque dado à engenharia social na literatura é particularmente revelador. Ao contrário de uma visão limitada do cibercrime como ataque estritamente técnico, muitos estudos mostram que os atacantes exploram sobretudo a confiança, a urgência, a familiaridade com marcas institucionais e a vulnerabilidade comportamental dos utilizadores. A importância do *phishing*, do *smishing* e de formas semelhantes de fraude confirma que as dimensões humanas e comunicacionais do risco continuam a ser decisivas, mesmo num ambiente altamente tecnologizado (Taha, 2021; Zimba et al., 2025; Daengsi et al., 2022).

Paralelamente, observa-se crescente atenção ao risco associado à digitalização dos pagamentos e à proliferação de ecossistemas *fintech*. A ampliação do número de transações instantâneas, a multiplicação de plataformas móveis e a integração de novos intermediários criaram oportunidades para novas formas de fraude digital, frequentemente baseadas em deteção difícil e em exploração de grandes volumes de dados. A literatura sugere, assim, que a sofisticação do cibercrime acompanha a sofisticação dos modelos de negócio financeiros,

produzindo um ambiente de inovação e vulnerabilidade em simultâneo (Stojanović et al., 2021; Al-Habashneh et al., 2025; Mustapha et al., 2023).

Outro elemento relevante é a crescente preocupação com dependências tecnológicas e infraestruturas partilhadas. Muitos estudos sublinham que a concentração de serviços em certos fornecedores *cloud* ou operadores tecnológicos pode reduzir custos e aumentar eficiência, mas também criar pontos únicos de falha e ampliar o risco sistémico. A ameaça deixa, assim, de ser apenas a intrusão direta numa instituição financeira e passa a incluir falhas e vulnerabilidades em ecossistemas de serviços de que várias instituições dependem (Aldasoro et al., 2022; Uddin et al., 2023; Wang et al., 2024).

2.5 Impactos do cibercrime: da perda direta à vulnerabilidade sistémica

A literatura recente destaca que os impactos do cibercrime financeiro vão muito além das perdas monetárias imediatamente observáveis. Embora o prejuízo direto associado a fraude, indisponibilidade de serviços ou comprometimento de dados continue a ser uma dimensão central, os estudos mais recentes mostram que os custos económicos do cibercrime incluem também despesas de remediação, reforço de segurança, danos reputacionais, efeitos sobre confiança do consumidor e custos de *compliance*. Em certos contextos, estes efeitos acumulados podem revelar-se mais gravosos do que o dano técnico inicial (Uddin et al., 2020; Aldasoro et al., 2022).

No plano organizacional, diversos estudos mostram que o risco cibernético se traduz numa componente crescente do risco operacional das instituições financeiras. A digitalização dos processos e a necessidade de investir continuamente em controlo, auditoria, monitorização e recuperação fazem com que o custo da segurança digital se torne um elemento estrutural da atividade financeira. Esta perspetiva é particularmente relevante numa dissertação integrada em Economia Industrial e de Empresa, pois permite compreender o risco cibernético como variável que afeta eficiência, competitividade e valor económico das organizações (Gatzert & Schubert, 2022; Uddin et al., 2023).

Ao nível sistémico, a literatura enfatiza o papel da interconectividade digital como amplificador de impacto. Os chamados *connected events* e o risco de cauda (*tail risk*) aparecem recorrentemente associados a cenários em que múltiplas instituições são afetadas por incidentes simultâneos ou por dependências comuns. Esta abordagem aproxima o cibercrime financeiro de outras formas de risco sistémico estudadas na literatura financeira, reforçando a necessidade de incluir o risco cibernético nas análises de estabilidade e supervisão (Aldasoro et al., 2022; Krishna et al., 2023).

A confiança surge também como variável económica crítica. Num setor assente na credibilidade institucional e na continuidade das transações, a perceção de insegurança pode reduzir adoção de serviços digitais, comprometer relações com clientes e afetar a disposição de utilização de canais inovadores. Em consequência, a literatura mostra que segurança digital e confiança económica estão estreitamente ligadas, especialmente em contextos de banca móvel, pagamentos eletrónicos e inclusão financeira digital (Al-Habashneh et al., 2025; Krishna et al., 2023; Shafie, 2025).

2.6 Regulação, governação e resposta institucional

O crescimento do risco cibernético no setor financeiro tem sido acompanhado por um reforço progressivo das respostas institucionais e regulatórias. A literatura recente documenta o desenvolvimento de estratégias nacionais de cibersegurança, o reforço de mecanismos de reporte de incidentes, a crescente atenção dada à segurança de cadeias de fornecimento e a formulação de quadros regulatórios mais exigentes, tanto a nível europeu como internacional (Vandezande, 2024; Aslam et al., 2022; Cojocaru, 2025).

No contexto europeu, a regulação recente demonstra uma clara orientação para a harmonização e para a resiliência operacional digital. Embora a literatura trate diferentes instrumentos com graus variados de detalhe, é recorrente a ideia de que o setor financeiro deixou de ser abordado apenas através de normas prudenciais clássicas e passou a ser alvo de uma regulação mais específica em matéria de risco digital. A ênfase em gestão do risco TIC, *incident reporting*,

testes de resiliência e supervisão de dependências críticas traduz uma nova fase da resposta institucional ao problema (Vandezande, 2024; van der Kleij et al., 2021).

Ao nível das organizações, a literatura evidencia igualmente a crescente institucionalização do risco cibernético. Este processo manifesta-se através da integração do tema nos relatórios anuais, nos sistemas de controlo interno, nas funções de auditoria e nos modelos de *governance*. A segurança digital passa, assim, a fazer parte do discurso formal de gestão e da arquitetura organizacional das instituições financeiras. Esta institucionalização é particularmente relevante, pois sinaliza que o risco deixou de ser tratado como questão lateral de tecnologia e passou a ser entendido como responsabilidade de topo e dimensão central da sustentabilidade organizacional (Gatzert & Schubert, 2022; Cojocaru, 2025).

2.7 Resiliência digital como novo paradigma

Um dos desenvolvimentos mais relevantes identificados na literatura é a ascensão do conceito de resiliência digital como paradigma dominante de resposta ao risco cibernético. Ao contrário de abordagens centradas unicamente em prevenção ou conformidade, a resiliência digital pressupõe a capacidade das instituições para continuar a operar, adaptar-se e recuperar mesmo quando ocorrem incidentes. Esta visão torna-se especialmente pertinente no setor financeiro, onde a continuidade de serviço e a confiança no sistema são cruciais (Annarelli et al., 2020; van der Kleij et al., 2021).

A literatura mostra que esta resiliência é construída em diferentes níveis. Num primeiro nível, surge a dimensão humana, com destaque para formação, sensibilização e criação de cultura organizacional orientada para segurança. Num segundo nível, destaca-se a capacidade operacional, incluindo planos de resposta a incidentes, estruturas de coordenação e aprendizagem organizacional. Num terceiro nível, surgem soluções técnicas, como sistemas de deteção baseados em aprendizagem automática, autenticação reforçada e monitorização contínua. Num quarto nível, mais estrutural, emergem modelos

arquiteturais como *Zero Trust* e tecnologias de registo distribuído que procuram reforçar confiança e integridade em ambientes financeiros digitais (Daengsi et al., 2022; Hillman et al., 2023; Dasgupta et al., 2022; Daah et al., 2024; Tsai, 2023).

A literatura não sugere que estas dimensões sejam alternativas entre si. Pelo contrário, verifica-se consenso crescente de que a resiliência digital resulta precisamente da combinação entre tecnologia, processos, arquitetura e comportamento organizacional. Esta leitura é especialmente importante para a presente dissertação, uma vez que permite articular o debate sobre segurança com as dimensões económicas e institucionais próprias do setor financeiro (Annarelli et al., 2020; Daah et al., 2024; Raddatz et al., 2023).

2.8 Posicionamento da dissertação na literatura existente

A literatura revista demonstra que o estudo do cibercrime financeiro se expandiu consideravelmente nos últimos anos, mas também revela um campo ainda marcado por forte fragmentação disciplinar. Existem estudos técnicos muito desenvolvidos sobre deteção de fraude, *phishing*, intrusão e *malware*, bem como trabalhos económicos sobre custo e risco operacional, análises regulatórias sobre enquadramento institucional e estudos organizacionais sobre *governance* e resposta a incidentes. No entanto, observa-se frequentemente que estas abordagens se desenvolvem em paralelo e nem sempre são integradas numa leitura comum do fenómeno (Dasgupta et al., 2022; Gatzert & Schubert, 2022; Vandezande, 2024).

É precisamente nesse ponto que a presente dissertação procura contribuir. Ao combinar revisão estruturada da literatura com leitura qualitativa aprofundada de artigos em texto integral, o estudo propõe uma abordagem capaz de articular resultados oriundos de perspetivas técnicas, económicas, regulatórias e organizacionais. A escolha do setor financeiro como foco reforça a pertinência da investigação, dado tratar-se de um espaço onde a digitalização, a interdependência, o risco sistémico e a pressão regulatória convergem de forma particularmente intensa.

Além disso, ao ser desenvolvida no âmbito do Mestrado em Economia Industrial e de Empresa, a dissertação posiciona-se numa interseção entre economia, gestão e cibersegurança, contribuindo para compreender o risco digital não apenas como questão tecnológica, mas como elemento estruturante do funcionamento dos mercados, da competitividade das organizações e da estabilidade financeira (Gatzert & Schubert, 2022; Uddin et al., 2023).

2.9 Posicionamento da dissertação face às revisões estruturadas existentes

A literatura recente sobre cibercrime, cibersegurança e risco digital no setor financeiro inclui já um conjunto relevante de revisões sistemáticas e revisões estruturadas, sobretudo em domínios mais especializados, como as ameaças em ecossistemas *FinTech*, o panorama de riscos associados à digitalização financeira e os mecanismos biométricos de reforço da segurança bancária. A comparação com esses trabalhos é importante, não apenas para situar esta dissertação no estado da arte, mas também para clarificar o seu contributo específico.

Entre os estudos mais diretamente comparáveis, destaca-se o trabalho de Javaheri et al. (2024), que se apresenta explicitamente como uma *systematic review* e aplica a metodologia PRISMA para examinar ameaças e estratégias defensivas no ecossistema *FinTech*. A partir de 74 estudos selecionados, os autores identificam 11 ameaças centrais e 9 estratégias defensivas, propondo uma taxonomia refinada do risco cibernético em *FinTech*. Este contributo é particularmente relevante para o eixo das tipologias de ameaça, uma vez que sistematiza vetores tecnológicos, humanos e procedimentais. No entanto, o foco do artigo permanece circunscrito ao universo *FinTech* e à classificação das ameaças e defesas, não abrangendo de forma aprofundada os impactos económicos, a governação regulatória ou a resiliência digital no setor financeiro em sentido mais amplo.

Também relevante é a revisão de Jain et al. (2023), apresentada como *systematic literature review* sobre o *risk landscape in fintech*. Com base em 84 artigos recuperados na Scopus, o estudo combina análise bibliométrica e análise de conteúdo para mapear tendências de publicação, principais temas e categorias de risco ligadas à inovação financeira digital. A sua principal contribuição reside no facto de mostrar a centralidade crescente do risco no debate sobre *FinTech* e de identificar áreas emergentes de investigação.

Contudo, o artigo apresenta uma orientação mais próxima de uma revisão bibliométrica do campo do que de uma análise integrada do cibercrime financeiro. A ênfase recai sobre a configuração do campo científico e sobre a categorização do risco em *FinTech*, mais do que sobre os efeitos económicos, institucionais e operacionais do fenómeno.

Por sua vez, Khan et al. (2023) realizam uma *systematic literature review* centrada no papel da biometria no reforço da cibersegurança no setor bancário. O estudo seleciona 101 artigos e organiza a análise em torno de quatro questões de investigação, relacionadas com tipos de biometria, aplicações em *FinTech*, benefícios e reforço dos sistemas bancários existentes. A revisão é particularmente útil para o eixo dos mecanismos de resiliência digital, na medida em que confirma a centralidade crescente da autenticação biométrica como camada adicional de proteção em ambientes bancários digitais. Ainda assim, trata-se de um estudo tematicamente muito mais delimitado do que a presente dissertação, uma vez que o seu foco recai quase exclusivamente sobre biometria e autenticação, sem integrar o problema mais vasto do cibercrime no setor financeiro.

A comparação com estes trabalhos permite clarificar o posicionamento da presente dissertação. Em primeiro lugar, o seu objeto é mais amplo. Enquanto as revisões estruturadas referidas se concentram em *FinTech*, em landscapes de risco ou em biometria, esta dissertação analisa o setor financeiro em sentido mais lato, incluindo banca, instituições financeiras, pagamentos digitais, *fintech* e infraestruturas de mercado. Em segundo lugar, o seu enquadramento é mais integrador. Em vez de se focar numa única dimensão do problema, a dissertação articula quatro eixos analíticos: tipologias de ameaça, impactos económicos, respostas institucionais e regulatórias e mecanismos de resiliência digital de modo a construir uma leitura transversal do fenómeno. Em terceiro lugar, o trabalho assume uma orientação explícita no âmbito da Economia Industrial e de Empresa, tratando o risco cibernético como determinante da eficiência, da competitividade, da governação e da estabilidade do setor financeiro.

