INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Partilha de Informação em Cibersegurança no Setor Bancário

Maria do Rosário da Encarnação Carmo

Mestrado em Engenharia Informática

Orientador:
Doutor Vitor Manuel Basto Fernandes, Professor Associado (com Agregação),
ISCTE - Instituto Universitário de Lisboa

Co-Orientadora:
Doutora Iryna Yevseyeva, Professora Associada em Ciência da Computação,
De Montfort University, Reino Unido

Setembro, 2025

TECNOLOGIAS
E ARQUITETURA

Departamento de Ciências e Tecnologias da Informação

Partilha de Informação em Cibersegurança no Setor Bancário

Maria do Rosário da Encarnação Carmo

Mestrado em Engenharia Informática

Orientador:
Doutor Vitor Manuel Basto Fernandes, Professor Associado (com Agregação),
ISCTE - Instituto Universitário de Lisboa

Co-Orientadora:
Doutora Iryna Yevseyeva, Professora Associada em Ciência da Computação,
De Montfort University, Reino Unido

Setembro, 2025

Às minhas filhas, família e amigos que estiveram ao meu lado.

Agradecimento

Às minhas filhas Mafalda e Catarina, pelo apoio incondicional, pela força, carinho e encorajamento que me proporcionaram ao longo desta jornada. Um agradecimento especial à minha filha Mafalda pelo apoio incansável na revisão linguística da dissertação, pela atenção aos detalhes, contribuindo significativamente para a qualidade do texto.

Aos amigos e família que estiveram ao meu lado, pelo companheirismo e palavras de motivação nos momentos difíceis. A todos aqueles que acreditaram em mim, inspirando-me a alcançar os meus objetivos.

Ao professor e colega de trabalho, Vítor Fernandes, pela sua incansável dedicação no acompanhamento desta dissertação. Agradeço o rigor e a disponibilidade demonstrados nas múltiplas revisões, o empenho nas investigações realizadas e a profundidade das discussões que tanto enriqueceram este trabalho. O seu contributo foi essencial não apenas para a concretização desta dissertação, mas também para o meu crescimento intelectual e pessoal ao longo deste percurso. Um agradecimento à professora Iryna Yevseyeva pelo apoio e colaboração.

Gostaria de expressar o meu agradecimento ao professor Gabriel Cipriano pela ajuda prestada na utilização do software MAXQDA, nomeadamente na codificação dos textos das entrevistas em códigos e grupos. A sua orientação revelou-se essencial para a estruturação e análise dos dados.

E a mim mesma, pela coragem de sonhar, persistir e chegar até aqui.

Resumo

A presente dissertação analisa a partilha de informação em cibersegurança no setor bancário, procurando compreender de que forma a troca de dados sobre ciberameaças e incidentes contribui para a resiliência organizacional face a riscos emergentes.

Metodologicamente, o estudo segue uma abordagem qualitativa, exploratória e construtiva, fundamentada na *Grounded Theory* e na Análise de Conteúdo. Foram realizadas entrevistas semiestruturadas a 17 profissionais de cibersegurança do setor bancário, em Portugal e na União Europeia, selecionados por amostragem teórica até à saturação dos dados. Nos participantes incluiu-se CISOs, entre outros profissionais. O processo analítico envolveu codificação aberta, categorização temática e triangulação dos dados com a literatura existente, recorrendo ao software MAXQDA 2024 como apoio.

Os resultados permitiram identificar barreiras culturais, legais, regulamentares, confiança, e concorrenciais à partilha de informação, bem como iniciativas que favorecem a colaboração interinstitucional. Foi ainda analisada a perceção dos profissionais relativamente às formas de partilha, evidenciando limitações, mas também oportunidades de reforço da cooperação.

Como contributo original, a dissertação propõe uma métrica para avaliar a maturidade da partilha de informação em cibersegurança, orientada para monitorizar práticas colaborativas, apoiar a resposta a incidentes e informar a tomada de decisão estratégica no setor bancário.

Este trabalho contribui para o avanço do conhecimento académico e fornece recomendações práticas que fortalecem a cooperação, reduzem riscos de ciberataques e promovem uma cultura de resiliência no sistema bancário.

Palavras-chave: Cibersegurança; Inteligência em Ameaças Cibersegurança; Setor Bancário; Partilha Informação; Barreiras; Métricas em Cibersegurança.

Abstract

This dissertation analyzes information sharing in cybersecurity within the banking sector, aiming to understand how the exchange of data on cyber threats and incidents contributes to organizational resilience against emerging risks.

Methodologically, the study follows a qualitative, exploratory, and constructive approach, grounded in Grounded Theory and Content Analysis. Semi-structured interviews were conducted with 17 cybersecurity professionals from the banking sector in Portugal and the European Union, selected through theoretical sampling until data saturation was reached. Participants included CISOs, among other professionals. The analytical process involved open coding, thematic categorization, and data triangulation with existing literature, using MAXQDA 2024 software for support.

The results revealed legal, cultural, regulatory, trust, and competitive barriers to information sharing, as well as initiatives that foster inter-institutional collaboration. The professionals' perceptions of sharing practices were also analyzed, highlighting limitations but also opportunities to strengthen cooperation.

As an original contribution, the dissertation proposes a metric to assess the maturity of cybersecurity information sharing, aimed at monitoring collaborative practices, supporting incident response, and informing strategic decision-making in the banking sector.

This research advances academic knowledge and provides practical recommendations to enhance cooperation, reduce the risks of cyberattacks, and promote a culture of resilience within the banking system.

Keywords: Cybersecurity; Cyber Threat Intelligence; Banking Sector; Information Sharing; Barriers; Cybersecurity Metrics.

Índice

Índice de Figuras

Índice de Tabelas

Lista de Siglas e Acrónimos

API - Application Programming Interface

ATT&CK - *Adversarial Tactics, Techniques, and Common Knowledge*

BCE - Banco Central Europeu

BP – Banco de Portugal

CBDCs - *Central Bank Digital Currency*

CERT - *Computer Emergency Response Team*

CIISI-EU - *ECB Cyber Information and Intelligence Sharing Initiative*

CIISI-PT – Centro para Partilha e Análise de Informação sobre Cibersegurança do Setor Bancário Português

CIRAS - *Cyber Incident Response and Assistance Scheme*

CIS - *Critical Security Controls*

CISO - *Chief Information Security Officer*

CMMI - *Capability Maturity Model Integration*

CNCS – Centro Nacional de Cibersegurança Portugal

CNPD – Comissão Nacional de Proteção de Dados

COBIT - *Control Objectives for Information and Related Technologies*

CROE - *Framework Resilience Oversight Expectations*

CSCF - *Customer Security Controls Framework*

CSIRT - *Computer Security Incident Response Team*

CTI - *Cyber Threat Intelligence*

CybOX - *Cyber Obeservable eXpression*

EBA - *European Banking Authority*

EIOPA - *European Insurance and Occupational Pensions Authority*

EM - Estados-Membros

ENISA - *European Union Agency for Cybersecurity*

ESA - *European Supervisory Authorities*

ESMA - *European Securities and Markets Authority*

EU-CSI - EU *Cybersecurity Index*

DORA - *Digital Operational Resilience Act*

DP – Desvio Padrão

FAIR - *Factor Analysis of Information Risk*

FIM - *Financial Market Infrastructures*

FICRO - Fórum com a Indústria para a Cibersegurança e Resiliência Operacional

FS-ISAC - *Financial Services Information Sharing and Analysis Center*

IA – Inteligência Artificial

ISCTE – Instituto Universitário de Lisboa

ISTA - Escola de Tecnologia e Arquitetura do ISCTE

IBM - *International Business Machines Corporation*

IMP - Índice de Maturidade de Partilha

IoAs - *Indicators of Attack*

IoCs - Indicadores de Comprometimento

IoOs - *Indicators of Observation*

ISACs - *Information Sharing and Analysis Centers*

ISACA - *Information Systems Audit and Control Association*

KPIs - *Key Performance Indicator*

KRI - *Key Risk Indicator*

M - Média

MISP - *Malware Information Sharing Platform*

MLR - *Multivocal Literature Review*

NCF – *NIST Cybersecurity Framework*

NDAs - *Non-Disclosure Agreements*

NIS 2- *Network and Information Security Directive*

NIST - *National Institute of Standards and Technology*

OCTAVE - *Operationally Critical Threat, Asset, and Vulnerability Evaluation*

OpenIOC - *Open Incident of Compromise*

OWL - *Web Ontology Language*

PenTest - Penetration Testing in IT Systems

PT – Portugal

QSD - Questionário Sociodemográfico

QNRCS - Quadro Nacional de Referência para a Cibersegurança

RGPD - Regulamento Geral sobre a Proteção de Dados

RJSC - Regime Jurídico da Segurança do Ciberespaço

SIEM - *Security Information and Event Management*

SGSI - Sistema de Gestão de Segurança da Informação

SI – Sistemas de Informação

SOC - *Security Operations Center*

STRIDE - *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*

STIX - *Structured Threat Information eXpression*

SWIFT – *Society for Worldwide Interbank Financial Telecommunication*

TAXII - *Trusted Automated eXange of Indicator Information*

TIBER-PT - *Threat Intelligence-Based Ethical Red Teaming* – Portugal

TIC - Tecnologias de Informação e Comunicação

TISPs - *Threat Intelligence Sharing Platforms*

TLP - *Traffic Light Protocol*

TTPs - *Tactics, Techniques and Procedures*

UE – União Europeia

VERIS - *Vocabulary for Event Recording and Incident Sharing*

WoS - *Web of Science*

Conceitos

Setor Bancário - Refere-se especificamente aos bancos e instituições que oferecem serviços tradicionais como contas correntes e poupança, empréstimos, financiamentos, cartões de crédito, etc.

Setor Financeiro - Conceito mais amplo que engloba o setor bancário, mas também inclui outras instituições financeiras, como seguradoras, corretoras de valores, fundos de investimento, fintechs.

Sistema Financeiro - Conjunto de instituições, mercados, instrumentos e normas que permitem a circulação de dinheiro e crédito dentro de uma economia. O seu principal objetivo é promover a eficiência na alocação de capital, garantindo liquidez, estabilidade e crescimento económico.

Blockchain - Tecnologia de registo distribuído que guarda dados em blocos ligados cronologicamente e protegidos por criptografia. É descentralizado, imutável e transparente, garantindo a integridade e segurança das informações registadas. Cada bloco contém um *hash* único que o conecta ao bloco anterior, dificultando alterações não autorizadas. É utilizado em diversas áreas, incluindo cibersegurança, para assegurar transações e partilha de informação de forma confiável.

CAPÍTULO 1

Introdução

1.1. Enquadramento e Motivação

As instituições financeiras são alvos frequentes de ciberataques, sendo especialmente apelativas dada a natureza sensível e valiosa das informações que processam diariamente. Atualmente, o setor bancário ocupa uma posição central na economia global, tratando diariamente informações sensíveis e valores financeiros substanciais, o que contribui para ser um alvo privilegiado para ciberataques. Nos últimos anos, os ciberataques têm aumentado em complexidade e frequência, consequentemente, o setor bancário necessita de abordagens robustas para garantir a segurança dos dados e a resiliência das suas operações [1]. Tal ainda tem de ser conjugado com as exigências regulatórias, legais e normativas, que visam proteger os dados dos clientes, como também, assegurar a estabilidade e a confiança no sistema financeiro global, o que torna esta realidade ainda mais complexa [2] [3].

Os sistemas financeiros são o pilar da economia moderna, uma vez que permitem a alocação eficiente de capital e impulsionam o crescimento económico, facilitam o investimento produtivo, o acesso ao crédito e a inovação empresarial [4]. Também regulam a estabilidade macroeconómica, evitando crises financeiras que podem afetar significativamente o funcionamento de setores económicos, Estados e relações económicas à escala internacional ou mesmo global [5] [6]. O sistema financeiro promove inclusão e equidade, garantindo que cidadãos e empresas possam aceder a serviços financeiros essenciais [7]. Contribui para o desenvolvimento sustentável, apoiando investimentos em áreas como saúde, educação e infraestruturas [8]. Constitui um fator essencial para a mobilidade social, permitindo a criação de riqueza e o financiamento de projetos individuais e coletivos [9]. Um sistema financeiro robusto é uma ferramenta de soberania nacional, protegendo os países contra-ataques externos e garantindo autonomia económica. Logo, Estados com sistemas financeiros fortes têm maior capacidade de negociação internacional e são menos vulneráveis a crises globais [10][11]. Pelo mencionado, a gestão de risco em cibersegurança é crucial para proteger a integridade dos sistemas financeiros no que concerne às operações bancárias, garantindo a confiança dos clientes e stakeholders [12][13]. Em Portugal (PT) as instituições bancárias são consideradas entidades críticas nacionais que prestam serviços essenciais [14].

O setor bancário europeu é um dos mais visados em ciberataques, ocupando o terceiro lugar, sendo superado pela saúde e administração pública (primeiro e segundo lugar, respetivamente), segundo os incidentes em matéria de *Network and Information Security Directive* (NIS) comunicados pelos Estados-Membros (EM) através do *Cyber Incident Response and Assistance Scheme* (CIRAS) e das

análises recentes da *European Union Agency for Cybersecurity* (ENISA) no relatório *Threat Landscape* de 2024 [15]. O relatório anual de 2024 do CIRAS [16], que agrega os incidentes reportados pelos EM no âmbito da Diretiva NIS, confirma que o setor bancário europeu registou um aumento de incidentes de origem maliciosa, em que os ativos técnicos mais afetados foram sistemas de pagamento, plataformas online e redes internas. A causa predominante é a ação maliciosa, detalhadamente, ataques de DDoS (9%), *bugs de software* (4%), alteração/atualização de software defeituoso (4%), *ransomware* (1%), falha de hardware (1%), seguida de falhas de sistema e erro humano.

A crescente dependência das tecnologias digitais e a rápida evolução das ameaças em cibersegurança têm colocado a cibersegurança no topo das prioridades das instituições financeiras em todo o mundo [1]. Com o objetivo de melhorar a resiliência do setor bancário, visto ser um dos setores críticos em termos europeus e mundiais, a União Europeia (UE) fez a revisão da diretiva NIS 2 e do regulamento *Digital Operational Resilience Act* (DORA) [17] [18] e, em junho de 2024, a ENISA assinou um memorando de entendimento multilateral com as Autoridades Europeias de Supervisão - *European Banking Authority* (EBA), *European Insurance and Occupational Pensions Authority* (EIOPA) e *European Securities and Markets Authority* (ESMA) - para reforçar a cooperação e a troca de informações sobre tarefas de interesse mútuo [1].

A análise teórica deste estudo é essencial para compreender como a cooperação entre instituições financeiras pode aumentar a resiliência a ciberameaças e reduzir as ocorrências e o impacto de ciberincidentes [19]. Especificamente, aborda a gestão de risco em cibersegurança com foco na partilha de informação no setor bancário, analisando abordagens e métodos utilizados, e de que forma essa partilha pode contribuir para o fortalecimento da cibersegurança no setor bancário [20]. Além disso, explora barreiras de dimensões legal, regulatória, normativa e técnica, e a existência de incentivos ou a razão para a sua ausência.

Assim, este estudo tem como objetivo entender como funciona a partilha de informação em cibersegurança no setor bancário, nomeadamente, perceber quais são as suas dificuldades e, posteriormente, contribuir com recomendações de novas perspetivas sobre como motivar uma colaboração mais efetiva e segura entre as instituições bancárias.

Por fim, a escolha pelo presente tema surge de uma confluência entre o meu interesse crescente pela segurança da informação e a consciência da importância vital que este tema tem para a sociedade contemporânea.

1.2. Questões de Investigação

1.2.1. Questões

Q1: Quais são as barreiras legais, regulamentares, normativas, técnicas e concorrenciais que dificultam a partilha de informação sobre cibersegurança no setor bancário?

Q2: Quais as medidas que podem incentivar a uma maior colaboração na partilha de informação sobre cibersegurança entre as instituições bancárias e que tipo de dados podem ser relevantes partilhar?

Q3: Como os incentivos regulatórios, económicos e tecnológicos podem ser usados para promover a partilha de informação sobre cibersegurança entre as instituições bancárias, em conformidade com os requisitos legais e regulamentares e qual o seu impacto na segurança coletiva do setor?

Q4: Que métricas existem, ou poderiam ser desenvolvidas, para avaliar o nível de maturidade na partilha de informação sobre cibersegurança no setor bancário?

1.2.2. Hipóteses

H1: Existem barreiras significativas que dificultam a partilha de informação sobre cibersegurança entre instituições bancárias, sendo as barreiras legais e de concorrência as mais determinantes.

H2: A adoção de medidas específicas, como plataformas seguras de partilha e quadros legais mais claros, pode aumentar significativamente a colaboração entre instituições bancárias, especialmente quando acompanhada da definição clara dos tipos de dados a partilhar.

H3: Os incentivos regulatórios, económicos e tecnológicos (alinhados com os requisitos legais e de *compliance*) têm um papel positivo na promoção da partilha de informação sobre cibersegurança.

H4: Não existem métricas padronizadas para avaliar a maturidade da partilha de informação em cibersegurança no setor bancário.

1.3. Metas

A presente dissertação tem como objetivo analisar a partilha de informação em cibersegurança no setor bancário. Pretende-se compreender como a troca de dados sobre ciberameaças e incidentes contribui para a resiliência do setor, face aos riscos de cibersegurança emergentes. Para alcançar o objetivo, define-se como objetivos específicos: identificar barreiras legais, regulamentares, normativas, técnicas e concorrenciais à partilha eficaz; propor medidas e iniciativas que incentivem a colaboração, definindo a informação a partilhar e a não partilhar; avaliar formas de partilha e planos estratégicos que promovam a maturidade e cooperação no setor; explorar incentivos regulatórios, económicos e organizacionais que favoreçam uma cultura de cooperação; analisar métricas para

avaliar a eficácia e maturidade da partilha, apoiando a resposta a incidentes e a tomada de decisão; e, por fim, desenvolver recomendações práticas que fortaleçam a cooperação e reduzam riscos de ciberataques.

1.4. Método/Processo de Desenvolvimento

A dissertação está organizada em cinco capítulos. O Capítulo 1 introduz e contextualiza a motivação e os objetivos da investigação, o Capítulo 2 apresenta a revisão da literatura onde são discutidos os principais conceitos para a dissertação. O Capítulo 3 detalha o método de investigação, a recolha de dados, amostragem e análise de conteúdo, no Capítulo 4 são apresentados os resultados do estudo e a sua discussão, o Capítulo 5 contém as conclusões, limitações à validade do estudo, recomendações para futuras investigações e para o setor bancário.

A revisão de literatura é multivocal para analisar os estudos feitos sobre partilha de informação em cibersegurança no setor bancário. O método de investigação adotado é de natureza qualitativa. A investigação foi realizada através do estudo de caso de como as entidades bancárias fazem a partilha de informação em cibersegurança. Para tal, seguiu-se uma abordagem da teoria *Grounded Theory* [21], utilizando entrevistas semiestruturadas a funcionários de entidades bancárias como principal método de recolha e o método de Análise de Conteúdo [22][23] para a análise de dados. Esta abordagem permite uma compreensão aprofundada das perceções e experiências dos profissionais do setor sobre os desafios e as oportunidades da partilha de informação em cibersegurança.

Os resultados obtidos foram confrontados com as conclusões extraídas da revisão de literatura, proporcionando uma análise crítica das práticas atuais e as possíveis limitações da partilha de informação em cibersegurança e das suas métricas, barreias e incentivos encontrados durante a investigação. Com base nas descobertas, esta dissertação propõe possíveis melhorias e recomendações para incentivar a partilha de informação em cibersegurança dentro do setor bancário e aborda os benefícios de uma maior cooperação interinstitucional.

CAPÍTULO 2

Revisão da Literatura/Estado da Arte

Esta revisão da literatura analisa o estado da arte da partilha de informação em cibersegurança no setor bancário, com foco nas dimensões legal, regulatória, normativa e técnica, e nos métodos usados para enfrentar os desafios da área, perspetivas de colaboração, incentivos e métricas.

A revisão de literatura segue o método *Preferred Reporting Items for Systematic Reviews and MetaAnalyses* (PRISMA)[24], garantindo rigor e transparência. Esta abordagem estruturada facilita uma visão abrangente do estado atual da investigação neste campo. O processo decorre em duas fases: (i) definição de critérios, questões de investigação, palavras-chave, bases de dados e exclusão de duplicados e de artigos que não se enquadrem no estudo; (ii) análise dos artigos selecionados e elaboração da conclusão.

2.1. Definição de Critérios

2.1.1. Bases de Dados

As bases de dados usadas foram de editoras científicas como *Scopus* [25], *Web of Science (WoS)* [26] e EBSCO [27]. A escolha deveu-se às suas coberturas temáticas amplas (economia, gestão e tecnologia), rigor editorial e ferramentas de pesquisa avançadas [28]. Em contraste, as bases *IEEE Xplore* e *ScienceDirect* são mais restritas à engenharia elétrica, eletrónica, redes, robótica, energia, ciências físicas, ciências da saúde e ciências de vida, portanto, não ofereciam a mesma adequação ao carácter teórico desta dissertação.

2.1.2. Palavras-Chave

A pesquisa usou o conjunto de palavras-chave definido e foi composta por duas partes unidas por um "*AND*" para criar a interseção dos resultados obtidos de ambas as partes. A primeira parte da pesquisa especifica artigos que se referem a gestão de risco, cibersegurança e *frameworks* de risco. Já a segunda parte está relacionada com o setor bancário.

("*Cybersecurity" or "Risk Management" or "Cyber Security Metrics" or "Cybersecurity risk phases" or "CyberSecurity Metrics" or " Cybersecurity Risk Management" or "Risk Management Metrics" or "Risk Management Framework" or "Cyber Threat Intelligence")*

AND ("Banking Sector" or "Legal Risk Standards in Banking" or "risk management metrics for banking" or "Information sharing in banking")

2.1.3. Critérios de Inclusão

Os critérios de inclusão definem quais as propriedades que os artigos devem apresentar para serem incluídos, sendo: artigos em inglês ou português; incluir as palavras-chave no título ou no resumo; publicações dos últimos 5 anos (a partir de 2020, inclusive); o tipo de publicação ser artigo de revista, artigo com revisão por pares ou artigo de conferência; área de pesquisa – sistemas de informação, economia e negócio; tipo de fonte *Journal*.

2.1.4. Critérios de Exclusão

Os critérios de exclusão definem características que não devem estar presentes nos artigos incluídos, como artigos: duplicados; não diretamente relacionado com o tema; com acesso não aberto.

2.1.5. Seleção dos Artigos

Primeiramente, eliminação de artigos que cumpram os critérios de exclusão e, em seguida, dentro dos artigos obtidos, selecionar os artigos relevantes para a revisão de literatura. As figuras em anexo (Apêndice A, B e C) ilustram a pesquisa organizada em secções baseadas em palavras-chave (Conceitos, População), critérios de inclusão e exclusão.

2.2. Revisão Literatura

Com o objetivo de contextualizar a investigação realizada, este capítulo apresenta um resumo dos principais contributos encontrados na literatura científica e "cinzenta" relevante para esta dissertação. A pesquisa nas bases de dados *WoS* (21-12-2024), *Scopus* (05-01-2025) e EBSCO (20-04-2025) resultou em 43, 100 e 47 artigos, respetivamente (Apêndices A, B e C). No entanto, destes artigos, apenas dois abordam diretamente a gestão de cibersegurança no setor bancário. Este domínio caracteriza-se por uma evolução constante, impulsionada por avanços tecnológicos e novas ameaças, mas verifica-se uma escassez de estudos académicos que tratem os desafios práticos enfrentados pelas instituições bancárias. Para colmatar esta lacuna, recorreu-se a fontes de informação “cinzentas”, como:

- Relatórios de entidades especializadas (ENISA; *National Institute of Standards and Technology* (NIST); e o Centro Nacional de Cibersegurança (CNCS));
- Publicações institucionais (bancos centrais, associações bancárias e empresas de cibersegurança);
- Normas e regulamentos (ISO 27001; ISO 27005; Regulamento Geral sobre a Proteção de Dados (RGPD); NIS 2; DORA).