Deste modo, a presente dissertação não surge como repetição das revisões estruturadas já existentes, mas como tentativa de síntese de nível superior, capaz de integrar resultados que a literatura tende a tratar separadamente. Se trabalhos como os de Javaheri et al. ajudam a compreender a diversidade das ameaças em *FinTech*, Jain et al. contribuem para mapear o campo dos riscos em *fintech*, e Khan et al. aprofundam a biometria como mecanismo de segurança bancária, esta dissertação procura responder a uma questão mais abrangente: o que revela a literatura científica recente sobre a evolução, o impacto e a mitigação do cibercrime no setor financeiro entre 2020 e 2026?. É precisamente nesta articulação entre ameaça, impacto, regulação e resiliência que reside o seu principal contributo.

Por fim, esta comparação também ajuda a clarificar a natureza metodológica do trabalho. As revisões estruturadas referidas aplicam protocolos formais de seleção, frequentemente identificados como SLR ou enquadrados por PRISMA. A presente dissertação, embora se inspire em práticas de revisão estruturada e sistematização bibliográfica, assume antes a forma de uma revisão estruturada da literatura com triangulação temática, orientada para interpretação integrada de um corpus alargado de estudos. Esta diferença metodológica não diminui a sua relevância; pelo contrário, é coerente com a ambição de construir uma leitura mais transversal do problema, compatível com a natureza multidimensional do cibercrime no setor financeiro.

3. Metodologia

3.1 Enquadramento metodológico

A presente dissertação adota uma abordagem metodológica de natureza qualitativa, apoiada por procedimentos de sistematização bibliográfica e análise temática da literatura científica. O desenho metodológico combina pesquisa estruturada em bases de dados académicas indexadas, seleção criteriosa de artigos científicos e leitura analítica aprofundada dos estudos considerados mais relevantes para responder à pergunta de investigação. Esta opção metodológica

é particularmente adequada a um objeto como o cibercrime no setor financeiro, cuja compreensão exige a articulação entre dimensões tecnológicas, económicas, organizacionais e regulatórias.

A metodologia procura articular duas exigências complementares. Por um lado, uma dimensão de mapeamento e seleção, orientada para identificar estudos recentes e relevantes no domínio do cibercrime financeiro. Por outro, uma dimensão interpretativa, dirigida à leitura aprofundada dos artigos selecionados, à comparação entre resultados e à construção de uma narrativa analítica coerente. Assim, a investigação não se limita a inventariar literatura, procurando antes organizar e interpretar a produção científica recente em torno de relações, tendências e implicações para o setor financeiro.

O objetivo central da investigação consiste em compreender o que revela a literatura científica recente sobre a evolução, o impacto e a mitigação do cibercrime no setor financeiro entre 2020 e 2026. Para esse efeito, a análise foi organizada em torno de quatro eixos analíticos: tipologias de ameaça, impactos económicos, respostas institucionais e regulatórias e mecanismos de resiliência digital. Estes eixos não foram definidos apenas como categorias *ex post*, mas funcionaram como critérios efetivos de pesquisa, triagem, extração de dados e interpretação dos resultados.

3.2 Estratégia de pesquisa bibliográfica

A pesquisa bibliográfica foi realizada em duas bases de dados académicas de referência: *Web of Science Core Collection* e Scopus. A utilização combinada destas duas bases teve como objetivo assegurar maior cobertura documental, reduzir o risco de omissão de estudos relevantes e reforçar a consistência do corpus final. Esta opção é particularmente adequada em áreas interdisciplinares como finanças, gestão, tecnologia e cibersegurança, nas quais a literatura relevante pode estar distribuída por revistas e campos científicos distintos.

Na *Web of Science Core Collection*, a pesquisa foi realizada através da funcionalidade de pesquisa avançada. Para a identificação da literatura

relevante, foi utilizado o campo *Topic* (TS), que inclui o título, o resumo, as palavras-chave dos autores e as *Keywords Plus*. A estratégia de pesquisa combinou termos relacionados com cibercrime, cibersegurança e risco digital com termos associados ao setor financeiro, recorrendo a operadores booleanos e truncaturas para ampliar a recuperação de variantes lexicais.

A expressão de pesquisa de base foi estruturada da seguinte forma:

TS=(
("*cybercrime*" *OR* "*cyber attack**" *OR* "*cybersecurity*" *OR* "*cyber risk*") *AND*
("*financial sector*" *OR banking OR* "*financial institution**" *OR fintech OR* "*digital payment**" *OR* "*mobile banking*")
)

De forma complementar, foi utilizada uma estratégia equivalente na base Scopus, recorrendo ao campo *TITLE-ABS-KEY*, que permite pesquisar simultaneamente no título, no resumo e nas palavras-chave. A expressão base foi adaptada à sintaxe da plataforma da seguinte forma:

TITLE-ABS-KEY(
("*cybercrime*" *OR* "*cyber attack**" *OR* "*cybersecurity*" *OR* "*cyber risk*") *AND*
("*financial sector*" *OR banking OR* "*financial institution**" *OR fintech OR* "*digital payment**" *OR* "*mobile banking*")
)

Neste sentido, foram utilizados termos associados ao domínio da cibersegurança e do cibercrime, designadamente "*cybercrime*", *"cyber attack", "cybersecurity" e "cyber risk", combinados com expressões representativas do universo financeiro, como "financial sector", "banking", *"financial institution", "fintech", "digital payment"* e "*mobile banking*". A utilização de operadores booleanos e truncaturas permitiu ampliar a recuperação de variantes lexicais e aumentar a sensibilidade da pesquisa, sem comprometer a coerência temática

do corpus. Esta formulação foi concebida para identificar estudos com ligação direta a ameaças cibernéticas, fraude digital, resiliência operacional, regulação e segurança em serviços financeiros digitalizados.

3.3 Processo de seleção dos artigos

A pesquisa inicial realizada no *Web of Science Core Collection* identificou 907 registos. Numa fase seguinte, foram aplicados filtros de refinamento relacionados com o período temporal, o tipo de documento, o idioma e a relevância temática, reduzindo o conjunto para 284 registos. Estes filtros permitiram excluir documentos pouco ajustados ao problema de investigação e concentrar a atenção em estudos com maior potencial de contributo para a análise.

No caso na pesquisa através do Scopus, esta identificou inicialmente 1018 registos. Após aplicação dos filtros relacionados com o período temporal, a relevância temática e a natureza científica das publicações, o conjunto foi reduzido para 383 artigos.

Após esta etapa, procedeu-se à triagem dos resultados com base no título, resumo e palavras-chave, com o objetivo de selecionar apenas os estudos com ligação direta ao cibercrime no setor financeiro. Foram privilegiados artigos que abordassem explicitamente temas como risco cibernético, fraude digital, *phishing*, resiliência digital, regulação, *governance*, banca, *fintech*, pagamentos digitais e instituições financeiras.

Foram excluídos os estudos que incidiam exclusivamente sobre cibersegurança em geral, sem ligação ao setor financeiro, bem como os trabalhos centrados em finanças sem relação clara com risco digital. A partir deste processo, foram selecionados 25 artigos da *Web of Science* para integração no corpus da dissertação.

Paralelamente, foram também integrados 45 artigos obtidos através da base Scopus, selecionados com base na mesma lógica temática e submetidos aos mesmos critérios de inclusão e exclusão. O recurso à Scopus permitiu reforçar a cobertura documental da investigação e incorporar estudos que, embora relevantes para o objeto de análise, não surgiam com a mesma visibilidade no *Web of Science*. Em conjunto, os artigos provenientes das duas bases constituem o corpus final de 70 artigos científicos, que sustenta a análise interpretativa desenvolvida no Capítulo 4.

O processo de seleção seguiu uma lógica inspirada no modelo PRISMA (*Preferred Reporting Items for Systematic Reviews and Meta-Analyses*), entendido aqui como referência para garantir

transparência nas etapas de identificação, filtragem, triagem e elegibilidade dos estudos. Na secção dos anexos deste trabalho encontra-se um fluxograma PRISMA.

3.4 Critérios de inclusão e exclusão

Os critérios de inclusão adotados nesta investigação privilegiaram estudos com ligação direta ao setor financeiro, nomeadamente banca, instituições financeiras, *fintech*, pagamentos digitais e *mobile banking*, desde que associados a temas como cibercrime, cibersegurança, *cyber risk*, fraude, *phishing*, resiliência ou regulação.

Foram incluídos artigos publicados no período temporal definido para a investigação e considerados relevantes para pelo menos uma das dimensões analíticas da dissertação. Procurou-se privilegiar estudos com contributo efetivo para a discussão do problema de investigação, quer através de evidência empírica, quer por via de enquadramento teórico, técnico ou regulatório diretamente aplicável ao setor financeiro.

Em contrapartida, foram excluídos artigos excessivamente gerais sobre cibersegurança, estudos puramente técnicos sem aplicação ao setor financeiro e trabalhos sem alinhamento temático claro com o problema de investigação.

Foram igualmente excluídos textos cuja relação com o setor financeiro fosse apenas tangencial, sem contributo substantivo para os objetivos analíticos da dissertação.

3.5 Organização e tratamento dos resultados

Os registos selecionados foram exportados do *Web of Science* e da Scopus para folha de cálculo, permitindo a sua organização e triagem estruturada. Para cada artigo foram registados elementos como título, autores, ano de publicação, revista, DOI e decisão de inclusão.

Numa fase posterior, os estudos considerados mais relevantes foram classificados de acordo com o seu contributo principal para a investigação. Esta reformulação assume um corpus final único de 70 artigos, distribuído de acordo com o eixo analítico predominante de cada estudo. Esta solução melhora a coerência interna do capítulo e evita a sobreposição entre diferentes estatutos documentais.

Depois de selecionados, os artigos do corpus final foram organizados segundo os quatro eixos analíticos definidos na investigação: tipologias de ameaça, impactos económicos, respostas institucionais e regulatórias e mecanismos de resiliência digital. Esta classificação permitiu estruturar a análise qualitativa e garantir maior coerência entre a metodologia e a discussão desenvolvida no capítulo seguinte.

3.6 Procedimentos de extração e análise dos dados

A análise dos artigos selecionados foi conduzida através de análise temática qualitativa, orientada pelos quatro eixos analíticos da investigação. Após a leitura integral dos estudos incluídos no corpus final, procedeu-se à identificação dos principais temas, resultados, conceitos e tendências presentes na literatura.

A análise procurou não apenas descrever os conteúdos dos artigos, mas também compará-los, identificar convergências e divergências e extrair implicações relevantes para o setor financeiro. Esta abordagem permitiu articular estudos de natureza metodológica diversa — incluindo revisões sistemáticas, análises econométricas, estudos de caso, análises regulatórias e investigações técnicas — e construir uma interpretação integrada do fenómeno do cibercrime financeiro. A triangulação temática mantém-se, assim, como princípio orientador da leitura interpretativa do corpus.

Sempre que os artigos apresentavam dados quantitativos relevantes, como amostras, percentagens, métricas de desempenho, perdas monetárias, coeficientes estatísticos ou indicadores de risco, esses elementos foram registados e posteriormente mobilizados para densificar a discussão. Esta opção foi particularmente importante para a construção do Capítulo 4, no qual cada eixo analítico inclui uma secção específica de dados quantitativos, permitindo reforçar a robustez empírica da análise sem abandonar o caráter predominantemente qualitativo da dissertação.

3.7 Composição do corpus analisado

O corpus final desta investigação é constituído por 70 artigos científicos, dos quais 25 resultam da pesquisa no *Web of Science Core Collection* e 45 foram obtidos através da Scopus. Este corpus foi considerado suficientemente abrangente para captar a diversidade temática da literatura recente sobre cibercrime no setor financeiro, ao mesmo tempo que preserva condições de leitura aprofundada e análise comparada.

Tabela 1 - Distribuição dos artigos pelos eixos analíticos

Eixo analítico	Número de artigos	Percentagem
Tipologias de ameaça	13	18,6%

Eixo analítico	Número de artigos	Percentagem

Impactos económicos	14	20,0%
Respostas institucionais e regulatórias	14	20,0%
Mecanismos de resiliência digital	29	41,4%
Total	**70**	**100,0%**

Fonte: Elaboração própria.

A distribuição do corpus final por eixo analítico evidencia uma maior concentração de estudos no eixo dos mecanismos de resiliência digital, com 29 artigos (41,4%), seguido dos impactos económicos e das respostas institucionais e regulatórias, ambos com 14 artigos (20,0%), e, por fim, das tipologias de ameaça, com 13 artigos (18,6%). Esta distribuição sugere que a literatura selecionada privilegia sobretudo abordagens orientadas para deteção, prevenção, mitigação e resposta a incidentes, sem descurar os impactos económicos e o enquadramento institucional do cibercrime no setor financeiro.