Estas fontes são particularmente relevantes em cibersegurança, dada a sensibilidade dos dados e a confidencialidade das operações bancárias, que limitam a divulgação em canais académicos tradicionais. Apesar de não serem revistos por pares, os relatórios técnicos e *white papers* oferecem

insights práticas valiosos. A inclusão destas fontes permite uma visão mais abrangente e atualizada da gestão de risco em cibersegurança no setor bancário, aproximando a teoria académica da prática do mercado. Para tal, foi aplicado o método PRISMA (Apêndice D), complementado por pesquisa por *snowball* [29] [30] e *multivocal literature review* (MLR) [31].

A cibersegurança é definida pelo CNCS como a prevenção, proteção e recuperação de sistemas e comunicações eletrónicas, garantindo disponibilidade, integridade, autenticidade, confidencialidade e não repúdio [32]. Já a ENISA acrescenta que envolve prevenção, deteção, mitigação, análise e investigação de incidentes, abrangendo ainda resiliência, robustez, responsabilização e fiabilidade [33]. Perante o aumento e a complexidade das ameaças, a cibersegurança procura dar resposta através da gestão de risco, que consiste em identificar, avaliar e mitigar riscos associados à segurança da informação e sistemas digitais, protegendo ativos contra incidentes como roubo de dados, *ransomware* ou interrupções operacionais. A *International Business Machines Corporation* (IBM) define a gestão de risco de cibersegurança como o processo de identificar, priorizar, gerir e monitorizar riscos em sistemas de informação, essencial para a proteção contra ciberataques e outras ameaças [34]. Para ser eficaz, deve ser transversal à organização e assumida pela gestão de topo, apoiada em modelos de referência internacional que contemplem processos, pessoas e tecnologias [35]. Esta gestão exige avaliar os ativos, reconhecendo a diversidade de riscos e impactos em diferentes níveis organizacionais [36], permitindo desenvolver estratégias de mitigação, priorização e planeamento, de modo a alinhar risco e retorno. Trata-se de um processo sistemático que identifica, avalia e prioriza ameaças e vulnerabilidades, ajudando as organizações a proteger objetivos de negócio com medidas adequadas [35]. A gestão de risco de cibersegurança no setor bancário é crítica devido à complexidade das operações financeiras e à elevada exposição a ataques. Em PT, os bancos registaram uma média de 2.684 ciberataques por semana nos últimos seis meses, sendo o quarto setor mais visado, após educação/investigação, saúde e transportes [37]. Para manter a confiança dos clientes e garantir a continuidade do negócio, os bancos devem adotar uma estratégia holística que integre gestão, tecnologia e operações [38]. A colaboração entre instituições bancárias e reguladores é igualmente essencial para reforçar a resiliência em cibersegurança. A dependência de fornecedores externos aumenta a superfície de ataque, tornando essencial garantir que parceiros adotem medidas de segurança adequadas [39]. Com a digitalização dos serviços bancários, a proteção de dados sensíveis é crítica para manter a confiança dos clientes e a integridade das transações. Tecnologias como inteligência artificial permitem detetar e responder a ameaças em tempo real, reforçando a prevenção de fraudes e ciberataques [40] [41].

O "risco" pode ser entendido como um evento ou circunstância com potencial efeito adverso na segurança das redes e sistemas de informação. Como não pode ser totalmente eliminado, torna-se essencial definir e implementar uma estratégia transversal que assegure um processo sistematizado e

contínuo de gestão de riscos [36]. No âmbito da gestão de risco é essencial compreender alguns conceitos [36]: Ameaça (potencial causa de um incidente indesejado que pode provocar danos a um sistema, indivíduo ou organização); Vulnerabilidade (fraqueza de um ativo ou controlo que pode ser explorada por uma ou mais ameaças); Impacto (resultado decorrente da verificação de um determinado evento de segurança sobre um ou mais recursos, traduzindo-se normalmente em consequências diretas ou indiretas); e Risco (circunstância ou evento razoavelmente identificável com um efeito potencial adverso na segurança das redes e sistemas de informação).

No processo de gestão dos riscos, as organizações identificam ameaças que possam explorar vulnerabilidades, bem como os níveis de risco associados, avaliando probabilidade e impacto [36], conforme ilustrado pela relação entre estes conceitos (Anexo A). A valorização de um ativo ou criticidade deve basear-se no impacto de uma eventual falha ou indisponibilidade, garantindo que recebe um nível adequado de proteção em função da sua importância. Esta classificação pode ter por base requisitos legais, valor, criticidade, valor de reposição, recuperação, limpeza ou substituição da informação ou, ainda, os valores de confidencialidade, integridade e disponibilidade, aplicando-se a fórmula: Max (Confidencialidade; Integridade; Disponibilidade) = Valorização de ativo [36]. Segundo o Guia para Gestão de Riscos em matérias de Segurança da Informação e Cibersegurança do CNCS [36], este processo envolve várias fases: Estabelecer o contexto (definição de âmbito, ativos, ambiente e objetivos); Levantamento do risco (identificação de ameaças e vulnerabilidades, avaliação de controlos e priorização dos riscos); Análise do risco, combinando probabilidade e impacto, que pode ser qualitativa (escalas subjetivas de Muito Baixo a Muito Alto) ou quantitativa (valores numéricos e dados históricos). No setor bancário, classificado como operador de serviços essenciais pelo Regime Jurídico da Segurança do Ciberespaço (RJSC) [42], aplica-se uma matriz de risco mais conservadora [36]. Seguem-se a avaliação e tratamento do risco (mitigação, transferência, aceitação ou eliminação) e a aceitação formal dos riscos residuais. Este processo inclui ainda comunicação e consulta contínuas com *stakeholders* e monitorização e revisão das medidas implementadas, garantindo adaptação a mudanças e novas ameaças. Sendo cíclico, deve ser repetido regularmente para assegurar a melhoria contínua da postura de cibersegurança [36] (Anexo B). A implementação de um processo bem estruturado protege os ativos digitais e assegura a continuidade do negócio. Complementarmente, a norma ISO/IEC 27005 [36] fornece orientações específicas para a gestão de riscos de segurança da informação.

A gestão de incidentes compreende as fases de prevenção (identificar e proteger), deteção, resposta e recuperação, conforme o Quadro Nacional de Referência para a Cibersegurança (QNRSC) [34]. Para aplicar estas medidas, as organizações devem investir em três pilares: o *Chief Information Security Officer* (CISO), responsável máximo pela segurança da informação; o *Security Operations Center* (SOC), que fornece infraestruturas e equipas de suporte; e o *Computer Security Incident*

Response Team (CSIRT) [34], equipa especializada em resposta a incidentes. Segundo o QNRSC (Anexo C), as fases incluem: Identificação do risco, que avalia contexto, ativos críticos e riscos, permitindo priorizar investimentos; Proteção, com medidas de segurança em Pessoas, Processos e Tecnologia; Deteção, para identificar incidentes atempadamente; Resposta, definindo ações de mitigação; e Recuperação, com planos que assegurem resiliência e retoma célere da atividade [34].

2.2.1. Barreiras e Partilha de Informação em Cibersegurança

De acordo com [43], no setor bancário a proteção de informações sensíveis e a integridade das operações financeiras são essenciais para garantir a confiança dos clientes, a estabilidade do mercado e a conformidade legal. Com ameaças de cibersegurança cada vez mais sofisticadas, o setor bancário enfrenta riscos operacionais e obrigações regulatórias complexas. A partilha de informação surge da necessidade de fazer face às ameaças de cibersegurança, sendo crucial pois, de acordo com [44] "… constata-se que é praticamente impossível um Estado ou organização garantir isoladamente a segurança do seu ciberespaço. Reter informações sobre ameaças e ataques apenas para si acaba por expor todos a consequências inevitáveis. Assim, a partilha de informação é vital para a segurança no ciberespaço.". Esta colaboração permite uma resposta mais eficaz às ameaças de cibersegurança, melhorando as capacidades de prevenção, deteção, resposta e recuperação de incidentes. De acordo com o DORA [18] a partilha de informação é essencial para o sucesso da prevenção do risco "… A eficácia das medidas de deteção e prevenção de riscos associados às Tecnologias de Informação e Comunicação (TIC) depende da partilha regular de informações entre entidades financeiras, o que aumenta a sensibilização para ciberameaças, previne incidentes, melhora a contenção e acelera a recuperação …". No entanto há várias barreiras tanto internas como externas, que dificultam ou limitam essa partilha. Essa podem ser classificadas em legais, regulamentares, normativas, técnicas, culturais e de concorrência [45].

As normas, leis e regulamentos de cibersegurança visam prevenir, detetar, responder e recuperar incidentes, bem como proteger dados e gerir riscos. No enquadramento legal e normativo do setor bancário destacam-se normas internacionais, leis nacionais, regulamentos europeus, diretivas comunitárias e diretrizes setoriais, cada um com objetivos específicos na regulação e orientação das práticas de segurança da informação. Nas normas internacionais destacam-se a ISO/IEC 27001 que tem requisitos para estabelecer, implementar e manter um Sistema de Gestão de Segurança da Informação (SGSI), que se foca na gestão de riscos e na implementação de controlos de segurança abrangentes) [46]; ISO/IEC 27005 (orientações para gestão de riscos de segurança da informação, em alinhamento com a ISO/IEC 27001) [36]; ISO/IEC 27035 (gestão de incidentes de segurança da informação (detetar, reportar, responder e aprender)) [47]; ISO/IEC 31000 (princípios e orientações

gerais para a gestão de riscos) [36].

No âmbito europeu o Regulamento Geral sobre a Proteção de Dados (RGPD, UE 2016/679) estabelece as regras para o tratamento e livre circulação de dados pessoais na UE [48]. Mais recentemente, o Regulamento DORA (UE 2022/2554) introduziu um quadro normativo específico para a resiliência operacional digital do setor financeiro, impondo requisitos rigorosos de gestão de riscos e continuidade operacional [17][18]. No âmbito das diretivas, a Diretiva (UE) 2016/1148, conhecida como Diretiva NIS, foi a primeira legislação europeia a estabelecer medidas para assegurar um elevado nível comum de segurança das redes e sistemas de informação [36]. Esta diretiva foi posteriormente substituída pela Diretiva NIS 2 (UE 2022/2555), aprovada em 2022, que reforça as exigências de cibersegurança para setores considerados críticos [49]. Por fim, destacam-se as diretrizes setoriais, que funcionam como orientações técnicas e operacionais, entre elas, as EBA *Guidelines on ICT and Security Risk Management*, que orientam a gestão de riscos tecnológicos e de cibersegurança no setor financeiro europeu em articulação com o regulamento DORA [50] e as ESMA *Guidelines*, que promovem a convergência supervisora e a aplicação consistente da legislação nos mercados financeiros [51].

Na legislação nacional destaca-se a Lei n.º 46/2018, de 13 de agosto, estabeleceu o RJSC, transpondo para a ordem jurídica nacional a Diretiva (UE) 2016/1148 (Diretiva NIS) [36]. O regime foi posteriormente atualizado pelo Decreto-Lei n.º 65/2021, em alinhamento com a nova Diretiva NIS 2 [36]. No contexto específico do setor bancário, a Lei do Sigilo Bancário (DL 298/92, Art. 78.º e seguintes) impõe restrições legais à partilha de dados dos clientes sem a devida autorização [52]. Existem ainda regulamentos normativos complementares, como a Instrução n.º 21/2019 do Banco de Portugal (BP), que estabelece o dever de reporte de incidentes de cibersegurança significativos ou severos por parte das entidades supervisionadas [53]. Assim, verifica-se que o enquadramento da cibersegurança no setor bancário resulta da articulação entre normas internacionais, legislação nacional, regulamentos europeus de aplicação direta, diretivas comunitárias transpostas para a ordem jurídica dos EM, diretrizes setoriais de autoridades de supervisão, garantindo uma abordagem multilateral e integrada à segurança da informação [54] [55].

Os desafios técnicos, especialmente no contexto de *Central Bank Digital Currency* (CBDCs) e pagamentos digitais transfronteiriços, tornam necessária uma abordagem que equilibre privacidade e integridade transacional [56]. Já de acordo com [57], na transformação digital do setor bancário, surgem barreiras significativas à partilha de informação em cibersegurança: a integração de sistemas legados apresenta desafios técnicos; a evolução das normas torna a conformidade complexa; os riscos com terceiros ressaltam barreiras concorrenciais e técnicas; e a necessidade de manter a confiança dos clientes evidencia barreiras culturais e de reputação.