3.8 Validação e controlo de qualidade

Para reduzir possíveis enviesamentos interpretativos, foram adotadas várias estratégias de validação ao longo do processo analítico. A classificação temática dos artigos foi sempre fundamentada em evidência explícita presente nos próprios textos, e não apenas em títulos, palavras-chave ou impressões gerais de leitura. Procurou-se igualmente garantir equilíbrio entre diferentes tipos de investigação, evitando uma leitura excessivamente centrada em abordagens técnicas, económicas ou regulatórias isoladamente. A integração de estudos sobre bancos, *fintech*, pagamentos digitais, *blockchain*, *phishing*, fraude e

resiliência operacional contribuiu para preservar a natureza multidimensional do objeto analisado.

A utilização combinada de duas bases de dados de grande cobertura, *Web of Science* e Scopus, funcionou também como mecanismo de controlo de qualidade, uma vez que permitiu comparar resultados, reduzir dependência de uma única base e ampliar a probabilidade de inclusão de estudos relevantes.

3.9 Limitações metodológicas

Apesar da consistência do procedimento adotado, importa reconhecer algumas limitações. Em primeiro lugar, a pesquisa bibliográfica foi realizada apenas em duas bases de dados — *Web of Science Core Collection* e Scopus, o que significa que estudos relevantes indexados noutras plataformas podem não ter sido captados. Ainda assim, esta opção permitiu garantir maior controlo da qualidade e comparabilidade do material selecionado.

Em segundo lugar, o corpus final é composto por 70 artigos, número que permite uma análise qualitativa robusta, mas que naturalmente não esgota a totalidade da produção científica recente sobre cibercrime no setor financeiro. A escolha privilegiou relevância temática e consistência analítica em detrimento de uma cobertura extensiva indiscriminada.

Por fim, os estudos incluídos apresentam metodologias muito diversas, variando entre revisões sistemáticas, análises econométricas, estudos qualitativos, investigações técnicas e análises regulatórias. Embora esta heterogeneidade constitua uma vantagem para a compreensão ampla do fenómeno, também limita a comparabilidade direta entre resultados e exige prudência na formulação de inferências gerais.

3.10 Síntese metodológica

Em síntese, a metodologia desta dissertação assenta numa revisão estruturada da literatura científica recente, realizada a partir do *Web of Science Core Collection* e da Scopus, seguida de triagem temática e análise qualitativa

aprofundada de um corpus final de 70 artigos científicos. O processo metodológico procurou assegurar coerência entre a pergunta de investigação, a estratégia de pesquisa, os critérios de seleção e a organização analítica dos resultados.

A classificação dos estudos segundo quatro eixos analíticos permitiu estruturar a discussão do Capítulo 4 e construir uma leitura integrada da literatura recente sobre cibercrime no setor financeiro. Deste modo, o Capítulo 3 estabelece a base metodológica da dissertação e assegura a ligação entre o processo de seleção bibliográfica e a análise interpretativa desenvolvida nos capítulos seguintes.

4 Análise e Discussão dos Resultados

4.1 Introdução

O presente capítulo analisa os resultados da revisão estruturada da literatura científica sobre cibercrime no setor financeiro, organizando a discussão em torno de quatro eixos analíticos: tipologias de ameaça, impactos económicos, respostas institucionais e regulatórias e mecanismos de resiliência digital. Esta estrutura permite compreender o fenómeno não como um conjunto disperso de incidentes técnicos, mas como uma realidade transversal à transformação digital da banca, dos pagamentos digitais, das *fintech* e das infraestruturas financeiras (Nefla & Jellouli, 2025; Uddin et al., 2020; Wang et al., 2024).

A literatura analisada mostra que a digitalização do setor financeiro ampliou simultaneamente eficiência e vulnerabilidade. A expansão do *mobile banking*, da *cloud*, das APIs, dos sistemas de pagamento em tempo real e das soluções de inteligência artificial aumentou a capacidade de escala e a conveniência dos serviços, mas criou também novas superfícies de ataque, novas dependências tecnológicas e novas exigências de governação do risco (Daah et al., 2024; Dubauskas & Išoraitė, 2025; Türegün, 2025).

Neste enquadramento, o cibercrime deixa de poder ser tratado como uma questão periférica de segurança informática. Ele passa a constituir uma variável estrutural da continuidade operacional, da competitividade, da confiança do utilizador e da estabilidade do próprio setor financeiro, exigindo abordagens integradas que articulem prevenção, deteção, resposta, regulação e adaptação institucional (Aldasoro et al., 2022; Ragazzo et al., 2025; Uddin et al., 2020).

4.2 Tipologias de ameaça no setor financeiro

A literatura revela que as ameaças predominantes no setor financeiro se distribuem por vários núcleos interligados, dos quais se destacam o *phishing*, o *smishing*, o *ransomware*, a fraude em pagamentos digitais, os ataques a aplicações móveis e *web*, o comprometimento de terceiros tecnológicos e os ataques a infraestruturas críticas. Em vez de surgirem como riscos isolados, estas ameaças tendem a combinar vetores técnicos, humanos e organizacionais, refletindo a crescente complexidade do ecossistema financeiro digital (Ahmed et al., 2021; Birthriya & Jain, 2022; Javaheri et al., 2024).

Entre estas ameaças, o *phishing* mantém uma centralidade particular. A literatura mostra que o seu sucesso decorre da exploração da confiança institucional, da capacidade de imitação de comunicações legítimas e da combinação com outros esquemas de fraude, como roubo de credenciais, engenharia social e *malware*. Esta persistência explica por que razão o *phishing* continua a ser uma das formas mais recorrentes de entrada no sistema financeiro digital, afetando utilizadores, trabalhadores e instituições (Doshi et al., 2023; Duarte et al., 2025; Taha, 2021).

As ameaças também se estendem ao universo dos pagamentos móveis, do *mobile banking* e das aplicações *fintech*. Nestes ambientes, a combinação entre elevada conveniência, autenticação distribuída, interoperabilidade e uso intensivo de dispositivos móveis cria vulnerabilidades específicas, sobretudo relacionadas com *spoofing*, *sniffing*, *malware*, permissões excessivas em aplicações e ataques a autenticação. A literatura sugere que estas ameaças são particularmente relevantes porque afetam diretamente canais de relação quotidiana entre cliente e instituição (Ahmed et al., 2021; Seraj et al., 2024; Tsai et al., 2024).

Outro vetor importante decorre das dependências de ecossistema. A expansão do *open banking*, da *cloud*, do *outsourcing* tecnológico e das integrações com *fintech* e fornecedores críticos desloca parte significativa da vulnerabilidade para fora da fronteira formal do banco. Assim, o risco cibernético assume uma natureza ecossistémica: falhas de terceiros, vulnerabilidades de software, deficiências de governação de fornecedores e interdependências em cadeia tornam-se parte integrante da ameaça financeira (Aldasoro et al., 2022; Ragazzo et al., 2025; Vandezande, 2024).

Por fim, a literatura recente chama atenção para ameaças com potencial mais amplo sobre

infraestruturas financeiras críticas, incluindo sistemas de pagamento, bancos centrais, redes interbancárias, plataformas *blockchain* e estruturas de liquidação. Nestes casos, o problema deixa de ser apenas o prejuízo sobre uma entidade individual e passa a ser a possibilidade de interrupção de funções essenciais do sistema financeiro. É precisamente esta possibilidade que aproxima o cibercrime financeiro de preocupações de estabilidade sistémica (Ragazzo et al., 2025; Smaga, 2026; Tsantikidou & Sklavos, 2024).

4.2.1 Dados quantitativos do eixo das tipologias de ameaça

Os dados quantitativos reforçam a gravidade e a escala destas ameaças. Segundo a análise sobre a NIS2, 22% das empresas da União Europeia reportaram consequências associadas a incidentes TIC em 2021, quando em 2018 esse valor era de 12%; no mesmo período, os ataques de *ransomware* cresceram 41% em 2022 e os ataques por *e-mail*, incluindo *phishing*, aumentaram 48%. Estes dados confirmam a intensificação do risco digital e a maior pressão sobre setores críticos, incluindo o financeiro (Vandezande, 2024).

No *phishing*, os estudos mostram resultados particularmente expressivos. Um sistema de deteção baseado em arquitetura *dual-layer* alcançou *accuracy* de 99,51%, *recall* de 99,68%, *precision* de 99,5% e F1-*score* de 99,52% na classificação de e-mails de *phishing* e *spam*. Já o modelo de Taha, baseado em *weighted soft voting*, obteve *accuracy* de 95% e *AUC* de 98,8% na deteção de *websites* de *phishing*. Mais recentemente, Duarte et al. (2025) obtiveram *recall* de 96,02% e *accuracy* de 97,28% na deteção precoce de URLs de *phishing* em *parked domains* aplicados a uma instituição financeira (Doshi et al., 2023; Duarte et al., 2025; Taha, 2021).

Nos sistemas móveis e no setor financeiro digital, a pressão também é elevada. Ahmed et al. (2021) referem que, em muitos países em desenvolvimento, o numerário ainda representa mais de 90% dos pagamentos, mas a migração para sistemas móveis aumenta o valor estratégico da segurança desses canais. Seraj et al. (2024), trabalhando com um *dataset* de 1650 aplicações maliciosas de *mobile banking* e aplicações benignas do Google Play, reportam accuracies de 99,7% com *ANN*/ *CNN* e 99,6% com *DNN* na deteção de *malware* em *mobile banking* (Ahmed et al., 2021; Seraj et al., 2024).

A literatura sobre ameaças em *FinTech* mostra ainda que o setor finance *and* insurance é um dos mais visados pelos atacantes desde 2018. Javaheri et al. (2024) sublinham que, entre fevereiro e abril de 2020, os ataques ao setor financeiro subiram 238% e 80% das instituições financeiras reportaram aumento

dos ataques. Estes dados sugerem que a transformação digital do setor não apenas aumenta a exposição, mas também acelera a sofisticação e a frequência dos vetores de ameaça (Javaheri et al., 2024).

Em síntese, os dados quantitativos do eixo das tipologias de ameaça confirmam que o setor financeiro enfrenta um padrão de risco particularmente intenso, diversificado e em rápida evolução. A frequência elevada de ataques, o crescimento expressivo do phishing, do ransomware e da fraude digital, bem como a incidência sobre mobile banking, fintech e infraestruturas críticas, mostram que a ameaça cibernética deixou de ser episódica para se tornar estrutural. Estes resultados reforçam a ideia de que a transformação digital do setor financeiro, ao mesmo tempo que amplia eficiência e conveniência, multiplica superfícies de ataque e expõe instituições e utilizadores a formas cada vez mais sofisticadas de exploração.

Esta tabela lista os artigos analisados:

Tabela 2 - Artigos que se enquadram no eixo das tipologias de ameaças

Autor / Ano	Tema principal	Descrição do contributo do artigo	Área geográfica
Javaheri et al. (2024)	Ameaças cibernéticas em *FinTech*	Realiza uma revisão sistemática da literatura sobre ameaças cibernéticas em *FinTech*, identificando uma taxonomia de riscos tecnológicos, humanos e procedimentais no	Global

		ecossistema financeiro digital.	
Darem et al. (2023)	Classificação de ciberameaças no setor bancário e financeiro	Classifica as ameaças cibernéticas no setor bancário segundo severidade e tecnicidade, abrangendo *ransomware*, *phishing*, *DDoS*, *data breaches* e outras formas de ataque.	Global
Jain et al. (2023)	Panorama de riscos em *FinTech*	Revê a literatura sobre o *risk landscape* em *FinTech*, mostrando como a digitalização financeira ampliou o peso do cibercrime, da assimetria tecnológica e dos riscos operacionais.	Global
Jović & Nikolić (2022)	Novos riscos emergentes em *FinTech*	Analisa a expansão de riscos associados à inovação financeira digital, com ênfase na emergência de novas vulnerabilidades técnicas,	Global
		operacionais e organizacionais.	

Kuzior et al. (2022)	Tendências de cibercrime em instituições financeiras	Examina padrões e tendências informacionais do cibercrime em instituições financeiras, destacando a evolução das ameaças dirigidas ao setor.	EUA / internacional
Smaga (2026)	Tendências de ataques a bancos centrais	Estuda ataques dirigidos a bancos centrais e identifica padrões de evolução do *threat landscape* contra infraestruturas financeiras críticas.	Global
Birthriya & Jain (2022)	*Phishing* por *e-mail*	Sistematiza o *phishing* por *e-mail* como vetor central de roubo de credenciais e fraude financeira, mostrando a persistência desta ameaça em ambientes bancários e digitais.	Global

Khiari et al. (2025)	Fraude em criptomoedas	Examina a fraude em mercados de criptomoedas e os seus efeitos sobre a volatilidade, revelando a centralidade da fraude como ameaça no ecossistema financeiro digital.	Global
Kuzmenko et al. (2021)	Cibercrime e inovação no setor financeiro	Relaciona a expansão da inovação financeira e da digitalização com o crescimento do cibercrime, evidenciando novas vulnerabilidades em sistemas financeiros modernos.	União Europeia
Marwan et al. (2022)	*Cybercrime*, *phishing* e *scams* na economia digital	Discute *cybercrime*, *phishing*, *scams* e outras formas de criminalidade digital em ecossistemas com *fintech*, *e-commerce* e serviços digitais.	Indonésia
Mosteanu & Faccia (2021)	*Cyber-threats* em tecnologias emergentes	Enquadra os *cyber-threats* associados a *blockchain*, inteligência artificial e outras tecnologias	Global

	aplicadas à finança	emergentes, realçando riscos estruturais para a indústria financeira.	
Choithani et al. (2024)	IA, criptomoedas e cibersegurança	Analisa ameaças emergentes em sistemas bancários e de criptomoedas sob a influência crescente da inteligência artificial e da digitalização financeira.	Índia / global
Shahzadi et al. (2025)	Riscos personalizados e gamificação em instituições financeiras	Explora riscos de cibersegurança associados à personalização e à gamificação em instituições financeiras, enfatizando vulnerabilidades comportamentais e novas superfícies de ataque.	Global

Fonte: Elaboração própria.