A dimensão da concorrência reflete-se no receio dos bancos em partilhar informação sensível,

uma vez que a cibersegurança é vista como vantagem competitiva. O medo de expor vulnerabilidades e comprometer a reputação perante clientes e investidores constitui um fator adicional de resistência [58] [59]. De acordo com [60], a proteção de dados sensíveis no setor bancário é frequentemente comprometida por barreiras legais e regulatórias, que impõem restrições severas à partilha. A dimensão cultural reflete a resistência interna à mudança, receio de exposição, falta de cultura de cooperação entre instituições bancárias e receio de perder vantagem competitiva ao partilhar vulnerabilidades.

De acordo com [61] apresenta uma análise abrangente da literatura sobre *Cyber Threat Intelligence* (CTI), destacando obstáculos como a falta de automatização, ausência de padrões interoperáveis, questões de confiança entre organizações e limitações legais que dificultam a adoção de práticas colaborativas. Já o artigo [57] é focado especificamente no setor bancário, evidenciando como a fragmentação regulatória, a pressão por conformidade e a ausência de mecanismos claros de coordenação impedem uma partilha eficaz de dados e inteligência de cibersegurança. No DORA também é identificado que "…na ausência de orientações a nível da união, diversos fatores, em especial a incerteza quanto à sua compatibilidade com as regras em matéria de proteção de dados, *anti-trust* e de responsabilidade, parecem ter inibido a referida partilha de informações…" [18] e as dúvidas que existem "…quanto ao tipo de informações que podem ser partilhadas com outros intervenientes no mercado, ou com autoridades não supervisoras (como a ENISA, para um contributo analítico, ou a Europol, para fins de aplicação da lei), levaram a que informações úteis não fossem partilhadas…" [18].

Assim, é necessário "criar mecanismos na UE que permitam acordos voluntários de partilha em ambientes fiáveis, ajudando o setor financeiro a prevenir e responder coletivamente às ciberameaças." [38]. Do ponto de vista legal, o RGPD impõe restrições rígidas à circulação de dados pessoais entre entidades, tornando o processo mais burocrático [48]. Além disso, as leis nacionais de sigilo bancário limitam a divulgação de informação financeira sem autorização [52]. Na dimensão regulamentar, de acordo com [62], destacam-se a sobreposição de normas, a burocracia e a falta de critérios harmonizados, o que cria barreiras práticas à cooperação. O regulamento DORA obriga à comunicação de incidentes aos reguladores, mas mantém a partilha entre bancos como voluntária [18]. De acordo com [63], "A justificação para a notificação voluntária reflete a necessidade de equilibrar a visão de supervisão com o encargo operacional e as preocupações de confidencialidade das entidades financeiras", ou seja, a sensibilidade da informação e a falta de critérios objetivos universais justificam a abordagem voluntária. A diretiva NIS 2 também estabelece requisitos de cibersegurança para entidades críticas, mas não impõe um mecanismo centralizado de partilha [49].

Detalhando, reguladores como o BCE e o BP exigem medidas rigorosas de cibersegurança, mas simultaneamente reforçam restrições de confidencialidade, o que limita a cooperação [64] [65]. Em

2022 o BP, aprovou um quadro de referência para a realização de testes de cibersegurança avançados, conhecido como *Threat Intelligence-Based Ethical Red Teaming* – PT (TIBER-PT), que visa avaliar e fortalecer a resiliência das infraestruturas de TIC e cibersegurança das instituições bancárias em PT. Este quadro incentiva a partilha de informação sobre ameaças e vulnerabilidades, mas sempre dentro dos limites impostos pelas obrigações de confidencialidade e proteção de dados [65].

No plano normativo, a diversidade de *frameworks* (ISO 27001, NIST, Basileia III) dificulta a harmonização de práticas, criando entraves à interoperabilidade e à comunicação eficaz sobre ameaças [66]. Quanto às barreiras técnicas, as heterogeneidades das infraestruturas de TIC complicam a partilha automatizada de dados. O DORA procura mitigar essas falhas ao impor requisitos mais rigorosos de gestão de riscos e resiliência operacional e introduz ferramentas como os *Penetration Testing in IT Systems* (*PenTest*), que aumentam a capacidade de as instituições prevenirem e mitigarem ciberameaças [18].

Para fortalecer a resiliência das instituições bancárias, promover a transparência e assegurar a cooperação internacional foram criadas *frameworks*. A adesão a normas e regulamentações é uma exigência legal e estratégica, mitigando riscos e evitando sanções, perda de confiança e danos reputacionais [34]. Essas *frameworks* reúnem boas práticas para identificar, proteger, detetar, responder e recuperar incidentes, estruturando a gestão de riscos em ambientes digitais complexos [67] [68]. Entre as principais destacam-se *NIST Cybersecurity Framework* (CSF), ISO/IEC 27001, *Critical Security Controls* (CIS) *Controls,*o *Control Objectives for Information and Related Technologies* (COBIT) e o MITRE *Adversarial Tactics, Techniques, and Common Knowledge* (ATT&CK) [67] [68]. A NIST CSF, baseada parcialmente no COBIT, organiza-se em cinco funções (identificar, proteger, detetar, responder e recuperar) [69]; a ISO/IEC 27001 define requisitos para um SGSI [46]; o COBIT, desenvolvido pela *Information Systems Audit and Control Association* (ISACA), oferece boas práticas de governação de Tecnologias de Informação e Comunicação (TIC) [70]; os CIS *Controls* apresentam 18 controlos críticos [71]; e o MITRE ATT&CK descreve táticas reais de adversários para apoiar a deteção e resposta a ataques [72]. No setor financeiro, destaca-se a *Framework Resilience Oversight Expectations* (CROE) do Banco Central Europeu (BCE), publicada em 2018, focada na resiliência das *Financial Market Infrastructures* (FMIs). Estrutura-se em cinco categorias de gestão de risco (gestão, proteção, deteção, resposta e recuperação) e três adicionais (testes, análise situacional e aprendizagem), com base no *Guidance on Cyber Resilience for FMIs* e na NIST CSF [69] [73] [74]. Outras metodologias incluem o *Factor Analysis of Information Risk* (FAIR), que quantifica riscos em termos financeiros [75] [76]; o *Operationally Critical Threat, Asset, and Vulnerability Evaluation* (OCTAVE), que apoia a avaliação estratégica e operacional [77] [78]; e o STRIDE, desenvolvido pela Microsoft, para modelar ameaças em *software*, categorizadas em *Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service e Elevation of Privilege* [79] [80].

Atualmente, as entidades financeiras devem reportar ao BP incidentes significativos ou severos em 2h, seguindo-se um reporte intercalar em 10 dias úteis e um final em 30 dias. Os incidentes devem ser também reportar ao CNCS e, se envolver dados pessoais, à Comissão Nacional de Proteção de Dados (CNPD). Informação relevante que sirva de suporte ao reporte de incidente, nomeadamente informação com maior detalhe sobre a arquitetura dos sistemas afetados, o impacto provável do incidente, medidas mitigadoras adotadas e/ou previstas ou outros documentos equivalentes que sejam relevantes, são de carácter voluntário [53]. A informação é partilhada com o BP, mas não é partilhada com as restantes instituições bancárias.

A sofisticação das ciberameaças no setor bancário exige colaboração entre instituições, sendo a partilha de informação crucial em todas as fases da cibersegurança [81]. Na prevenção, permite antecipar riscos e adotar medidas proativas com base em vulnerabilidades e táticas de agentes maliciosos [18] [65]. Na deteção, facilita a identificação rápida de intrusões, *malware* ou exploração de vulnerabilidades. De acordo com o estudo [82] , confirma-se que a partilha de dados potência técnicas de *machine learning*, aumentando a eficácia na deteção de ataques. Já na resposta, a coordenação entre bancos é essencial para mitigar impactos de incidentes. A recuperação é reforçada pela troca de experiências e melhores práticas, permitindo restaurar operações de forma eficiente, fortalecer defesas e preservar a confiança dos clientes no sistema financeiro [18] [83].

2.2.2. Medidas para Colaboração entre Instituições Bancárias

De acordo com um estudo [84], existem muitas normas e plataformas para a partilha de informação sobre ciberameaças, onde foram feitos vários esforços de normalização para facilitar essa partilha, como exemplo *Trusted Automated eXange of Indicator Information* (TAXII), *Structured Threat Information eXpression* (STIX), *Cyber Obeservable eXpression* (CybOX) e *Open Incident of Compromise* (OpenIOC) que é uma normalização e plataforma. Do estudo que foi feito sobre as 22 *Threat Intelligence Sharing Platforms* (TISPs), os autores concluem que estas oferecem benefícios significativos na luta contra ameaças de cibersegurança, mas existe uma necessidade urgente de padronização, melhores práticas de interoperabilidade e políticas de confiança que incentivem a colaboração segura e eficiente. Verificou-se também que as TISPs apenas serviam para recolha de dados, não existindo uma análise dos dados, e conclui-se que a norma de descrição STIX e de partilha TAXII são as mais usadas em todas as TISPs.

A arquitetura STIX foi publicada entre 2013 e 2014 e atualmente tem dezoito conceitos fundamentais de cibersegurança com construções independentes e reutilizáveis [85]. Estas descrevem os observáveis de cibersegurança (v.g.: hashes, endereços IP), os indicadores, os incidentes, as técnicas e os procedimentos táticos dos adversários (v.g.: padrões de ataque; cadeias de destruição), os alvos

de exploração (v.g.: vulnerabilidades; pontos fracos), os cursos de ação (v.g.: resposta a incidentes; estratégias de atenuação), as campanhas de ciberataques e os atores das ciberameaças, etc., (Anexo D). Esta arquitetura é importante para fornecer dados significativos aos processos de segurança de informação, como a prevenção, a deteção ou resposta [84].

A nível internacional para o setor financeiro existem várias plataformas para a partilha de informação, a mais conhecida e usada é a *Financial Services Information Sharing and Analysis Center* (FS-ISAC) [86], é uma organização sem fins lucrativos, orientada pelos seus membros que atualmente são 7.000 e de mais de 70 países, que promove a partilha de informação em cibersegurança, a cooperação em instituições e a resiliência no sistema financeiro global, protegendo as instituições bancárias e os indivíduos que servem. Através de uma rede de partilha de informações em tempo real, o FS-ISAC utiliza Inteligência Artificial (IA) na análise de ameaças, o conhecimento e as práticas dos seus membros para a segurança e defesa coletiva do setor financeiro, mas a adesão ainda não é uniforme.

A nível europeu tem-se conhecimento do CIRAS, uma plataforma da ENISA, que tem como objetivo ajudar e coordenar a resposta a incidentes de cibersegurança a nível europeu, especialmente no setor financeiro. A iniciativa procura melhorar a capacidade de resposta e a cooperação entre as entidades financeiras em caso de ataques [87]. A *Cyber Information and Intelligence Sharing Initiative* (CIISI-EU), é uma iniciativa de partilha de informação e inteligência de cibersegurança estabelecida pelo BCE, em conjunto com as principais infraestruturas financeiras europeias, a ENISA e a Europol, com o objetivo de fortalecer a resiliência e cibersegurança do setor financeiro na Europa, inspirada no modelo dos *Information Sharing and Analysis Centers* (ISACs) [88]. Lançada em fevereiro de 2020, a CIISI-EU visa criar uma comunidade de confiança onde as entidades participantes podem partilhar informações estratégicas, operacionais, táticas e técnicas vitais, discutir ameaças de cibersegurança e trocar as melhores práticas [89]. Com o DORA a colaboração, antes vista como um desafio, surge agora como um pilar essencial para mitigar riscos digitais em tempo real. "… importa incentivar as entidades financeiras a partilharem informações específicas e sensíveis sobre ciberameaças, aproveitando conhecimentos e experiências práticas a nível estratégico, tático e operacional, para reforçar a capacidade de avaliar, monitorizar, defender e responder a incidentes" [18]. A partilha de informação nos incidentes é obrigatória com os reguladores competentes de cada EM, "…deverão apresentar essa notificação às autoridades nacionais competentes, que subsequentemente a deverão transmitir ao BCE." [18]. A partilha de informação e informações sobre as ciberameaças e as vulnerabilidades com os parceiros é feita numa base voluntária [90].

Uma das principais iniciativas em PT é o Fórum com a Indústria para a Cibersegurança e Resiliência Operacional (FICRO), estabelecido pelo BP. Este fórum visa aprofundar a cooperação entre o BP e as instituições supervisionadas, fomentando o diálogo e a partilha de informação sobre cibersegurança.