4.3 Impactos económicos do cibercrime financeiro

Os impactos económicos do cibercrime no setor financeiro vão muito além da perda monetária imediata. A literatura mostra que os incidentes cibernéticos produzem custos de remediação, reforço tecnológico, auditoria, litigância, indisponibilidade operacional, pressão regulatória, erosão reputacional e perda de confiança. Por isso, o ciber-risco não deve ser entendido apenas como custo técnico de segurança, mas como variável que afeta a eficiência, a estrutura de custos e a capacidade de intermediação financeira (Aldasoro et al., 2022; Türegün, 2025; Uddin et al., 2020

).

A literatura também sugere que a distribuição do dano económico é assimétrica. Muitos incidentes são relativamente pequenos, mas uma fração reduzida concentra perdas muito elevadas, o que aproxima o ciber-risco de uma lógica de *tail risk*. Além disso, em ambientes altamente digitalizados, o dano económico potencial amplifica-se quando existe forte dependência de *cloud*, terceiros críticos ou infraestruturas comuns, já que o efeito de contágio se torna mais provável (Aldasoro et al., 2022; Smaga, 2026).

Outro impacto relevante é a alteração do próprio comportamento económico do banco. Alguns estudos mostram que o cibercrime afeta recolha de depósitos, oferta de crédito, maturidade do crédito e gestão prudencial da liquidez. Em vez de atuar apenas como custo externo, o ciber-risco altera decisões internas de gestão, podendo induzir mais cautela, mais retenção de liquidez e menor capacidade de expansão creditícia (Boungou, 2023; Uddin et al., 2023).

A digitalização cria ainda uma relação particularmente estreita entre segurança e desempenho. Estudos recentes indicam que bancos que integram estrategicamente medidas de cibersegurança na sua governação e nas suas práticas de divulgação tendem a apresentar melhor desempenho financeiro e maior resiliência institucional. Isto sugere que a cibersegurança pode funcionar não apenas como custo defensivo, mas também como ativo estratégico de credibilidade e robustez (López et al., 2025; Türegün, 2025).

4.3.1 Dados quantitativos do eixo dos impactos económicos

A literatura oferece vários indicadores quantitativos relevantes. Aldasoro et al. (2022), com base em 3705 eventos cibernéticos, mostram que os custos são mais elevados para empresas maiores e para incidentes que afetam várias organizações em simultâneo. Mostram também que o setor financeiro sofre maior número de ataques, embora com custos médios inferiores a outros setores em alguns casos, e que maior despesa em IT está associada a custos futuros menores de incidentes (Aldasoro et al., 2022). Uddin et al. (2020) citam estimativas segundo as quais as perdas anuais do setor bancário podem atingir 97 mil milhões de dólares, cerca de 9% dos lucros líquidos globais da banca em 2016, e referem ainda que a despesa tecnológica dos bancos alcançava 7,16% da receita bruta. Já Wang et al. (2024), citando o Global *Financial Stability Report* 2024 do FMI, referem perdas anuais de 2,5 mil milhões de dólares para os bancos associadas a ciberameaças e mais de 12 mil milhões de dólares em perdas acumuladas em 20 anos, num universo superior a 20.000 ciberataques (Uddin et al., 2020; Wang et al., 2024).

Em termos de efeitos diretos sobre a intermediação bancária, Boungou (2023), usando dados de 2144 bancos norte-americanos entre 2011 e 2019, conclui que os ciberataques reduzem a recolha de depósitos e a oferta de crédito, afetando a intermediação bancária. Jin et al. (2023) mostram, por sua vez, que provisões discricionárias para perdas em empréstimos estão positivamente associadas a futuros ataques cibernéticos e que os bancos tendem a realizar menos *earnings management* após esses incidentes (Boungou, 2023; Jin et al., 2023).

A dimensão macroeconómica também é expressiva. O artigo sobre a NIS2 refere que o custo global do cibercrime terá atingido 5,5 biliões de euros no final de 2020, acima dos 2,7 biliões em 2015, enquanto Kuzior et al. (2022) recordam que o custo médio global de um incidente em 2022 foi de 4,35 milhões de dólares. Estes números ajudam a perceber que o cibercrime financeiro não é apenas um risco microeconómico das instituições, mas também um problema com relevância agregada (Kuzior et al., 2022; Vandezande, 2024).

De forma global, os dados quantitativos sobre impactos económicos demonstram que o

cibercrime no setor financeiro produz efeitos muito mais amplos do que a perda monetária direta. As métricas apresentadas mostram custos significativos ao nível de remediação, desempenho bancário, intermediação financeira, reputação e estabilidade, confirmando que o risco cibernético atua como fator económico permanente da atividade financeira. Assim, os resultados quantitativos sustentam a conclusão de que a cibersegurança deve ser entendida não apenas como custo defensivo, mas como variável com implicações diretas na eficiência, competitividade e robustez económica das instituições financeiras.

Esta tabela lista os artigos analisados:

Tabela 3 - Artigos que se enquadram no eixo dos impactos económicos

Autor / Ano	Tema principal	Descrição do contributo do artigo	Área geográfica
Uddin et al. (2024)	Transformação digital e risco operacional bancário	Demonstra que a digitalização bancária aumenta a exposição ao risco operacional, elevando custos e pressões sobre desempenho e estabilidade bancária.	Comparativo internacional
Aldasoro et al. (2022)	Determinantes e custos do ciber- risco	Analisa custos e determinantes de incidentes cibernéticos, mostrando que eventos maiores e mais interconectados geram perdas económicas mais severas	Estados Unidos / comparativo setorial
Jin et al. (2023)	Ciberataques e *earnings management*	Mostra que ciberataques afetam provisões bancárias e práticas de *earnings management*, revelando efeitos económicos e contabilísticos mensuráveis.	Estados Unidos
Boungou (2023)	Ciberataques e intermediação bancária	Demonstra que os ciberataques reduzem depósitos, alteram a maturidade do crédito e deterioram a função de intermediação bancária.	Estados Unidos
		Relaciona a integração estratégica da cibersegurança com	

Türegün (2025)	Risco cibernético e desempenho financeiro	melhor desempenho financeiro e mostra que incidentes severos deterioram resultados e aumentam custos de remediação	Internacional
Wang et al. (2024)	Cibersegurança e transformação digital bancária	Discute os custos e perdas monetárias gerados pela digitalização acelerada da banca e pelos riscos de privacidade e cibersegurança.	Paquistão / internacional
Gatzert & Schubert (2022)	*Cyber risk management* e valor da firma	Mostra que a formalização da gestão do risco cibernético se associa positivamente ao valor de mercado das instituições financeiras.	Estados Unidos
López et al. (2025)	*Disclosure* e custos de incidentes cibernéticos	Mobiliza dados monetários de incidentes e *disclosure* no setor financeiro, mostrando que a exposição a incidentes e o enquadramento institucional têm efeitos económicos relevantes	Chile / América Latina
Kuznyetsova et al. (2022)	Inclusão financeira e estabilidade	Relaciona inclusão financeira, segurança informacional e estabilidade, mostrando como vulnerabilidades digitais condicionam desempenho económico e financeiro.	Ucrânia / UE
Mhlanga (2020)	IA e inclusão financeira	Analisa o papel da inteligência artificial na inclusão financeira e nos custos e benefícios	

	digital	económicos da digitalização financeira.	Global
Thach et al. (2021)	*Technology quality management* e *banking activities*	Explora a relação entre tecnologia 4.0, ciber-risco e desempenho em atividades bancárias em mercados emergentes	Vietname / mercados emergentes
AL-Habashneh et al. (2025)	Qualidade de aplicações financeiras e satisfação do cliente	Mostra efeitos económicos indiretos da segurança, confiança e privacidade sobre a satisfação e aceitação das aplicações financeiras móveis.	Jordânia
Dubauskas & Išoraitė (2025)	Desenvolvimento bancário, IA, *blockchain* e cibersegurança	Discute efeitos estruturais da inovação tecnológica sobre o desenvolvimento bancário e os custos de adaptação securitária.	Global
Nefla & Jellouli (2025)	Tecnologias emergentes e finança sustentável	Relaciona desafios das tecnologias emergentes com sustentabilidade financeira e custos de gestão do risco digital.	Global

Fonte: Elaboração própria.

4.4 Respostas institucionais e regulatórias

A literatura analisada mostra que o agravamento do risco cibernético no setor financeiro motivou uma mudança gradual, mas nítida, na resposta institucional: de uma lógica centrada na conformidade mínima para uma lógica orientada para resiliência operacional digital. Esta evolução

é importante porque reconhece que a segurança financeira contemporânea depende não apenas da prevenção de incidentes, mas da capacidade de gerir dependências tecnológicas, preservar funções críticas e recuperar de forma coordenada perante disrupções complexas. O ponto decisivo é que a regulação deixa de tratar a cibersegurança como matéria lateral de suporte tecnológico e passa a integrá-la no núcleo da governação prudencial, da continuidade operacional e da proteção sistémica (Cojocaru, 2025; Ragazzo et al., 2025; Vandezande, 2024).

No contexto europeu, DORA, NIS2 e os instrumentos complementares em torno de infraestruturas críticas traduzem esta mudança de paradigma. Em vez de tratar o risco digital como extensão técnica do risco operacional tradicional, a regulação recente passa a exigir enquadramentos explícitos de gestão do risco TIC, reporte estruturado de incidentes, testes de resiliência, gestão do risco associado a terceiros e responsabilização dos órgãos de administração.

O elemento qualitativamente novo não é apenas a existência de mais normas, mas a tentativa de aproximar supervisão prudencial, governação tecnológica e continuidade operacional num mesmo quadro regulatório (Ragazzo et al., 2025; Vandezande, 2024).

A centralidade crescente do *third-party risk* e dos prestadores críticos de *cloud* constitui uma das dimensões mais relevantes desta resposta. A literatura recente insiste em que a concentração tecnológica alterou a natureza do risco financeiro: falhas em poucos fornecedores podem gerar efeitos transversais a múltiplas instituições, convertendo dependências operacionais em vulnerabilidades sistémicas. Daí que a resposta regulatória deixe de poder concentrar-se apenas na instituição supervisionada e tenha de incorporar também cadeias de *outsourcing*, relações contratuais, substituibilidade tecnológica e capacidade de continuidade perante falhas externas (Aldasoro et al., 2022; Ragazzo et al., 2025; Vandezande, 2024).

Ao nível organizacional, a institucionalização do risco cibernético traduz-se na sua integração na governação corporativa, no controlo interno, na auditoria, no *compliance* e nos mecanismos de *disclosure*. Esta evolução é particularmente visível nos estudos sobre relatórios anuais e discurso de gestão, que mostram que o risco digital se tornou responsabilidade de topo e componente da linguagem formal da empresa. A literatura sugere, contudo, que existe diferença entre reconhecer o risco e possuir verdadeira capacidade organizacional para o gerir. O discurso institucional pode

sinalizar maturidade, mas não substitui investimento, coordenação, treino e clareza de responsabilidades (López et al., 2025; Türegün, 2025).

4.4.1 Dados quantitativos do eixo das respostas institucionais e regulatórias

Os indicadores quantitativos deste eixo ajudam a medir a profundidade e a desigualdade das respostas institucionais. No caso da Indonésia, a literatura reporta mais de 150 milhões de utilizadores de internet, 106 *fintechs* registadas em 8/4/2019, transações P2P no valor de IDR 33 biliões (cerca de USD 2 mil milhões), 803 *fintechs* bloqueadas e entre 40 e 50 denúncias mensais de *phishing* num posto policial de Jacarta. Estes números revelam uma resposta estatal reativa, baseada em bloqueio, supervisão e queixa. (Marwan et al., 2022)

No Vietname, um estudo mostra que 43,8% dos bancos tinham certificação de segurança da informação em 2017, contra 27,6% em 2016; 100% tinham *core banking* e 100% *mobile banking*, mas apenas 59,4% possuíam sistemas de gestão de risco. O mesmo artigo refere ainda que, na Coreia, 90% das empresas usam produtos de segurança e 41% usam serviços de segurança, funcionando como contraste internacional de maturidade institucional (Thach et al., 2021).

O estudo comparativo sobre desenvolvimento de políticas nacionais de cibersegurança analisa 7 países e identifica 14 atributos comuns de política cibernética; os EUA lideram em *online banking* policy e o Canadá em *e-commerce* e *spam* policy. Na Ucrânia, o índice de prontidão digital coloca os bancos em 68, face a 78 na UE; em segurança da informação, os bancos ucranianos marcam 81, contra 95 na UE; no uso de tecnologias digitais, 47, contra 96. Estes dados sugerem que a capacidade regulatória e institucional depende da maturidade sistémica do ecossistema digital (Kuznyetsova et al., 2022; Mishra et al., 2022).

No plano europeu, a NIS2 surge num contexto em que 22% das empresas da UE sofreram incidentes em 2021; articula-se com a CER, cobrindo 11 setores críticos, e com a DORA, cobrindo 21 tipos de entidades financeiras. O estudo também refere que a ENISA deve emitir relatórios bienais sobre cibersegurança na UE, o que reforça mecanismos de accountability e supervisão. Já o estudo sobre *cyber risk management* na banca e seguros usa uma amostra de 124 firms e 992

annual *reports*, mostrando que firms com CyberRM têm Tobin's Q 11% superior, com efeitos de 6,37% para bancos e 19,98% para seguradoras. Finalmente, o estudo sobre transformação digital bancária usa 15 entrevistas com especialistas de TI bancária para mostrar como regulação como PCI DSS e GDPR é operacionalizada dentro dos bancos (Gatzert & Schubert, 2022; Vandezande, 2024; Wang et al., 2024).

Os dados quantitativos relativos às respostas institucionais e regulatórias mostram que o agravamento do risco cibernético foi acompanhado por um reforço claro da capacidade regulatória, supervisora e organizacional no setor financeiro. A evolução de indicadores de maturidade institucional, cobertura normativa, exigências de resiliência e integração do risco digital na governação demonstra que as respostas deixaram de se centrar apenas na conformidade formal, passando a refletir uma preocupação crescente com continuidade operacional, controlo de terceiros e supervisão sistémica. Em termos gerais, esta evidência quantitativa confirma que a regulação e a governação do risco digital se tornaram componentes centrais da arquitetura institucional do setor financeiro contemporâneo.

Esta tabela lista os artigos analisados:

Tabela 4 - Artigos que se enquadram no eixo das respostas institucionais e regulatórias

Autor / Ano	Tema principal	Descrição do contributo do artigo	Área geográfica
López et al. (2025)	Divulgação de cibersegurança no setor financeiro	Analisa como a exposição a incidentes, as práticas de *governance* e o contexto regulatório influenciam o *disclosure* bancário em cibersegurança.	Chile / América Latina
Vandezande (2024)	NIS2 e reforço do quadro europeu de cibersegurança	Examina a evolução do quadro europeu de cibersegurança, incluindo NIS2 e a articulação com outras respostas regulatórias relevantes para o setor financeiro.	União Europeia
Gatzert & Schubert (2022)	Gestão do risco cibernético na banca e seguros	Mostra a crescente institucionalização do *cyber risk management* e da consciência do risco cibernético em bancos e seguradoras.	Estados Unidos
Krishna, Krishnan & Sebastian (2023)	Compromisso nacional com a cibersegurança	Demonstra que o compromisso nacional com a cibersegurança funciona como enquadramento institucional favorável à adoção de pagamentos digitais.	Comparativo internacional

Mishra et al. (2022)	Desenvolvimento de políticas nacionais de cibersegurança	Compara atributos de políticas de cibersegurança em sete países e mostra a centralidade do *online banking* e da proteção digital nas respostas públicas.	Comparativo internacional
Mohapatra & Ghosh (2024)	Proteção do investidor e digitalizaçã o financeira	Discute o reforço institucional da proteção do investidor num contexto de digitalização financeira e ciber-risco.	Índia
Gavenaite-Sirvydiene & Miecinskien e (2023)	*Framework* de avaliação de áreas de cibersegurança	Propõe um quadro institucional de avaliação de áreas de cibersegurança no setor financeiro.	Lituânia
Al Batayneh, Qasaimeh & Al- Qassas (2021)	*Governance* da segurança da informação na banca	Desenvolve um sistema de scoring para avaliar *frameworks* de *governance* da segurança da informação no setor bancário.	Jordânia
Bagherifam et al. (2025)	*RegTech*, *SupTech* e governação regulatória digital	Analisa o papel de *RegTech* e *SupTech* na transformação da supervisão financeira e da capacidade regulatória digital.	Global

Ragazzo et al. (2025)	Risco geopolítico e respostas regulatórias na banca	Examina como o risco geopolítico e os ciberataques influenciam a redefinição das respostas regulatórias no setor bancário.	Multinacional
Cojocaru (2025)	Regulação e *governance* para *cyber resilience*	Propõe um quadro teórico para alinhar regulação e *governance* em *cyber resilience* no setor financeiro do Reino Unido.	Reino Unido
Gonçalves et al. (2024)	Gestão de projetos e exigências regulatórias no setor bancário	Analisa metodologias de projeto usadas para cumprir exigências regulatórias no setor bancário nacional.	Brasil
Marwan et al. (2022)	*Digital law* e *good governance policy*	Discute a relação entre *digital law*, *cybercrime* e *good governance* em contexto de expansão *fintech* e economia digital.	Indonésia
Shah & Raj (2025)	CBDC, *blockchain* e parcerias público-privadas	Examina o papel institucional e regulatório de *blockchain* e parcerias público-privadas no desenho e implementação de CBDCs.	Índia

Fonte: Elaboração própria.

4.5 Mecanismos de resiliência digital

A noção de resiliência digital ocupa lugar central na literatura recente porque desloca o debate da simples prevenção para a capacidade de manter funções críticas, absorver perturbações, responder de forma coordenada e recuperar com rapidez. No setor financeiro, esta mudança é especialmente relevante: como a continuidade do serviço, a confiança do utilizador e a estabilidade do sistema dependem da disponibilidade permanente das infraestruturas, a questão

principal deixa de ser se os incidentes podem ocorrer e passa a ser em que medida as instituições conseguem limitar o dano e restaurar a operação. Em termos analíticos, a resiliência surge como resposta à insuficiência de uma visão puramente defensiva da segurança (Annarelli et al., 2020; Gavenaite-Sirvydiene & Miecinskiene, 2023).

Um primeiro plano de resiliência é humano e cultural. A literatura sobre *phishing* em contexto bancário mostra de forma consistente que treino, simulações, *reporting* interno, aprendizagem organizacional e apoio ao cliente reduzem a vulnerabilidade a ataques de engenharia social e melhoram a deteção precoce de sinais suspeitos. Esta conclusão corrige uma visão excessivamente tecnocêntrica da segurança financeira: trabalhadores e utilizadores não são apenas fonte de risco, podendo tornar-se sensores organizacionais importantes quando existe cultura de segurança, rotinas de reporte e feedback institucional (Daengsi et al., 2022; Hillman et al., 2023).

Um segundo plano é operacional e de governação. A literatura mostra que a resiliência depende da existência de processos claros de triagem, contenção, escalonamento, comunicação, continuidade e recuperação. O estudo empírico de Tariq et al. é particularmente ilustrativo ao mostrar que, entre as funções do *framework* NIST, as dimensões detect e respond assumem os efeitos mais fortes sobre a prevenção da fraude bancária. Em termos qualitativos, isto significa que instituições resilientes não são apenas as que tentam impedir a intrusão, mas as que conseguem operar bem sob incerteza (Tariq et al., 2024; van der Kleij et al., 2022).

O terceiro plano é técnico-analítico. Sistemas baseados em *machine learning*, *deep learning*,

cognitive computing e monitorização transacional em tempo real surgem recorrentemente como mecanismos promissores para deteção de *phishing*, fraude e anomalias. A literatura reconhece, porém, limitações importantes, como falsos positivos, sensibilidade reduzida a padrões raros, dependência da qualidade dos dados e necessidade de supervisão humana na interpretação dos alertas. Assim, os algoritmos melhoram a capacidade defensiva, mas não eliminam o problema organizacional da decisão sob risco (Banirostam et al., 2025; Ghosh, 2025; Nicholls et al., 2021).

Um quarto plano de resiliência diz respeito à arquitetura de confiança. Autenticação multifator, biometria, segmentação de acesso, verificação contínua de identidade, princípios *Zero Trust* e camadas de proteção distribuída aparecem na literatura como respostas adequadas a um ambiente em que acessos legítimos podem ser comprometidos e em que o perímetro tradicional da rede já não coincide com o perímetro do negócio. A função da segurança passa, assim, a ser menos a criação de uma fronteira rígida e mais a verificação permanente da legitimidade das interações, dos acessos e das transações (Daah et al., 2024; Khan et al., 2023; Tsai et al., 2024).

4.5.1 Dados quantitativos do eixo dos mecanismos de resiliência digital

Os dados quantitativos deste eixo são os mais densos do corpus. Em deteção de *phishing*, o sistema DEPHIDES atinge 98,74% de *accuracy* com capacidade superior a 130.000 URLs por segundo. O modelo de Taha, baseado em *weighted soft voting*, alcança 95% de *accuracy* e 98,8% de *AUC*. Um modelo aplicado a *parked domains* numa instituição financeira obteve 96,02% de *recall* e 97,28% de *accuracy*. Estes resultados mostram que a deteção automatizada de *phishing* já atinge desempenhos muito elevados em tarefas delimitadas (Duarte et al., 2025; Sahingoz et al., 2024; Taha, 2021).

Na componente humana, os números de awareness são particularmente fortes. No estudo tailandês com 20.134 trabalhadores, 23,4% abriram o primeiro *e-mail* de *phishing* e 22,1% clicaram no link; após intervenção, 94% deixaram de clicar e 98% deixaram de inserir password, correspondendo a uma redução de 71,5% na abertura do *e-mail* de *phishing*. No estudo israelita com cerca de 5.000 trabalhadores, a taxa de clique caiu de 25% para 13% e depois para 7%,

embora as mensagens personalizadas continuassem a gerar taxas entre 29,8% e 34,5% (Daengsi et al., 2022; Hillman et al., 2023).

Em síntese, os dados quantitativos do eixo dos mecanismos de resiliência digital evidenciam que as soluções de deteção, prevenção e resposta alcançaram níveis muito elevados de desempenho técnico, sobretudo em contextos de phishing, fraude transacional, malware e autenticação. No entanto, os resultados também mostram que a eficácia da resiliência não depende apenas da sofisticação tecnológica, mas da sua articulação com treino, cultura organizacional, supervisão humana, governação e capacidade de resposta operacional. Deste modo, a evidência quantitativa reforça a conclusão de que a resiliência digital no setor financeiro é uma capacidade integrada, simultaneamente técnica, humana e institucional, indispensável para limitar danos e assegurar continuidade em ambientes de risco crescente.

Esta tabela lista os artigos analisados:

Tabela 5 - Artigos que se enquadram no eixo dos mecanismos de resiliência digital

Autor / Ano	Tema principal	Descrição do contributo do artigo	Área geográfica
Sahingoz, Buber & Kugu (2024)	Deteção de *phishing* com *deep learning*	Desenvolve o sistema DEPHIDES para deteção de *phishing* por URL com *deep learning*.	Turquia
Taha (2021)	Deteção de *websites* de *phishing*	Propõe uma abordagem de ensemble *learning* com *weighted soft voting* para distinguir *websites* legítimos e de *phishing*.	Arábia Saudita
Almazroi & Ayub (2023)	Deteção de fraude em pagamentos	Desenvolve um modelo de *machine learning* para	Arábia Saudita / Paquistão
	online	deteção de fraude em transações financeiras *online*.	
Stojanović et al. (2021)	Deteção de fraude em aplicações *FinTech*	Avalia métodos de *machine learning* e anomaly detection para prevenção de fraude em ambientes *FinTech*.	Europa

Srokosz et al. (2023)	Scoring antifraude com *machine learning*	Desenvolve um sistema antifraude para apoio a CISIRTs em ambiente bancário.	Polónia
Kuttiyappan & Rajasekar (2023)	Deteção de ataques maliciosos na banca	Propõe um classificador *ResNet* para identificar ataques maliciosos em transações bancárias.	Índia
Khan et al. (2023)	Biometria e cibersegurança bancária	Analisa a biometria como mecanismo de autenticação reforçada contra fraude e acessos indevidos na banca.	Global
Tariq et al. (2024)	NIST e prevenção da fraude bancária	Mostra como as funções do *framework* NIST reforçam a prevenção da fraude em bancos comerciais.	Jordânia
AL-Dosari, Fetais & Kucukvar (2024)	IA e ciberdefesa na banca	Explora o uso de inteligência artificial como componente central de *cyber* defence systems bancários.	Qatar