Os objetivos incluem sensibilizar os membros dos órgãos de administração para a importância da prevenção de eventos de cibersegurança, fomentar a compreensão dos requisitos legais e regulamentares, e debater diferentes abordagens à prevenção de incidentes [65] [83]. Além disso, o BP lançou a plataforma CIISI-PT, um centro para a partilha e análise de informação sobre ameaças de cibersegurança no setor bancário. Em atividade desde setembro de 2023, esta plataforma tem mostrado sinais positivos de crescimento, mas a participação das instituições bancárias ainda é limitada [83].

O *Computer Emergency Response Team* (CERT) é um serviço oferecido pelo CNCS, que desempenha um papel crucial no apoio às organizações nacionais, na gestão de incidentes de cibersegurança, responsável por monitorizar, coordenar e responder a incidentes de cibersegurança. O principal objetivo de um CERT é proteger sistemas de informação, detetar e mitigar ciberataques, fornecer orientação técnica e ajudar as organizações a recuperar de incidentes de segurança. O CERT integra-se numa rede global de resposta a incidentes, promovendo um ecossistema de confiança para melhorar a resiliência e cibersegurança de PT [91].

O CNCS [92], em colaboração com a RNCSIRT [93], desenvolveu uma taxonomia prática e detalhada que se alinha com esse enquadramento legal, garantindo coerência entre a operacionalização técnica e os requisitos regulamentares. O CNCS tem uma taxonomia reduzida (Anexo E), que é complementada pela RNCSIRT_Taxonomia_v3.3 [93], que tem taxonomia para incidentes de segurança, correlação entre eventos e incidentes e múltiplas classificações.

Na informação a partilhar entre os bancos na NIST SP 800-150 [94], identifica a partilha de indicadores de Comprometimento (IOCs), como endereços IP maliciosos, domínios, *file hashes*, *URLs* suspeitos. Essenciais para prevenir e deteção precoce de ameaças. Táticas, Técnicas e Procedimentos (TTPs) usados por adversários como padrões de ataque, *malware* e vulnerabilidades exploradas. Permite fortalecer defesa coletiva com base nas ações reais dos adversários. Avisos de vulnerabilidades e *patches*, como divulgação responsável de CVEs ajuda bancos a fechar brechas antes que sejam exploradas globalmente. Dados a não partilhar de acordo com [95], são dados internos sensíveis, como registos de utilização, relatórios internos com dados reputacionais ou vulnerabilidades específicas devem ser guardados sob NDA ou acordos contratuais, limitando o acesso. Informação privada sobre arquitetura interna, detalhes de topologia de rede, credenciais, ou *logs* detalhados não devem circular sem anonimização ou agregação mínima, para prevenir exploração por terceiros.

2.2.3. Incentivos para Promover a Partilha de Informação entre Instituições Bancárias

O artigo [96] destaca a necessidade de colaboração entre organizações para detetar e mitigar ciberataques sofisticados, sobretudo os que exploram vulnerabilidades desconhecidas (*zero-day*).

Apesar da existência de ferramentas técnicas, a adoção real é limitada por falta de confiança e incentivos. Os autores propõem uma plataforma colaborativa que permite trocar alertas de rede, mesmo entre concorrentes, através de fluxos ponto a ponto em (quase) tempo real, aumentando assim as suas capacidades gerais de deteção. Em resumo, o artigo aborda a falta de confiança e de incentivos que dificultam a colaboração em cibersegurança, oferecendo uma solução descentralizada que promove a partilha de informação crítica entre organizações.

De forma complementar o artigo anterior, o artigo [97] observa que obrigações e sanções desencorajam a partilha voluntária, restringindo-a ao estritamente necessário. Assim, propõe, um novo paradigma na troca de informação sobre cibersegurança, que incentiva todos os participantes (produtores, consumidores, investidores, doadores e proprietários) a partilhar informações relevantes de forma dinâmica, onde todos terão incentivos específicos para partilhar, investir e consumir informações de inteligência sobre ameaças e riscos. O artigo apresenta uma revisão abrangente sobre os conceitos fundamentais e tecnologias associadas à Inteligência de Ameaças em Cibersegurança (CTI), focando-se em taxonomias, padrões de partilha e ontologias, como STIX™ e Web Ontology Language (OWL), evidenciando como podem ser usados para uniformizar e melhorar a partilha de inteligência de ameaças. Esta abordagem é importante especialmente considerando o problema de interoperabilidade. Também sugere a utilização de Blockchain e contratos Inteligentes (dApps) como solução para os problemas de confiança e descentralização, alinhada com tendências emergentes em cibersegurança. Esta proposta demonstra uma visão inovadora sobre a partilha de inteligência de ameaças. Identifica como obstáculos para a partilha eficaz de inteligência, problemas relacionados à privacidade, falta de padronização e preocupações comerciais. Apesar da proposta sólida, mas baseada numa revisão teórica, (não há estudos de caso e testes práticos), não explora em profundidade como regulamentações específicas podem afetar a implementação das soluções sugeridas e como poderiam ser implementados na prática. Isso é especialmente relevante em setores altamente regulamentados, como o setor bancário.

2.2.4. Indicadores e Métricas

A utilização de métricas e *Key Performance Indicator* (KPIs) é fundamental para avaliar a eficácia das práticas de cibersegurança nas instituições bancárias. Essas métricas permitem monitorizar a exposição a riscos, a eficácia das medidas de segurança implementadas e a capacidade de resposta a incidentes [98]. Entre as principais métricas destacam-se [99], tempo médio de deteção e resposta a incidentes; número de incidentes reportados e partilhados; frequência de atualizações de ameaças; nível de confiança nas informações partilhadas; integração entre sistemas internos e plataformas de partilha. A monitorização contínua dessas métricas fornece uma visão abrangente do cenário de

ameaças e da eficácia das estratégias de segurança adotadas, permitindo ajustes proativos conforme necessário.

O modelo Capability Maturity Model Integration (CMMI) é amplamente utilizado para avaliar e melhorar a maturidade dos processos organizacionais, incluindo a cibersegurança, definindo cinco níveis de maturidade: *Initial*; *Managed*; *Defined*; *Quantitatively Managed*; *Optimizing* (Apêndice E). Este modelo fornece uma estrutura para as instituições bancárias identificarem lacunas nas suas práticas de segurança e desenvolverem planos de melhoria contínua. [100].

Maturidade na Partilha de Informação em Cibersegurança segundo o NIST [94], indica que a partilha de informação sobre ciberameaças é um elemento essencial para fortalecer a resiliência coletiva das instituições financeiras. O guia NIST SP 800-150 propõe um conjunto de boas práticas que, embora não estruturadas formalmente em níveis, permitem construir uma escala de maturidade organizacional na partilha de informação. Com base nas recomendações do NIST, é possível definir cinco níveis de maturidade (Apêndice F): Inicial, Básico, Intermédio, Avançado e Otimizado.

No contexto da cibersegurança, os Indicadores de Comprometimento (IoCs) são elementos essenciais para a deteção e resposta a incidentes. Estes indicadores são evidências observáveis que sugerem uma potencial intrusão ou atividade maliciosa num sistema ou rede. A partilha de IoCs entre organizações, especialmente através de estruturas colaborativas como os ISACs, é fundamental para fortalecer a postura de segurança coletiva. Os IoCs podem ser classificados em várias categorias, incluindo, IoCs Atómicos (elementos indivisíveis, como endereços IP maliciosos, nomes de ficheiros suspeitos ou domínios associados a atividades nefastas); IoCs Calculados (resultados de cálculos, como *hashes* de ficheiros maliciosos – v.g.: SHA-256 - que identificam conteúdos específicos); IoCs Comportamentais (padrões de comportamento anómalos, como acessos fora do horário habitual ou movimentos laterais não autorizados dentro de uma rede) [101].

A partilha de IoCs em ISACs é muito importante, de acordo com [102], a partilha estruturada de IoCs em plataformas como os ISACs, permite a Deteção Proativa (identificar ameaças emergentes antes que causem danos significativos); Resposta Coordenada (facilitar uma resposta rápida e eficaz a incidentes, minimizando o impacto); Fortalecimento da Resiliência (melhorar a capacidade das organizações para resistir e recuperar de ataques de cibersegurança).

No setor bancário, a implementação de um ISAC [102] permite que as instituições bancárias partilhem informações críticas sobre ameaças, promovendo uma defesa coletiva mais robusta, visando assim Centralizar a Informação (reunir dados relevantes sobre ameaças de cibersegurança num único ponto de acesso); Promover a Colaboração (incentivar a cooperação entre instituições bancárias para enfrentar desafios comuns); Aumentar a Eficiência (reduzir a duplicação de esforços na identificação e mitigação de ameaças). Esta abordagem colaborativa é essencial num cenário de ameaças em constante evolução, onde a partilha de informação é uma ferramenta poderosa para a proteção do

ecossistema financeiro.

O EU *Cybersecurity Index* (EU-CSI) desenvolvido pela ENISA em colaboração com os EM, fornece uma avaliação abrangente da postura de cibersegurança na UE, incluindo dimensões como recursos, competências, políticas, tecnologias e sensibilização. Os dados do índice foram utilizados como base para o primeiro *Report on the State of Cybersecurity in the Union* de dezembro de 2024 [103]. Neste relatório a ENISA indica que em PT, em relação às dimensões dos recursos é classificado como tendo recursos limitados, especialmente em termos de financiamento e pessoal especializado em cibersegurança; nas competências apresenta nível médio, com programas de formação e certificação em crescimento. No entanto, há uma lacuna significativa na retenção de talentos e na formação contínua de profissionais em áreas críticas; nas políticas é referenciado que tem políticas bem estruturadas, alinhadas com o NIS2, e uma estratégia nacional de cibersegurança atualizada. O relatório destaca o compromisso político e institucional, mas recomenda maior integração entre setores público e privado; nas tecnologias, a adoção desta é moderada, com investimentos em infraestruturas críticas e soluções de cibersegurança. Contudo, o relatório sugere que PT deve acelerar a modernização tecnológica e a adoção de soluções baseadas em inteligência artificial e automação; na sensibilização demonstra níveis razoáveis, com campanhas públicas e iniciativas educacionais, ainda assim, o relatório recomenda maior envolvimento da sociedade civil e das PME na cultura de cibersegurança. Indica que 12 % das entidades desconhecem a diretiva NIS2 e 40 % das lideranças não receberam formação em cibersegurança.

De acordo com [104], PT apresenta uma maturidade média de 2,8 em 5 nas práticas de cibersegurança organizacional, o que está ligeiramente abaixo da média da UE (3,1); 64% das organizações portuguesas aumentaram o investimento em cibersegurança nos últimos 12 meses, com apenas 29% das entidades indicarem terem um orçamento dedicado exclusivamente à cibersegurança; 58% das organizações abrangidas pela NIS2 afirmam estar em processo de adaptação às novas exigências, sendo que 22% já cumprem integralmente os requisitos mínimos definidos pela diretiva; 41% das organizações têm equipas internas dedicadas à cibersegurança, enquanto 35% utilizam serviços externos de monitorização e resposta a incidentes; 47% das organizações realizam formações regulares em cibersegurança, sendo que apenas 18% têm programas estruturados de sensibilização para todos os colaboradores.

2.2.5. Conclusão

A presente revisão de literatura permitiu compreender de forma abrangente o estado atual da arte. Foi feita uma introdução à gestão de risco em cibersegurança, pois a partilha de informação é um subtema desta área. Esta envolve identificar, avaliar e mitigar ameaças que possam comprometer a

segurança da informação e dos sistemas digitais. É um processo transversal, contínuo e sistemático, essencial para proteger ativos e garantir a continuidade do negócio, especialmente no setor bancário. Inclui fases como levantamento, análise, tratamento e monitorização dos riscos, com base em normas como a ISO/IEC 27005. No setor bancário, classificado como operador de serviços essenciais pelo RJSC, a gestão de risco assume especial relevância, dado o elevado número de ataques e a criticidade dos ativos. Para ser eficaz, deve ser transversal à organização, envolver gestão de topo e integrar medidas técnicas, operacionais e de gestão. A colaboração entre instituições e o uso de tecnologias como IA são fundamentais para reforçar a resiliência. A gestão de incidentes complementa este processo, abrangendo prevenção, deteção, resposta e recuperação, suportadas por pilares como CISO, SOC e CSIRT, assegurando resiliência e continuidade da atividade.