Mishra (2023)	IA e gestão de cibersegurança financeira	Propõe uma abordagem baseada em inteligência artificial para proteção de dados, redução de risco e prevenção de ataques no setor financeiro.	Arábia Saudita
Daah et al. (2024)	*Zero Trust* com *blockchain*	Propõe uma *framework Zero Trust* para a indústria financeira, integrando *blockchain* como camada adicional de confiança.	Reino Unido
Daengsi et al. (2022)	Awareness *anti-phishing* em instituição financeira	Avalia uma intervenção de awareness *anti-phishing* em larga escala numa instituição financeira tailandesa.	Tailândia
Hillman, Harel & Toch (2023)	Treino *anti-phishing* em larga escala	Analisa a eficácia de campanhas simuladas de *phishing* numa instituição financeira.	Israel
Ullah et al. (2022)	Deteção de *malware* em tráfego Android	Desenvolve um mecanismo híbrido de deteção de *malware* relevante para *mobile banking* e ecossistemas financeiros móveis.	China / internacional

Ahmed et al. (2021)	Segurança em *mobile payment systems*	Sistematiza mecanismos de autenticação, encriptação e segurança em pagamentos móveis.	Global
Kanimozhi & Prem Jacob (2021)	Intrusion detection com IA	Compara classificadores de IA para deteção de botnets em NIDS, com interesse para infraestruturas financeiras.	Índia
Doshi et al. (2023)	Deteção de *phishing* e *spam* por arquitetura *dual-layer*	Propõe uma arquitetura *dual-layer* com *deep learning* para classificar *phishing* e *spam* em *e-mail*.	Índia
Van der Kleij et al. (2022)	Apoio à decisão em gestão de incidentes	Desenvolve *decision support* para *threat and incident managers* do setor financeiro.	Países Baixos
Raddatz et al. (2023)	Adoção de aplicações baseadas em *blockchain*	Mostra o papel da privacidade percebida e da consciência dos riscos na adoção de aplicações *blockchain* no contexto bancário.	Estados Unidos

Tsai (2023)	*Blockchain* em *supply chain* finance	Propõe um modelo *blockchain-enabled* para reforçar segurança, transparência e confiança em *supply chain* finance.	Taiwan
Feng et al. (2023)	Deteção de transações associadas a ciberataques em *blockchain*	Desenvolve uma abordagem orientada para *blockchain* para detetar transações comprometidas em tempo real.	Global
Ghosh (2025)	*Framework XAI-RNN-SGRU* para fraude financeira	Propõe um modelo avançado de explicabilidade e redes neuronais para fraude e cibersegurança financeira.	Global
Banirostam et al. (2024/2025)	Métodos de deteção de fraude em cartões eletrónicos	Compara métodos de deteção de fraude em pagamentos eletrónicos em contexto de big data.	Global
Seraj et al. (2024)	Segurança em *mobile banking*	Desenvolve uma abordagem explicável para proteção do *mobile banking* contra *malware* e acessos maliciosos.	Reino Unido / Arábia Saudita / Jordânia
Nicholls et al. (2021)	*Deep learning* contra financial *cybercrime*	Revê aplicações de *deep learning* ao combate ao financial *cybercrime*.	Global

Mustapha et al. (2023)	Soluções de cibersegurança para *apps* móveis *FinTech*	Analisa soluções de cibersegurança no ecossistema de aplicações móveis *FinTech*.	Global
Ozkan, van Lingen & Spruit (2021)	Modelo de maturidade CYSFAM	Propõe um modelo de maturidade de capacidades de cibersegurança testado numa instituição financeira.	Não explicitado
Tsai, Liou & Lee (2024)	*Online banking* suportado por *blockchain*	Propõe um esquema de *online banking* suportado por *blockchain* com reforço de segurança e integridade.	Taiwan
Duarte et al. (2025)	Deteção precoce de *phishing* URLs em *parked domains*	Desenvolve uma abordagem de *machine learning* aplicada a instituição financeira para deteção precoce de URLs de *phishing*.	Brasil

Fonte: Elaboração própria.

4.6 Síntese do capítulo

A análise realizada neste capítulo mostra que o cibercrime no setor financeiro resulta da convergência entre ameaças híbridas, impactos económicos cumulativos, necessidade de novas respostas institucionais e crescente centralidade da resiliência operacional digital. As evidências reunidas indicam que o problema não pode ser tratado como questão periférica de segurança informática. Trata-se, antes, de uma variável estrutural da organização e do funcionamento do setor financeiro em contexto de digitalização intensiva (Cojocaru, 2025; Javaheri et al., 2024; Uddin et al., 2020).

Desta leitura integrada emerge uma conclusão central: o risco cibernético é inseparável do próprio modelo de eficiência, conectividade e inovação que caracteriza o setor financeiro contemporâneo. A mesma infraestrutura que acelera serviços, reduz fricções e amplia acesso também multiplica dependências, pontos de falha e exigências de governação. É com base nesta leitura que o capítulo seguinte apresenta as conclusões finais da investigação (Aldasoro et al., 2022; Nefla & Jellouli, 2025; Türegün, 2025).

5 Conclusão

5.1 Introdução

A presente dissertação procurou responder à seguinte questão de investigação: o que revela a literatura científica recente sobre a evolução, o impacto e a mitigação do cibercrime no setor financeiro entre 2020 e 2026? A análise foi conduzida a partir de quatro eixos — tipologias de ameaça, impactos económicos, respostas institucionais e regulatórias e mecanismos de resiliência digital —, que permitiram integrar evidência dispersa em diferentes tradições disciplinares e construir uma leitura comum do fenómeno (Javaheri et al., 2024; Nefla & Jellouli, 2025; Uddin et al., 2020).

5.2 Resposta à pergunta de investigação

A literatura recente mostra, em primeiro lugar, que o cibercrime no setor financeiro se tornou mais híbrido, mais interdependente e mais ecossistémico. As ameaças deixaram de se concentrar apenas em intrusões técnicas clássicas e passaram a articular engenharia social, fraude transacional, vulnerabilidades em serviços *cloud*, ecossistemas *fintech*, *mobile banking* e infraestruturas distribuídas. O risco decorre menos de um vetor isolado do que da convergência entre digitalização acelerada, interdependências tecnológicas e pressão por continuidade em tempo real (Ahmed et al., 2021; Javaheri et al., 2024; Smaga, 2026).

Em segundo lugar, a literatura mostra que os impactos do cibercrime ultrapassam a perda monetária imediata. Os custos incluem remediação, reforço tecnológico, apoio ao cliente, litigância, *compliance*, erosão de confiança e efeitos de contágio potencial sobre o sistema. O risco cibernético aparece, assim, como variável económica estrutural, com implicações para eficiência, valor da firma, reputação, estabilidade operacional e, em certos contextos, estabilidade financeira (Boungou, 2023; Türegün, 2025; Uddin et al., 2020).

Em terceiro lugar, a literatura revela que a resposta institucional se desloca de uma lógica de *compliance* técnico para uma lógica de resiliência operacional digital. DORA, NIS2 e outros quadros regulatórios recentes mostram que o setor financeiro passou a ser tratado como infraestrutura crítica cuja continuidade depende de coordenação entre governação, supervisão, reporte, gestão de terceiros e capacidade de recuperação. A cibersegurança deixou de ser função técnica lateral e passou a integrar o núcleo da governação prudencial e organizacional (Bagherifam et al., 2025; Ragazzo et al., 2025; Vandezande, 2024).

Em quarto lugar, a literatura confirma que a mitigação eficaz do cibercrime financeiro depende da articulação entre tecnologia, governação, cultura organizacional e cooperação institucional. Modelos analíticos de deteção, autenticação reforçada, treino *anti-phishing*, *frameworks* como NIST, *Zero Trust*, biometria e *blockchain* mostram resultados promissores, mas nenhum destes mecanismos é suficiente isoladamente. A resiliência relevante para o setor é sempre combinada (Daah et al., 2024; Khan et al., 2023; Nicholls et al., 2021).

5.3 Principais conclusões por eixo

Os quatro eixos analíticos que estruturaram esta dissertação — tipologias de ameaça, impactos económicos, respostas institucionais e regulatórias e mecanismos de resiliência digital — não devem ser lidos como blocos autónomos, mas como dimensões complementares de uma mesma realidade. Em conjunto, permitiram construir uma leitura integrada do cibercrime no setor financeiro, mostrando que a evolução das ameaças, os seus efeitos económicos, a resposta institucional e a capacidade de mitigação fazem parte de um mesmo processo de transformação digital do setor (Aldasoro et al., 2022; Annarelli et al., 2020; Uddin et al., 2020).

No eixo das tipologias de ameaça, a principal conclusão foi que o cibercrime financeiro assumiu uma natureza cada vez mais híbrida, interdependente e ecossistémica. Este eixo permitiu mostrar que phishing, fraude em pagamentos

digitais, vulnerabilidades em fintech e riscos sobre infraestruturas críticas não são fenómenos isolados, mas expressões de um mesmo ambiente digitalizado em que eficiência e vulnerabilidade se reforçam mutuamente. Assim, este primeiro eixo foi essencial para estabelecer o problema central da dissertação: a digitalização do setor financeiro ampliou não apenas a inovação, mas também a complexidade do risco (Ahmed et al., 2021; Javaheri et al., 2024; Ragazzo et al., 2025).

No eixo dos impactos económicos, a dissertação mostrou que o cibercrime ultrapassa claramente a esfera técnica e produz efeitos sobre desempenho, intermediação, custos, reputação e confiança. Este eixo foi decisivo para ligar o tema da cibersegurança ao enquadramento da Economia Industrial e de Empresa, evidenciando que o risco cibernético afeta diretamente a eficiência, a competitividade e a robustez económica das instituições financeiras. Deste modo, o trabalho demonstrou que o cibercrime financeiro deve ser tratado como variável económica estrutural do funcionamento do setor (Boungou, 2023; Gatzert & Schubert, 2022; Türegün, 2025).

No eixo das respostas institucionais e regulatórias, a principal ideia geral foi que a evolução do cibercrime foi acompanhada por um reforço da densidade regulatória e da capacidade institucional de resposta. Este eixo permitiu mostrar que a mitigação do risco não depende apenas de escolhas técnicas das instituições, mas também da existência de quadros regulatórios, mecanismos de supervisão e modelos de governação adequados a um setor altamente interdependente. Assim, a dissertação evidenciou que a resposta ao cibercrime é também uma questão de arquitetura institucional e de coordenação sistémica (Cojocaru, 2025; Vandezande, 2024; López et al., 2025).

No eixo dos mecanismos de resiliência digital, o principal contributo para o conjunto do trabalho foi demonstrar que a mitigação eficaz exige uma resposta integrada, que combine tecnologia, processos, cultura organizacional e capacidade adaptativa. Este eixo permitiu fechar a lógica global da dissertação: depois de identificar as ameaças, compreender os seus impactos e analisar as

respostas institucionais, tornou-se claro que a capacidade de enfrentar o cibercrime depende da construção de resiliência digital como competência estratégica do setor financeiro (Annarelli et al., 2020; Daah et al., 2024; Daengsi et al., 2022).

Em síntese, os quatro eixos analíticos convergem numa mesma conclusão: o cibercrime no setor financeiro não constitui uma anomalia externa ao processo de digitalização, mas uma dimensão estrutural das condições contemporâneas de funcionamento do setor. Foi precisamente esta articulação entre ameaça, impacto, regulação e resiliência que permitiu à dissertação construir uma leitura transversal e coerente do problema, respondendo à questão de investigação e reforçando a relevância do tema no quadro da Economia Industrial e de Empresa. (Aldasoro et al., 2022; Cojocaru, 2025; Uddin et al., 2020).

5.4 Implicações para o setor financeiro

Para bancos e instituições financeiras, a principal implicação é a necessidade de tratar o risco cibernético como componente estratégica e não como extensão residual da tecnologia. Isso implica integrar cibersegurança na governação, no planeamento de continuidade, nos mecanismos de *disclosure*, na gestão de terceiros e na relação com clientes (López et al., 2025; Türegün, 2025).

Para reguladores e supervisores, a principal implicação é que a resposta ao ciber-risco deve combinar harmonização normativa com capacidade operacional, supervisão de dependências críticas e mecanismos de teste e aprendizagem. A concentração *cloud* e a interdependência digital sugerem que parte importante do risco futuro será sistémica e não apenas institucional (Bagherifam et al., 2025; Ragazzo et al., 2025; Vandezande, 2024).

Para *fintechs* e prestadores tecnológicos, a implicação central é que a expansão da inovação financeira sem reforço equivalente de segurança, autenticação e controlo de dependências tende a ampliar risco reputacional, custos de conformidade e fricção de adoção. A segurança digital deve ser encarada como

pré-condição da escalabilidade do negócio (Dubauskas & Išoraitė, 2025; Javaheri et al., 2024; Nefla & Jellouli, 2025).

5.5 Limitações da investigação

Apesar da robustez analítica do trabalho, importa reconhecer algumas limitações. A literatura mobilizada é metodologicamente heterogénea, combinando revisões sistemáticas, estudos econométricos, análises regulatórias, estudos de caso e trabalhos técnicos, o que limita a comparabilidade direta entre resultados. Parte dos dados quantitativos monetários utilizados provém de relatórios institucionais citados na literatura científica, o que exige prudência na interpretação. Além disso, a rápida evolução do campo significa que parte das ameaças, respostas e soluções poderá sofrer alteração relevante num horizonte temporal curto (Bagherifam et al., 2025; Javaheri et al., 2024; Uddin et al., 2020).

5.6 Pistas para investigação futura

A investigação futura pode desenvolver-se em quatro direções principais. A primeira consiste em aprofundar estudos empíricos sobre efeitos financeiros reais dos incidentes cibernéticos em bancos, seguradoras e *fintechs*. A segunda passa por investigar de forma mais sistemática o *third-party* concentration *risk*, sobretudo em serviços *cloud* e infraestruturas críticas partilhadas. A terceira refere-se à comparação entre jurisdições regulatórias, avaliando diferenças de eficácia entre modelos de supervisão e resiliência digital. A quarta consiste em estudar mais profundamente a articulação entre fatores humanos, analíticos e arquiteturais na construção de mecanismos de resiliência realmente eficazes (Aldasoro et al., 2022; Cojocaru, 2025; Ghosh, 2025; Ragazzo et al., 2025).

5.7 Conclusão final

A principal conclusão desta dissertação é que o cibercrime financeiro não pode ser entendido como anomalia externa ao processo de digitalização. Ele é, antes, parte integrante das novas condições de funcionamento do setor financeiro.

Quanto maior a velocidade, a conectividade, a automação e a dependência de terceiros, maior a eficiência potencial, mas também maior a complexidade do risco. Neste sentido, o ciber-risco deve ser tratado como determinante da eficiência, da competitividade e da estabilidade do setor financeiro contemporâneo. É precisamente esta leitura que justifica o lugar desta investigação no âmbito da Economia Industrial e de Empresa (Aldasoro et al., 2022; Annarelli et al., 2020; Uddin et al., 2020; Vandezande, 2024).

Referências

Ahmed, W., Rasool, A., *Javed*, A. R., Kumar, N., Gadekallu, T. R., Jalil, Z., & Kryvinska, N. (2021). *Security in next generation mobile payment systems*: A *comprehensive survey*. *IEEE Access*, 9. https://doi.org/10.1109/ACCESS.2021.3105450

Al Batayneh, A. A., Qasaimeh, M., & Al-Qassas, R. S. (2021). A *scoring system for information security governance framework using deep learning algorithms*: A *case study on the banking sector*. ACM *Journal of Data and Information Quality*, 13(2), *Article* 9. https://doi.org/10.1145/3418172

AL-Dosari, K., Fetais, N., & Kucukvar, M. (2024). *Artificial intelligence and cyber defense system for banking industry*: A *qualitative study of* AI *applications and challenges*. *Cybernetics and Systems*, 55(2), 302–330. https://doi.org/10.1080/01969722.2022.2112539

AL-Habashneh, A. G., *Mohammad*, S. *I*. S., Vasudevan, A., Al-Adwan, A. S., *Mohammad*, A. A. S., & Jiang, L. Q. (2025). *Impact of the quality of financial and banking applications used on smartphone on the customer satisfaction of Jordanian Islamic Bank*. *International Review of Management and Marketing*, 15(1), 99–106. https://doi.org/10.32479/irmm.17706

Aldasoro, *I.*, Gambacorta, L., Giudici, P., & *Leach*, T. (2022). *The drivers of cyber risk*. *Journal of Financial Stability*, 60, 100989. https://doi.org/10.1016/j.jfs.2022.100989

Almazroi, A. A., & Ayub, N. (2023). *Online payment fraud detection model using machine learning techniques*. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3339226

Aslam, M., Abbasi, M. A. K., *Khalid*, T., *Shan*, R. U., Ullah, S., *Ahmad*, T., Saeed, S., Alabbad, D. A., & *Ahmad*, R. (2022). *Getting* smarter *about smart cities*: *Improving data security and privacy through compliance*. *Sensors*, 22, 9338. https://doi.org/10.3390/s22239338

Bagherifam, N., Naghdi, S., Ahmadian, V., Fazlzadeh, A., & Shishehgarkhaneh, M. B. (2025). *Digital regulatory governance*: *The role of RegTech and SupTech in transforming financial oversight and administrative capacity*. *International Journal of Financial Studies*, 13(4), 217. https://doi.org/10.3390/ijfs13040217

Banirostam, H., Banirostam, T., Pedram, M. M., & Rahmani, A. M. (2025). *Analysis and evaluation of various fraud detection methods for electronic payment cards transactions in big data*. *Journal of Signal Processing Systems*, 96, 849–870. https://doi.org/10.1007/s11265-025-01947-w

Bank for International Settlements. (2022). *Cyber risk in central banking* (*BIS Working Papers No*. 1039).

Birthriya, S. K., & *Jain*, A. K. (2022). A *comprehensive survey of phishing email detection and protection techniques*. *Information Security Journal*: A *Global Perspective*, 31(4), 411–440. https://doi.org/10.1080/19393555.2021.1959678

Boungou, W. (2023). *Cyber-attacks and banking* intermediation. *Economics Letters*, 233, 111354. https://doi.org/10.1016/j.econlet.2023.111354

Capital One. (2019). *2019 cyber incident: What happened, how we responded.* https://www.capitalone.com/digital/facts2019/

Choithani, T., Chowdhury, A., *Patel*, S., *Patel*, P., *Patel*, D., & *Shah*, M. (2024). A *comprehensive study of artificial intelligence and cybersecurity on Bitcoin*, crypto *currency and banking system*. *Annals of Data Science*, 11(1), 103–135. https://doi.org/10.1007/s40745-022-00433-5

Cojocaru, A. (2025). *Aligning regulation and governance for cyber resilience*: A *theoretical framework for the UK financial sector*. *Computers & Security*, 157, 104627. https://doi.org/10.1016/j.cose.2025.104627

Daah, C., Qureshi, A., Awan, *I.*, & Konur, S. (2024). *Enhancing Zero Trust models in the financial industry through blockchain integration*: A proposed *framework*. *Electronics*, 13(5), 865. https://doi.org/10.3390/electronics13050865

Daengsi, T., Pornpongtechavanich, P., & Wuttidittachotti, P. (2022). *Cybersecurity awareness enhancement*: A *study of the effects of age and gender of Thai employees associated with phishing attacks*. *Education and Information Technologies*. https://doi.org/10.1007/s10639-021-10806-7

Darem, A. A., Alhashmi, A. A., Alkhaldi, T. M., Alashjaee, A. M., Alanazi, S. M., & Ebad, S. A. (2023). *Cyber threats* classifications *and* countermeasures in banking *and financial sector*. IEEE Access. https://doi.org/10.1109/ACCESS.2023.3327016

Doshi, J., Parmar, K., Sanghavi, R., & Shekokar, N. (2023). A *comprehensive dual-layer architecture for phishing and spam email detection*. *Computers* & *Security*, 133, 103378. https://doi.org/10.1016/j.cose.2023.103378

Duarte, J. D., *Junior*, P. C., da *Costa*, J. P. J., da *Costa*, E. J., de Melo, L. P., *Nunes*, R. R., *Soares*, C. G. V. N., & *Silva*, T. E. da C. (2025). *Machine learning for early detection of phishing* URLs *in parked domains*: *An approach* applied *to* a *financial institution*. *IEEE Access*, 13. https://doi.org/10.1109/ACCESS.2025.3599454

Dubauskas, G., & Išoraitė, M. (2025). *Banking development peculiarities*: *Blockchain*, *artificial intelligence* (AI) *and cybersecurity issues*. *Entrepreneurship and Sustainability Issues*, 12(3), 61–72. https://doi.org/10.9770/x7965543644

Electronic Privacy Information Center. (n.d.). *Equifax data breach.* https://archive.epic.org/privacy/data-breach/equifax/

European Central Bank. (2024, *July* 26). *ECB concludes cyber resilience stress test.*

European Commission, & *European* Insurance *and* Occupational Pensions Authority. (2025). *DORA – Regulamento (UE) 2022/2554 e atos delegados e de execução.*

European Union Agency for Cybersecurity. (2024). *Finance sector threat landscape 2024.* https://www.enisa.europa.eu/sites/default/files/2025-02/Finance-Sector-Threat-Landscape-2024.pdf

Feng, Z., *Li*, Y., & *Ma*, X. (2023). *Blockchain-oriented approach for detecting cyber-attack transactions*. *Financial Innovation*, 9, 81. https://doi.org/10.1186/s40854-023-00490-6

Financial Services Information Sharing and Analysis Center. (2024). *Navigating Cyber 2024.*

Gatzert, N., & *Schubert*, M. (2022). *Cyber risk management in the US banking and insurance industry*: A *textual and empirical analysis of determinants and value*. *Journal of Risk and Insurance*. https://doi.org/10.1111/jori.12381

Gavenaite-Sirvydiene, J., & Miecinskiene, A. (2023). A *framework for cyber security areas evaluation in financial sector*. *Transformations in Business* & *Economics*, 22(3), 192–205.

Ghosh, S. (2025). A *novel framework for financial cybersecurity and fraud detection using XAI-RNN-SGRU*. *IEEE Access*. https://doi.org/10.1109/ACCESS.2025.3570216

Gonçalves, A., da Silveira, M. A. P., Marcolin, C. B., & Kubo, E. K. de M. (2024). Metodologias de projetos para atender exigências regulatórias: Um estudo com gerentes de projeto do setor bancário nacional. Revista de Gestão e Projetos (GeP), 15(3), 625–650. https://doi.org/10.5585/gep.v15i3.26590

Hillman, D., Harel, A., & Toch, E. (2023). *Evaluating organizational phishing awareness training on an enterprise scale*. *Computers & Security*, 132, 103364. https://doi.org/10.1016/j.cose.2023.103364

IBM. (2024). *Cost of a data breach 2024: Financial industry.*

International Monetary Fund. (2024). *Cyber risk*: A *growing concern for* macrofinancial *stability*. *In Global financial stability report: The last mile—Financial vulnerabilities and risks* (*Chapter* 3). https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024

Jain, R., Kumar, S., Sood, K., Grima, S., & Rupeika-Apoga, R. (2023). A *systematic literature review of the risk landscape in fintech*. *Risks*, 11(2), 36. https://doi.org/10.3390/risks11020036

Javaheri, D., Fahmideh, M., Chizari, H., Lalbakhsh, P., & Hur, J. (2024). *Cybersecurity threats* in *FinTech*: A *systematic review*. Expert Systems *with* Applications, 241, 122697. https://doi.org/10.1016/j.eswa.2023.122697

Jin, J., *Li*, N., Liu, S., & Nainar, S. M. K. (2023). *Cyber attacks*, *discretionary loan loss provisions*, *and banks' earnings management*. *Finance* Research *Letters*, 54, 103705. https://doi.org/10.1016/j.frl.2023.103705

Jović, Ž., & Nikolić, *I.* (2022). *The* darker *side of fintech*: *The emergence of new risks*. *Zagreb International Review of Economics & Business*, 25(*Special Conference Issue*). https://doi.org/10.2478/zireb-2022-0024

Kanimozhi, V., & *Jacob*, T. P. (2021). *Artificial intelligence outflanks all other machine learning classifiers in network intrusion detection system on the realistic cyber dataset* CSE-CIC-IDS2018 *using cloud computing*. ICT *Express*, 7, 366–370. https://doi.org/10.1016/j.icte.2020.12.004

Khan, H. U., Malik, M. Z., Nazir, S., & *Khan*, F. (2023). *Utilizing bio metric system for enhancing cyber security in banking sector*: A *systematic analysis*. *IEEE Access*. https://doi.org/10.1109/ACCESS.2023.3298824

Khiari, W., Lajmi, A., Neffati, A., & Fahem, A. E. (2025). *Cryptocurrency fraud and its effects on price volatility in the cryptocurrency market*. *Journal of Chinese Economic and Foreign Trade Studies*, 18(2), 243–275. https://doi.org/10.1108/JCEFTS-05-2024-0034

Kleij, R. van D., Schraagen, J. M., *Cadet*, B., & *Young*, H. (2022). *Developing decision support for cybersecurity threat and incident managers*. *Computers & Security*, 113, 102535. https://doi.org/10.1016/j.cose.2021.102535

Krishna, B., Krishnan, P., & *Sebastian*, B. (2023). *Examining the relationship between national cybersecurity commitment*, *culture*, *and digital payment usage*: *An institutional trust theory perspective*. *Information Systems Frontiers*. https://doi.org/10.1007/s10796-022-10280-7

Kuttiyappan, D., & V., R. (2023). *Improving the cyber security over banking sector* by *detecting the malicious attacks using the wrapper stepwise Resnet classifier*. KSII *Transactions on Internet and Information Systems*, 17(6). https://doi.org/10.3837/tiis.2023.06.007

Kuzior, A., *Brożek*, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. (2022). *Countering cybercrime risks in financial institutions*: *Forecasting information trends*. *Journal of Risk and Financial Management*, 15(12), 613. https://doi.org/10.3390/jrfm15120613