A partilha de informação entre instituições é essencial para prevenir, detetar, responder e recuperar de ciberameaças, mas enfrenta barreiras que dificultam uma colaboração eficaz e sistemática. Essas barreiras são legais (RGPD, sigilo bancário), normativas (diversidade de *frameworks*), regulamentares (sobreposição normativa, reporte obrigatório, mas sem partilha entre bancos), técnicas (infraestruturas heterogéneas), concorrenciais (medo de exposição de vulnerabilidades), culturais e de confiança. Além de a cibersegurança no setor bancário exigir conformidade com normas internacionais, regulamentos europeus e legislação nacional, como as ISO/IEC 27001, NIST CSF RGPD, DORA e NIS/NIS2.

Frameworks como NIST, ISO/IEC 27001 e COBIT estruturam boas práticas de gestão de risco. Persistem, no entanto, tensões entre exigências de supervisão, proteção de dados e necessidade de cooperação, exigindo uma abordagem multilateral entre entidades para equilibrar segurança, confiança e competitividade.

A colaboração entre instituições bancárias é essencial para detetar ciberataques sofisticados. Esta colaboração é apoiada por normas e plataformas como STIX, TAXII e CIISI-PT, que facilitam a partilha estruturada de informação sobre ameaças. Iniciativas como o FICRO, CERT, CIRAS e CIISI-EU, promovem cooperação nacional e europeia, mas a participação ainda é limitada. Globalmente, o FS-ISAC reúne mais de 7.000 instituições de 70 países, utilizando IA para análise de ameaças. No entanto, apesar dos avanços, persistem desafios como a falta de padronização, interoperabilidade, confiança entre entidades e incentivos. Estudos propõem soluções descentralizadas, onde organizações podem trocar, vender e adquirir alertas de segurança em tempo quase real, com incentivos económicos e uso de tecnologias como STIX™, OWL e soluções com *Blockchain* e *smart contracts* para promover colaboração segura e superar barreiras de padronização e confiança. Apesar do carácter inovador, os estudos são teóricos, sem casos práticos e carecem de análise sobre a aplicação em setores regulamentados como o bancário.

Por último, a utilização de métricas e KPIs ajudam a avaliar a eficácia da cibersegurança, como tempo de resposta, confiança nas informações e integração de sistemas. Os IoCs são essenciais para a deteção e resposta a ciberataques, sendo classificados em atómicos, calculados e comportamentais. A partilha estruturada de IoCs em plataformas como ISACs fortalece a resiliência coletiva e permite respostas coordenadas. O EU-CSI revela que PT tem políticas estruturadas, mas enfrenta desafios em recursos, maturidade média (2,8/5), lacunas na retenção de talento, na formação contínua e modernização tecnológica. Modelos como o CMMI apoiam a melhoria contínua da maturidade organizacional em cibersegurança e o guia NIST SP 800-150 propõe um conjunto de boas práticas que, embora não estruturadas formalmente em níveis, permitem construir uma escala de maturidade organizacional na partilha de informação.

CAPÍTULO 3

Método de Investigação

De acordo com [105], o desenvolvimento de um método de investigação é uma das tarefas mais desafiadoras na construção do estudo. O presente estudo é de natureza qualitativa, exploratória e construtiva, orientado para a compreensão profunda dos fatores que influenciam a partilha de informação em cibersegurança entre instituições bancárias. A opção por uma abordagem qualitativa justifica-se pela escassez de literatura científica sobre o tema, especialmente no contexto nacional e europeu, e pela necessidade de explorar barreiras, iniciativas de colaboração e incentivos a partir da perspetiva dos intervenientes diretos. Além disso, a investigação foi realizada através do estudo de caso de como as entidades bancárias fazem a partilha de informação em cibersegurança.

3.1. Participantes

Inicialmente, fizeram-se 28 contactos, dos quais se obtiveram 24 convites aceites para a realização de uma entrevista. De seguida, realizaram-se as entrevistas até se alcançar a saturação teórica (quando novos dados não trazem mais informações relevantes). Com isto, a amostra do estudo foi constituída por 17 participantes com idades compreendidas entre os 36 e os 63 anos (M = 50.40; DP = 9), onde *M* representa a média e *DP* o desvio padrão. A maioria dos participantes situa-se entre os 45 e os 55 anos de idade, reside em território nacional e trabalham para um banco português. Quanto ao tempo de experiência em cibersegurança, os participantes têm entre dois e 30 anos de experiência (M =15.30; DP =10.5). O único requisito para integrar a amostra era ser um profissional experiente de cibersegurança, sendo que os participantes tinham funções como gestores de risco, analistas de cibersegurança, equipa de SOC, CISO, auditores bancários e consultores.

Por fim, visto que a maioria dos participantes seriam de fácil identificação, devido ao cargo que ocupam, as suas idades foram divididas em intervalos (< 40; 40 ≤ idade < 50; > 50) e o sexo omitido, de maneira a ser respeitado o anonimato e a confidencialidade. Porém, pode-se adiantar o cargo laboral dos participantes: três CISO, dois Cybersecurity Architect, dois Cybersecurity Analyst (um deles na equipa de SOC), dois Cybersecurity Auditor, um Cybersecurity Legal, um CIO, um Information Security Officer, um Cybersecurity Risk Manager, um Incident Responder, um de controlo interno, um Vice-Presidente com o pelouro da Cibersegurança e um Consultor em Cibersegurança (Tabela 3.1).

Tabela 3.1 - Dados Demográficos

Entrevistado	Função	Função Cibersegurança	País	Experiência Cibersegurança	Exp. Banca	Idade
E_01	Diretor	Gestor de Risco	PT	$[\cdots, 5]$	$[30, \cdots]$	$]50, \cdots]$
E_02	Diretor	Resposta Incidentes	PT	$[\cdots, 5]$	$[\cdots, 20[$	$[\cdots, 40[$
E_03	CIO	–	PT	$[20, \cdots]$	$[20, 30[$	$]50, \cdots]$
E_04	Diretor	CISO	PT	$[20, \cdots]$	$[\cdots, 20[$	$]50, \cdots]$
E_05	Diretor	Analista	PT	$]5, 20[$	$[20, 30[$	$]50, \cdots]$
E_06	Diretor	Arquiteto	PT	$[20, \cdots]$	$[20, 30[$	$]50, \cdots]$
E_07	Diretor	Controlo Interno	PT	$[\cdots, 5]$	$[30, \cdots]$	$]50, \cdots]$
E_08	Vice-Presidente	Vice-Presidente	UE	$]5, 20[$	$[\cdots, 20[$	$[\cdots, 40[$
E_09	Diretor	Arquiteto	PT	$[\cdots, 5]$	$[20, 30[$	$]50, \cdots]$
E_10	Diretor	Legal	PT	$]5, 20[$	$[20, 30[$	$]50, \cdots]$
E_11	Técnico	Analista	PT	$[20, \cdots]$	$[20, 30[$	$]50, \cdots]$
E_12	Resp. Seg. Informação	Resp. Seg. Informação	UE	$[20, \cdots]$	$[20, 30[$	$[40, 50]$
E_13	Diretor	Auditor	PT	$]5, 20[$	$[\cdots, 20[$	$[40, 50]$
E_14	Coord. Cibersegurança	CISO	PT	$]5, 20[$	$[\cdots, 20[$	$[40, 50]$
E_15	Diretor	CISO	PT	$]5, 20[$	$[20, 30[$	$]50, \cdots]$
E_16	Técnico	Auditor	PT	$]5, 20[$	$[\cdots, 20[$	$[\cdots, 40[$
E_17	Consultor	Consultor	PT	$[20, \cdots]$	$[20, 30[$	$]50, \cdots]$

De acordo com [106], argumentam que as teorias devem emergir dos dados recolhidos em vez de serem impostas previamente. Os autores defendem que em vez de escolher uma amostra fixa desde o início, os investigadores devem usar a amostragem teórica, onde novos dados são recolhidos conforme a teoria se desenvolve. Esse processo ocorre até se alcançar a saturação teórica. O processo de amostragem seguiu assim as orientações de [106], procurando que os participantes no estudo fossem profissionais com experiência relevante no tema em estudo.

3.2. Instrumentos

Guião da Entrevista

De acordo com [107] [108] [109] , as entrevistas são das melhores técnicas quando se pretende obter a opinião, perspetiva e experiências dos profissionais sobre um determinado tema. De acordo com [109] [110], a entrevista pode ser definida como "uma conversa entre duas ou mais pessoas ". Conforme identificado por [109], as entrevistas podem ser estruturadas, não estruturadas ou completamente abertas e semiestruturadas. As entrevistas estruturadas consistem num conjunto fixo de perguntas padronizadas, garantindo uniformidade nas respostas e facilitando a comparação entre os participantes, as não estruturadas caracterizam-se pela ausência de uma ordem rígida de questões, permitindo que o entrevistado conduza a conversa e revele *insights* espontâneos sobre o assunto em questão e as semiestruturadas combinam perguntas predefinidas com a flexibilidade de explorar tópicos emergentes durante a entrevista, permitindo uma compreensão mais profunda do tema.

Inicialmente, previa-se fazer entrevistas de *Focus Group*, que de acordo com [111] [112] é uma técnica usada para a recolha de dados, através da interação do grupo sobre um tópico apresentado

pelo investigador, podendo ser utilizada em diferentes momentos do processo de investigação. Porém, tal não foi realizado porque os participantes não foram recetíveis às entrevistas em *Focus Group*. Desta forma, as entrevistas foram individuais, umas em formato online e outras presenciais e segundo o método de semiestruturadas. Para tal, seguiu-se uma abordagem da teoria *Grounded Theory* [21], conforme proposta por [113], utilizando entrevistas semiestruturadas como principal método de recolha de dados e o método de analise de conteúdo [22] [23] para a análise de dados, permitindo o desenvolvimento de uma teoria substantiva emergente dos dados empíricos. Esta abordagem é particularmente adequada para contextos em que há pouco conhecimento teórico consolidado e onde se pretende gerar compreensão fundamentada sobre fenómenos complexos. Logo, a sua utilização permitiu uma compreensão aprofundada das perceções e experiências dos participantes sobre os desafios e as oportunidades da partilha de informação em cibersegurança.

O guião das entrevistas (Apêndice G) foi elaborado tendo por base a literatura analisada sobre o tema. Não foram, contudo, identificado guiões ou escalas neste domínio de conhecimento, que pudessem ser adotadas para o presente estudo. Também foram definidas regras e objetivo para a entrevista (Apêndice H). Com o objetivo de testar o guião de entrevista previamente elaborado, fez-se um pré-teste com um profissional com mais de 15 anos de experiência em cibersegurança. Esta etapa permitiu avaliar a clareza e pertinência das questões, bem como a adequação da sua sequência e do tempo necessário para a sua aplicação. Com base neste pré-teste, foram introduzidos alguns ajustes ao guião da entrevista, o que contribuiu para aumentar a validade e a fiabilidade do guião, assegurando a sua adequação à recolha de dados do estudo.

Questionário Sociodemográfico

O Questionário Sociodemográfico (QSD) foi construído para este estudo, teve como objetivo a caracterização dos participantes e é constituído pelas cinco perguntas iniciais das entrevistas. Para este estudo utilizaram-se as seguintes variáveis: idade, cargo na empresa, experiência na banca e experiência em cibersegurança e função em cibersegurança.

3.3. Procedimento

Numa primeira fase, definiu-se o âmbito do estudo (Definição do Problema) que consiste em analisar como é feita a partilha de informação em cibersegurança no setor bancário. Posteriormente foram enviados para a Comissão de Ética da ISTA (Escola de Tecnologia e Arquitetura do ISCTE) os seguintes documentos: guião das entrevistas; termo de responsabilidade e confidencialidade; formulário Comissão Ética; *Debriefing*; questionário de tratamento dados pessoais. Após a aprovação pela Comissão de Ética, deu-se seguimento aos contactos de profissionais de diferentes organizações, via *email* ou telefonicamente, a solicitar a participação neste estudo e com uma breve introdução sobre o

mesmo. Após este contacto, e para quem aceitou realizar a entrevista, a mesma foi convenientemente agendada. Posteriormente, foi enviado formalmente via *email* o consentimento informado para preenchimento e, no caso das entrevistas não presenciais, um *link* para a participação numa videochamada na data previamente combinada.