Kuzmenko, O. V., Kubálek, J., Bozhenko, V. V., Kushneryov, O. S., & *Vida*, *I.* (2021). *An approach to managing innovation to protect financial sector against cybercrime*. *Polish Journal of Management Studies*, 24(2). https://doi.org/10.17512/pjms.2021.24.2.17

Kuznyetsova, A., Kuzmenko, T., & Frolova, *I.* (2022). *Development of financial inclusion from the standpoint of ensuring financial stability*. *Problems and Perspectives in Management*, 11(1). https://doi.org/10.21511/pmf.11(1).2022.03

López, F. A., Jara-Sarrúa, L., Morales-Parada, F., & Palos-Sánchez, P. R. (2025). *Cybersecurity disclosure in the financial sector*: *An examination of the influence of incident exposure*, *governance practices*, *and regulatory* context. *Electronic Commerce* Research. https://doi.org/10.1007/s10660-025-10081-5

Marwan, A., Garduño, D. O.-C., & Bonfigli, F. (2022). *Detection of digital law issues and implication for good governance policy in Indonesia*. Bestuur, 10(1), 22–32. https://doi.org/10.20961/bestuur.v10i1.59143

Mhlanga, D. (2020). *Industry* 4.0 *in finance*: *The impact of artificial intelligence* (AI) *on digital financial inclusion*. *International Journal of Financial Studies*, 8(3), 45. https://doi.org/10.3390/ijfs8030045

Mishra, A., Alzoubi, Y. *I.*, Anwar, M. J., & *Gill*, A. Q. (2022). *Attributes impacting cybersecurity policy development*: *An evidence from seven nations*. *Computers & Security*, 120, 102820. https://doi.org/10.1016/j.cose.2022.102820

Mishra, S. (2023). *Exploring the impact of AI-based cyber security financial sector management*. Applied *Sciences*, 13, 5875. https://doi.org/10.3390/app13105875

Mohapatra, C. S., & Ghosh, D. (2024). *Investor protection paradigm in India*: *Mounting criticality of digitalisation*. *Margin—The Journal of* Applied *Economic* Research, 17(3–4), 251–278. https://doi.org/10.1177/00252921241262674

Mosteanu, N. R., & Faccia, A. (2021). *Fintech frontiers in quantum computing*, *fractals*, *and blockchain distributed ledger*. *Paradigm shifts and open innovation*. *Journal of Open Innovation*: *Technology*, *Market*, *and Complexity*, 7(1), 19. https://doi.org/10.3390/joitmc7010019

Mustapha, *I.*, Vaicondam, Y., Jahanzeb, A., Usmanovich, B. A., & Yusof, S. H. B. (2023). *Cybersecurity challenges and* solutions *in the fintech mobile app ecosystem*. *International Journal of Interactive Mobile Technologies*, 17(22), 100–116. https://doi.org/10.3991/ijim.v17i22.45261

Nefla, D., & Jellouli, S. (2025). *Emerging technologies in finance*: *Challenges for* a *sustainable finance*. *Cogent Business & Management*, 12(1), 2495191. https://doi.org/10.1080/23311975.2025.2495191

Nicholls, J., Kuppa, A., & Le-Khac, N.-A. (2021). *Financial cybercrime*: A *comprehensive survey of deep learning approaches to tackle the evolving financial crime landscape*. *IEEE Access*, 9. https://doi.org/10.1109/ACCESS.2021.3134076

Ozkan, B. Y., van Lingen, S., & Spruit, M. (2021). *The cybersecurity focus area maturity* (CYSFAM) *model*. *Journal of Cybersecurity and Privacy*, 1, 119–139. https://doi.org/10.3390/jcp1010007

Raddatz, N., Coyne, J., Menard, P., & Crossler, R. E. (2023). *Becoming* a *blockchain user*: *Understanding consumers' benefits* realisation *to use blockchain-based applications*. *European Journal of Information Systems*, 32(2), 287–314. https://doi.org/10.1080/0960085X.2021.1944823

Ragazzo, C. E. J., *Costa*, R. V. de F., & Tourinho, V. (2025). *Geopolitical risks and cyberattacks* as *catalysts*: Redefinition *of regulatory responses* (*and gaps*) *in the banking sector*. *Journal of Financial Regulation and Compliance*. https://doi.org/10.1108/JFRC-04-2025-0097

Sahingoz, O. K., *Buber*, E., & Kugu, E. (2024). DEPHIDES: *Deep learning based phishing detection system*. *IEEE Access*. https://doi.org/10.1109/ACCESS.2024.3352629

Saltzer, J. H., & *Schroeder*, M. D. (1975). *The protection of information in computer systems*. *Proceedings of the IEEE, 63*(9), 1278–1308. https://doi.org/10.1109/PROC.1975.9939

Seraj, S., Sadiq, A. S., Kaiwartya, O., Aljaidi, M., Konios, A., Ali, M., & Abazeed, M. (2024). MoBShield: A novel XML *approach for* securing *mobile banking*. Computers, Materials & Continua, 79(2). https://doi.org/10.32604/cmc.2024.048914

Shah, M. A., & *Raj*, N. (2025). *Examining the role of blockchain and public-private partnerships in design and deployment of blockchain-enabled* CBDC. *Digital Business*, 5, 100111. https://doi.org/10.1016/j.digbus.2025.100111

Shahzadi, A., Ishaq, K., Nawaz, N. A., Rosdi, F., & Khan, F. A. (2025). Unveiling personalized *and* gamification-based *cybersecurity risks within financial*

institutions. PeerJ Computer *Science*, 11, e2598. https://doi.org/10.7717/peerj-cs.2598

Smaga, P. (2026). *Evaluating cyber attacks on central banks – identification of trends in cyber threat landscape*. *Computers* & *Security*, 160, 104742. https://doi.org/10.1016/j.cose.2025.104742

Srokosz, M., Bobyk, A., Ksiezopolski, B., & Wydra, M. (2023). *Machine-learning-based* scoring system *for* antifraud CISIRTs in banking environment. Electronics, 12(1), 251. https://doi.org/10.3390/electronics12010251

Stojanović, B., *Božič*, J., Hofer-Schmitz, K., Nahrgang, K., *Weber*, A., Badii, A., Sundaram, M., *Jordan*, E., & Runevic, J. (2021). *Follow the trail*: *Machine learning for fraud detection in fintech applications*. *Sensors*, 21(5), 1594. https://doi.org/10.3390/s21051594

Taha, A. (2021). *Intelligent ensemble learning approach for phishing website detection based on weighted soft voting*. *Mathematics*, 9(21), 2799. https://doi.org/10.3390/math9212799

Tariq, E., Akour, *I.*, Al-Shanableh, N., Alquqa, E. K., Alzboon, N., Al-Hawary, S. *I.* S., & Alshurideh, M. T. (2024). *How cybersecurity influences fraud prevention*: *An empirical study on Jordanian commercial banks*. *International Journal of Data and Network Science*, 8, 69–76. https://doi.org/10.5267/j.ijdns.2023.10.016

Thach, N. N., Hanh, H. T., Huy, D. T. N., Thuy, do M., & Van *Hong*, P. (2021). *Technology quality management of the industry* 4.0 *and cybersecurity risk management on current banking activities in emerging markets*: *The case in Vietnam*. *International Journal for Quality* Research, 15(3), 845–856. https://doi.org/10.24874/IJQR15.03-10

Tsai, C.-H. (2023). *Supply chain financing scheme based on blockchain technology from* a *business application perspective*. *Annals of Operations* Research, 320, 441–472. https://doi.org/10.1007/s10479-022-05033-3

Tsai, C.-H., Liou, D.-K., & *Lee*, H.-L. (2024). *Blockchain-supported online banking scheme*. *Egyptian Informatics Journal*, 27, 100516. https://doi.org/10.1016/j.eij.2024.100516

Türegün, N. (2025). *Digital transformation and cybersecurity risks*. *International Journal of Accounting Information Systems*, 56, 100749. https://doi.org/10.1016/j.accinf.2025.100749

Uddin, M. H., Mollah, S., *Islam*, N., & *Ali*, M. H. (2023). *Does digital transformation matter for operational risk exposure*?. *Technological Forecasting and Social Change*, 197, 122919. https://doi.org/10.1016/j.techfore.2023.122919

UK Government. (2024). *Cyber security breaches survey 2024.*

Vandezande, N. (2024). *Cybersecurity in the* EU: *How the* NIS2*-directive stacks up against its predecessor*. *Computer Law & Security Review*, 52, 105890. https://doi.org/10.1016/j.clsr.2023.105890

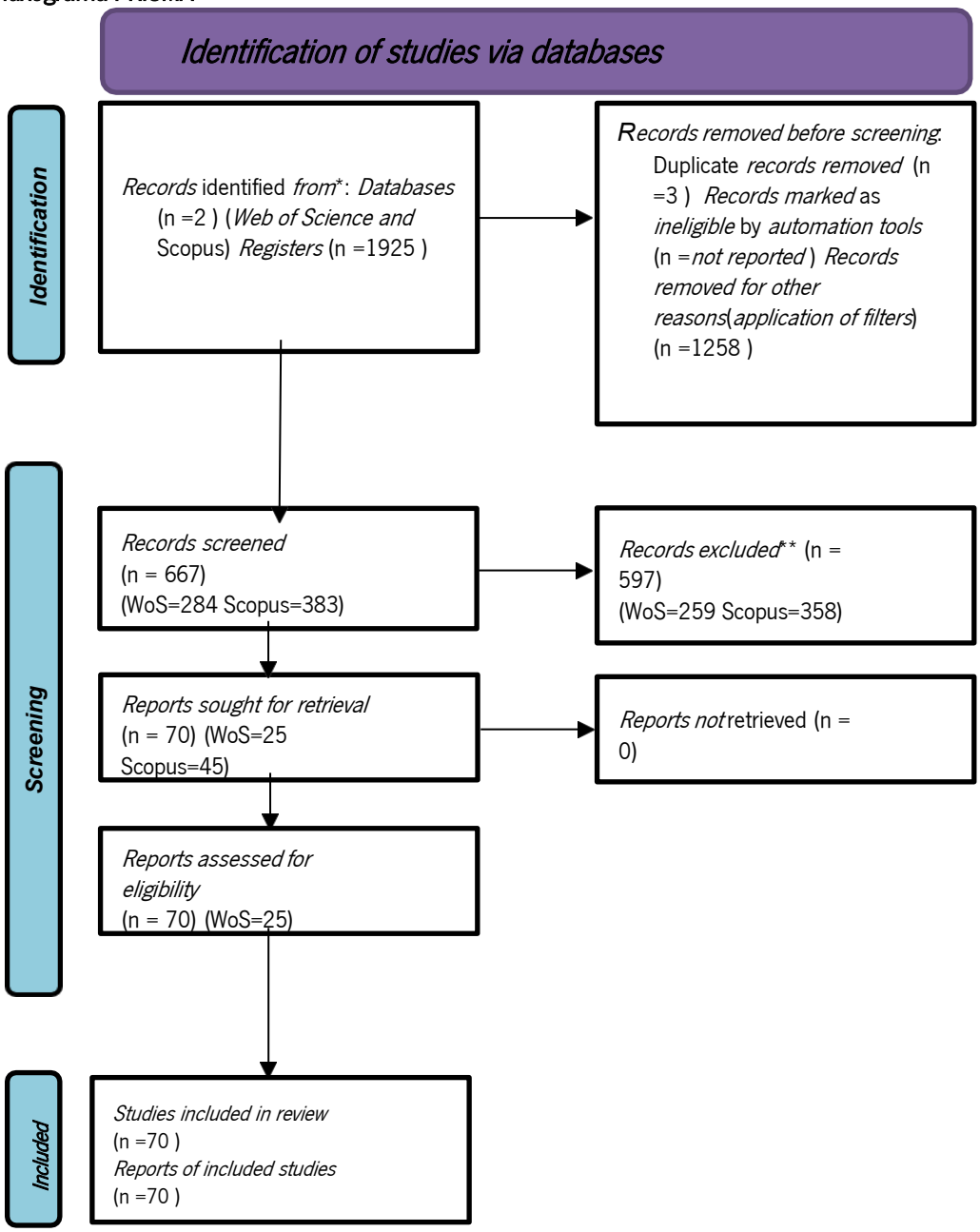
Verizon. (2024). *2024 data breach investigations report.*

Wang, S., Asif, M., Shahzad, M. F., & Ashfaq, M. (2024). *Data privacy and cybersecurity challenges in the digital transformation of the banking sector*. *Computers & Security*, 146, 104051. https://doi.org/10.1016/j.cose.2024.104051

World Bank. (2023). *Global financial cybersecurity outlook 2023.*

Anexo

Fluxograma PRISMA



* *Consider, if feasible to* do *so, reporting the number of records identified from each database or register searched* (*rather than the total number across all databases/ registers*).

** *If automation tools were used, indicate how many records were excluded* by a *human and how many were excluded* by *automation tools*.

Source: Page MJ, et al. BMJ 2021;372:n71. doi: 10.1136/bmj.n71.

This work is licensed under CC BY 4.0. *To view* a *copy of this license, visit* https://creativecommons.org/licenses/by/4.0/