Numa segunda fase, e após a receção dos consentimentos informados devidamente assinados, procedeu-se à realização das entrevistas (Recolha de Dados). O número de participantes não foi previamente definido, em vez disso, utilizou-se o princípio de saturação teórica, inspirado na *Grounded Theory* [21], como critério para encerrar o processo de entrevistas. Assim, novas entrevistas foram realizadas até que os dados adicionais não trouxessem informações relevantes ou significativamente novas em relação às categorias emergentes. A saturação teórica é bastante importante porque determina se os dados recolhidos apresentam novas informações que sejam relevantes. As entrevistas aconteceram *online* ou presencialmente e foram gravadas via *Microsoft Teams*. Em média, as entrevistas tiveram uma duração de 80 minutos, totalizando 22.7h de registo de áudio.

Numa terceira fase, fez-se a transcrição integral das entrevistas e, posteriormente, a análise de dados que foi realizada segundo o método de análise de conteúdo [22] [23] e *Grounded Theory* [21]. A Figura 3.1 reflete a junção dos métodos aplicados.

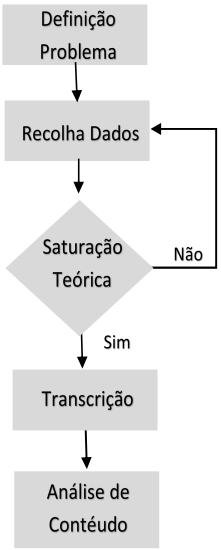


Figura3.1 - Processo Aplicado

Esse desenho metodológico procurou combinar a flexibilidade da saturação teórica, que assegurou uma recolha de dados orientada pela relevância empírica, com a sistematização da análise de conteúdo, que possibilitou uma interpretação rigorosa e organizada dos dados.

3.4. Análise de Conteúdo

Após a realização, transcrição e registo das entrevistas, os dados recolhidos foram analisados recorrendo-se ao método de análise de conteúdo [22] [23], que descreve e quantifica o conteúdo de mensagens de forma sistemática e objetiva. Este método é rigoroso e flexível para identificar, organizar e interpretar padrões recorrentes (temas) num *corpus* textual, permitindo compreender em profundidade significados partilhados pelos participantes. A metodologia segue três etapas fundamentais: (i) pré-análise – onde foram anotadas as ideias principais; (ii) exploração do material – os dados foram codificados, categorizados e agrupados por temas; (iii) tratamento/interpretação dos resultados – os resultados foram redigidos. A sua relevância advém da possibilidade de aplicação em diferentes enquadramentos epistemológicos e de uma perspetiva mais estruturada, tradicionalmente associada a perspetivas positivistas, assegurando simultaneamente rigor científico e flexibilidade analítica. De acordo com [22] [23], uma das principais vantagens deste método é a sua flexibilidade, no entanto, deve ser usado com alguma orientação, permitindo que o investigador seja objetivo a obter informação rica, detalhada e útil. Segundo os mesmos autores, é um método de natureza qualitativa que difere de outros métodos, essencialmente porque pode ser tanto qualitativo quanto quantitativo (contagem de frequência de palavras, categorias, etc.). Este método foi usado em conjunto com o *Grounded Theory* [21], porque permite uma análise de conteúdo através de um processo de codificação aberta [114] [115].

Esta investigação incidiu ainda, sobre uma abordagem abdutiva ou mista, isto é, dedutiva, na medida em que o guião da entrevista na sua estrutura já sinalizava alguns temas que se pretendiam explorar, mas também, indutiva pela abertura a novos elementos que emergiram dos dados recolhidos. Sendo este método um processo recursivo, o investigador pode mover-se entre as várias fases, tendo lido e relido as transcrições das entrevistas, refez codificações e categorizações, garantindo confiabilidade e replicabilidade[116] [117].

Na fase inicial de categorização adotou-se um procedimento inspirado na codificação aberta proposta pela *Grounded Theory* [21], assim, os dados foram lidos em detalhe e fragmentados em unidades de significado, que receberam códigos provisórios sem categorias pré-definidas. Esse processo possibilitou a emergência de códigos a partir do próprio material empírico. Posteriormente, em consonância com a lógica da análise de conteúdo [22] [23], esses códigos foram reunidos em categorias temáticas mais amplas, permitindo uma sistematização dos sentidos presentes nas entrevistas. Essa estratégia híbrida combinou a flexibilidade indutiva da codificação aberta com a rigorosidade categorial da análise de conteúdo, favorecendo uma interpretação que respeita tanto a espontaneidade dos dados quanto a necessidade de organização e clareza analítica.

A análise procura identificar similaridades, divergências e padrões entre as opiniões dos

profissionais e correlacionar esses dados com as informações obtidas na revisão da literatura. A análise das entrevistas irá dar uma visão complementar à revisão da literatura, oferecendo uma compreensão mais detalhada da partilha de informação em cibersegurança. Este processo foi feito com recurso ao *software* MAXQDA 2024. Esta ferramenta foi usada por ser das mais adotadas em estudos deste tipo, proporcionar avançado à análise de dados qualitativos e métodos mistos, e ser amplamente utilizada por investigadores em diversas áreas do conhecimento. Criado pela empresa alemã VERBI *Software*, o MAXQDA oferece uma plataforma robusta para organizar, codificar, analisar e visualizar dados não numéricos, como textos, entrevistas, áudios, vídeos e dados de redes sociais. O *software* suporta métodos como *Grounded Theory*, análise de conteúdo qualitativo, análise de discurso e estudos de caso [118]. As categorias existentes já se encontravam bem desenvolvidas em termos das suas propriedades e dimensões, demonstrando variação com relações bem estabelecidas entre as categorias [119].

CAPÍTULO 4

Resultados e Discussão

Com o objetivo de responder às questões de investigação formuladas, analisou-se o *corpus* textual das transcrições das entrevistas e obtiveram-se quatro grandes temas: (i) barreiras à partilha de informação; (ii) colaboração para partilha de informação; (iii) incentivos à partilha de informação; (iv) métricas (Figura 4.1).

Para assegurar concisão, este capítulo apresenta apenas um número limitado de exemplos ilustrativos (um a três), estando os restantes disponíveis no Apêndice I.

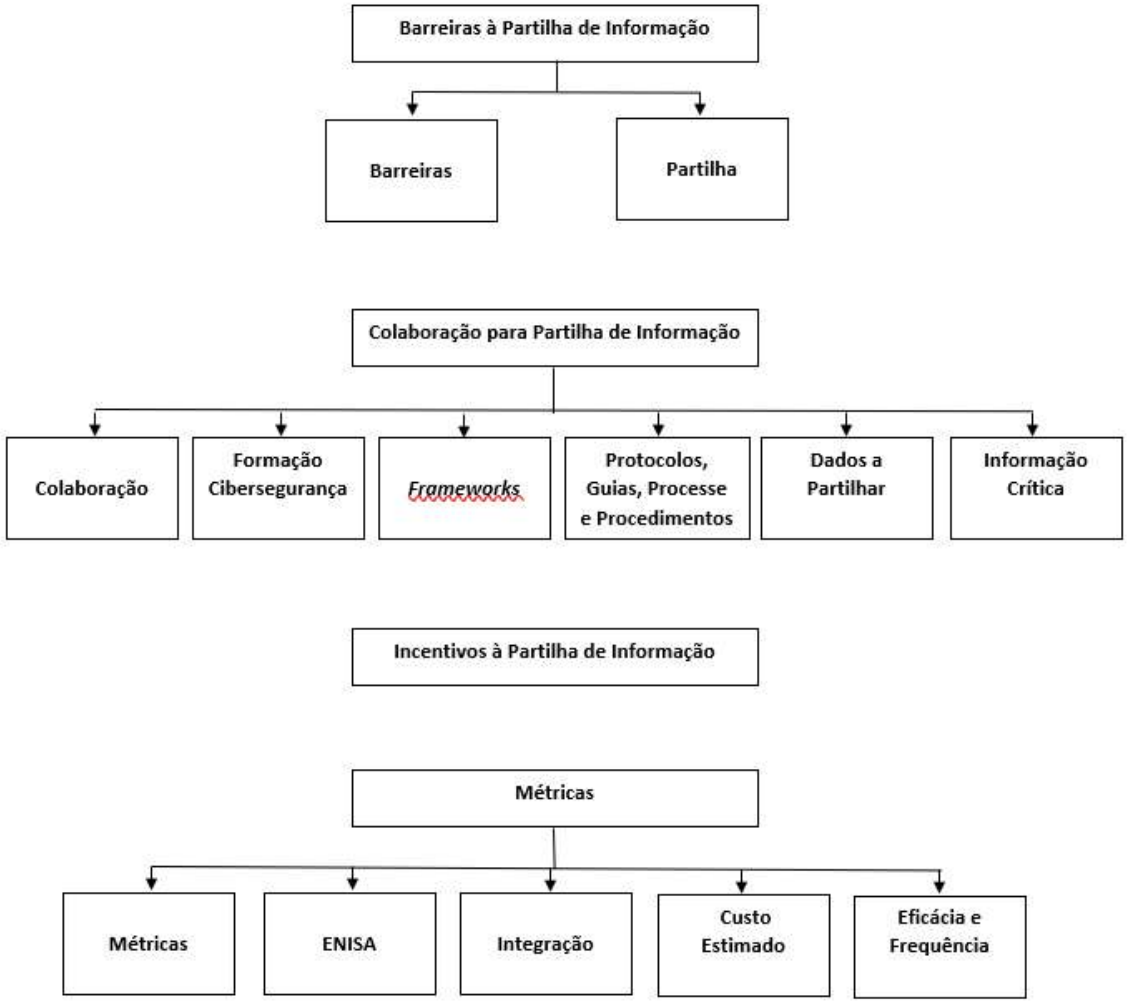


Figura 4.1 – Gráfico Temático

4.1. Resultados do Estudo

As tabelas deste capítulo, refletem a opinião/conceções dos 17 participantes no estudo e não a realidade total do setor, estes falaram na sua perspetiva e não em representação da sua instituição. Como foi adotada uma amostra por conveniência e não por um processo probabilístico, é possível observar um viés na forma como os dados estão representados. Este, o viés amostral, pode ter amplificado certos dados e minimizado outros, influenciando os resultados. Como temos dois participantes no estudo de bancos da UE e 15 de PT e para não ter dados tão enviesados, os cálculos das tabelas foram feitos por contagens e percentagens, as percentagens em UE e PT foram calculadas sobre o total de menções dentro de cada grupo (UE: X menções; PT: Y menções; Total: X + Y menções). Excetuam-se as tabelas 4.1, 4.3, 4.4 que refletem a opinião dos participantes por função e a tabela 4.10 que são informações sobre métricas.

4.1.1. Barreiras e Partilha de Informação

Dentro deste grande tema foram identificados dois subtemas: i) Barreiras; ii) Partilha.

Relativamente ao primeiro subtema, foi possível aferir pelos discursos dos participantes as principais barreiras relativamente à partilha de informação em cibersegurança no setor bancário, estas foram discriminadas pelas funções (Tabela 4.1), ou seja, reflete a opinião do participante enquadrada dento da função.

Tabela 4.1 - Barreiras Partilha de Informação por Funções de Cibersegurança

Barreiras	CISO	Consultor	Analista	Arquiteto	Auditor	Legal	Gestão Risco	Resposta Incidentes	Resp. Seg. Informação	Vice Presidente	Total
Falta Abertura do Regulador - Supervisão	0%	0%	0%	0%	0%	25%	0%	0%	0%	0%	2,40%
Reputacionais	0%	0%	12,5%	0%	0%	0%	0%	0%	0%	0%	2,40%
Confiança	22,2%	0%	0%	0%	16,7%	0%	0%	0%	0%	0%	7,10%
Técnicas	0%	0%	12,5%	0%	0%	0%	0%	0%	0%	0%	2,40%
Concorrências	22,2%	0%	25%	25%	16,7%	0%	50%	33,3%	0%	0%	19,00%
Legais, Normativas Regulamentares	22,2%	0%	12,5%	25%	16,7%	75%	0%	33,3%	100%	100%	28,60%
Culturais	33,3%	100%	37,5%	50%	50%	0%	50%	33,3%	0%	0%	38,10%

Além das barreiras identificadas na revisão de literatura os participantes identificaram barreiras reputacionais (medo de que a divulgação de ciberataques afete a imagem pública e a confiança dos clientes, pois um banco que revela um ataque pode ser visto como vulnerável, mesmo que a partilha beneficie o setor) e barreiras de confiança (falta de confiança entre instituições bancárias quanto ao uso responsável da informação partilhada e que não exista reciprocidade na partilha).

O tipo de barreia com maior tendência foi a barreira cultural com 38.10% (12 participantes), seguindo-se a barreira do tipo legal/normativa/regulamentar (28.6%) e de concorrência (19%). Estas barreira também apresentam a maior distribuição pelas várias funções e são vistas como transversais, afetando múltiplas funções na organização. A função de *Cybersecurity* Legal, *Information Security Officer* e Vice-Presidente com o pelouro da Cibersegurança atribuem valores elevados a barreiras

legais, regulamentares, normativas, sendo que dois destes participantes pertencem a bancos da UE. Todavia, nas instituições portuguesas é quase unânime que as barreias culturais são as mais críticas, seguidas das barreiras legais/regulamentares/normativas e concorrências. As barreiras reputacionais e as técnicas apenas são identificadas por *Cybersecurity Analyst*. Para estes participantes, as barreiras culturais são muito difíceis de ultrapassar (ver também Apêndice I – excerto 1):

"Alterar a mente dos portugueses" (E_13)

"(…) há muito a cultura do protecionismo" (E_08)

"(…) visão de security by obscurity" (E_03)

Nas barreiras legais, normativas, regulamentares o que é mais focado é o sigilo bancário, o RGPD, demasiadas leis, regulamentos, diretivas e *frameworks*, muito complexas de interpretação, além de alguns contraditórios entre si. As barreiras técnicas são mínimas pois a integração entre sistemas pode ser feita através de *Application Programming Interface* (API´s) e existem taxonomias definidas para reporte de incidentes ao nível de entidades como o CERT e a CSIRT/CNCS.

"A taxonomia do CSIRT foi pensada para fazer a ponte com a legislação, porque, na lei da Cibersegurança e no decreto-lei que a regula, vem mencionada uma taxonomia (…)" (E_17)

"A taxonomia que está definida, é um que na prática é um mapeamento da taxonomia da ENISA para o nível nacional. É uma taxonomia que é definida pelo CNCS" (E_14).

Por outro lado, também se analisou as barreiras identificadas pelos participantes em função de PT e da UE (Tabela 4.2). Verificou-se que os participantes portugueses mencionam todas os tipos de barreiras, enquanto os participantes da UE só mencionam as legais, normativas, regulamentares. Os participantes da UE tendem para as barreiras legais, normativas, regulamentares, enquanto os participantes PT para as barreiras culturais e só depois para as legais, normativas, regulamentares.

Tabela 4.2 – Barreiras: Partilha de Informação por participantes de PT/UE

Barreiras	PT	PT %	EU	EU %	Total	Total %
Falta Abertura do						
Regulador - Supervisão	1	2,3%	0	0%	1	2,20%
Reputacionais	1	2,3%	0	0%	1	2,20%
Confiança	3	9,3%	0	0%	3	8,70%
Técnicas	1	2,3%	0	0%	1	2,20%
Concorrências	7	20,90%	0	0%	7	19,60%
Legais, Normativas						
Regulamentares	7	20,90%	2	100%	9	26,10%
Culturais	12	41,90%	0	0%	12	39,10%

No subtema “Partilha”, pela análise da existência ou não de partilha de informação segundo a função dos participantes, verifica-se pela análise do discurso dos participantes que a tendência para a partilha de informação em cibersegurança no setor bancário é reduzida, com cerca de 67.6% dos participantes a identificar que não existe partilha (Tabela 4.3). Os participantes que identificam que existe partilha, tem a ver com a partilha de informação informal entre os pares ou entre fornecedores.

Tabela 4.3 – Existência de Partilha de Informação por Função

Função	Existe	Não existe
CISO	57,10%	42,90%
Consultor Cibersegurança	25,00%	75,00%
Cybersecurity Architect	0,00%	100,00%
Cybersecurity Auditor	0,00%	100,00%
Cybersecurity Legal	0,00%	100,00%
Cybersecurity Risk Manager	25,00%	75,00%
Cybersecurity Analyst	25,00%	75,00%
Incident Responder	0,00%	100,00%
Vice-Presidente de Cibersegurança	40,00%	60,00%
Information Security Officer	50,00%	50,00%
CIO	40,00%	60,00%
Total	32,40%	67,60%

Algumas opiniões dos participantes (ver também Apêndice I – excerto 2):

“Partilha de informação bilaterais ou informais” (E_17)

“os problemas de defesa e ataques partilhamos com o fornecedor de SOC externo, que partilha entre os seus clientes, mas de forma confidencial, sem identificar ninguém, o que faz com que exista partilha entre entidades bancárias” (E_05)

Já pela análise do discurso dos participantes da UE, foi analisado que existe uma boa partilha. Opinião de participantes:

“(…) faz-se bem estas partilhas de uma forma muito simples, são muito abertos e existem muitos esforços de partilha de informação e a nível geográfico, também há entidades mais agregadoras a nível nacional. É uma partilha bastante aberta sobre grande parte da informação. E no nosso caso ainda somos membros do FS-ISAC que é uma plataforma que nós achamos que funciona bastante bem” (E_08)

“Partilhamos com a FS-ISAC” (E_12).

Pela análise dos discursos dos participantes sugere existir uma tendência do setor bancário português para partilhar apenas os incidentes aos reguladores porque é obrigatório. Opinião de

participantes:

"Normalmente a partilha é de resposta a incidentes. Faz-se essencialmente com a PJ e no BPNET posteriormente CNCS" (E_04)

"Só com as autoridades de controlo, só incidentes a partilha é feita na fase de deteção. Pois é obrigatório reportar os incidentes ao abrigo do DORA" (E_11).

Os participantes que indicam que não existe partilha tem muito a ver com as barreiras culturais (ver também Apêndice I – excerto 3):

"no setor bancário existe ainda muita dificuldade em participar e ser transparente, mesmo quando até se sabe publicamente que sofreram ataques de cibersegurança" (E_06)

"(…) cada banco trabalha separadamente (…)" (E_10).

A falta de partilha de informação no setor bancário português tem muitas implicações negativas ao nível da fraude, pois facilita a propagação da mesma. Aqui, os participantes focam que o BP não autoriza que exista partilha sobre a fraude alegando o RGPD, algo com o qual não estão de acordo, pois noutros países da UE, também sujeitos ao RGPD, a partilha é feita. Por exemplo, em Itália foi criada uma plataforma para esse efeito que está disponível para outos países da UE. Em PT, quando se deteta uma fraude, o primeiro passo a fazer é bloquear a conta, ou seja, são bloqueadas as entradas e saídas de dinheiro. Porém, estas contas muitas vezes têm esquemas de crime organizado, como *malware* bancário ou transações ilícitas, então só se deveria bloquear as saídas de dinheiro, de maneira que os criminosos não se apercebessem do bloqueio. A forma como funcionam alerta os criminosos e estes trocam de banco. Opinião de alguns participantes, onde um refere que a fraude cresceu muito após o COVID (ver também Apêndice I – excerto 4):

"Os italianos superaram o problema da fraude através de uma plataforma que criaram. A pessoa inscreve na plataforma a informação que tem e que justifica a fraude e eles colaboram no sentido de parar os fluxos financeiros e até de fazer o estorno oficiosamente e depois comunicam às autoridades também. Aliás, tanto quanto eu saiba, a própria polícia de finança está também representada" (E_17)

"(…) sobretudo a partir do Covid, onde foi o grande boom (…) cada vez mais é um tema que está em cima da mesa, mas não parece que ainda se dê a devida importância, mas é um tema transversal" (E_10)

Apesar da dimensão da amostra em estudo, a análise dos discursos dos participantes sugere em

relação às barreiras à partilha de informação em cibersegurança que as barreiras culturais e as legais, regulamentares, normativas são as mais relevantes e transversais, afetando várias funções dentro das organizações. Destes discursos observa-se uma diferença entre a realidade portuguesa, onde predomina a barreira cultural, e a realidade europeia, onde as barreiras legais, regulamentares, normativas são mais expressivas. A analise dos discursos dos participantes segure que a partilha de informação no setor bancário português é limitada, ocorrendo sobretudo de forma informal ou apenas em resposta a requisitos regulatórios, em alguns bancos da UE as práticas são mais estruturadas.

4.1.2. Colaboração para partilha de Informação

Dentro deste grande tema foram identificados cinco subtemas: i) Colaboração; ii) Formação em Cibersegurança; iii) *Frameworks*, Normas, Protocolos, Guias, Modelos, Processos e Procedimentos; vi) Dados à Partilha; v) Informação Crítica.

No primeiro subtema – Colaboração, de acordo com os participantes, seria necessário, para incrementar a colaboração à partilha de informação: (i) fomentar a relação entre bancos de forma informal; (ii) ter no conselho de administração de cada banco um membro ou assessor com poderes de decisão e conhecimento em cibersegurança.

Como medidas a implementar seria: (i) convívios informais, para as pessoas se conhecerem e começar a ganhar confiança entre elas, e o BP, como entidade reguladora e sem interesse comercial, poderia auxiliar nestes convívios para ajudar a alterar a mentalidade das pessoas, por forma a terem uma cultura pró-ativa e de partilha; (ii) o BP organizar *WorkShops*, para explicar a importância da partilha, os seus benefícios e os prejuízos que podem existir pela não partilha. Com isso começarem a partilhar, nem que fosse em plataformas onde a informação partilhada e recebida é anonimizada como a FS-ISAC.

Opiniões de participantes (ver também Apêndice I – excerto 5):

"Fomentar a relação entre bancos menos formal para aumentar o relacionamento e aumentar a partilha" (E_4)

"O regulador ajudar na mudança cultural. Confiança entre as pessoas. Já todos perceberam que a partilha é benéfica, mas é difícil a partilha" (E_3)

A fraude é grave em PT e, como tal, deveria ser feita uma mudança urgente, de forma a passar a existir uma partilha grande e, assim, não deixar que os criminosos continuassem a atuar sem controlo. Neste sentido, deveria existir uma cooperação grande com o BP em relação ao RGPD, para existir partilha de dados que não sejam sensíveis, como número de contribuinte, titular das contas, e até

mesmo se for necessária uma intervenção junto do poder político, ou criar um conceito igual ao italiano. Opinião de participantes:

"o setor financeiro em vez de não fazer nada, poderiam juntar-se todos e fazerem esse périplo entre o próprio regulador e o poder político, apresentando soluções para resolver a fraude" (E_17)

"A plataforma criada pelos italianos é muito mais acessível e fácil e está aberta a outros países europeus" (E_17)

A IA pode ter um papel muito relevante para a colaboração na partilha de informação em cibersegurança e CTI, pois pode detetar ameaças em tempo real (consegue analisar grandes volumes de dados e identificar padrões suspeitos), classificar os ciberataques (v.g.: malicioso, suspeito e benigno), os milhares de indicadores de ameaça que se recebe diariamente e priorizar o que deve ser partilhado primeiro, evitando, assim, sobrecarga de informação, focando-se naquilo que é realmente crítico, tomar decisões imediatas para conter ciberataques e reduzir falsos positivos. Os bancos da América Latina estão muito avançados em IA para deteção de fraude [120].

O subtema – Formação em Cibersegurança, apesar da dimensão da amostra em estudo, pela análise do discurso dos participantes foi identificado uma falta de recursos com formação e experiência na área de cibersegurança, podendo prejudicar a colaboração na partilha de informação, devido as instituições bancárias terem receio de que a informação partilhada possa ser intercetada, manipulada, aumento do risco do erro humano, mas por outro lado não existem incentivos para a formação de pessoas. Da análise feita aos participantes, alguns não têm qualquer tipo de formação e os que têm, o tipo de formação varia muito entre eles (Tabela 4.4). Embora a maioria tenha formação em cibersegurança. Os dados foram organizados por função.

Tabela 4.4 – Certificação em Cibersegurança por Função

Função	**SIM**	**NÃO**
CISO	3	0
Consultor Cibersegurança	1	0
Cybersecurity Architect	1	1
Cybersecurity Auditor	2	0
Cybersecurity Legal	1	0
Cybersecurity Risk Manager	1	0
Cybersecurity Analyst	1	1
Incident Responder	0	1
Vice-Presidente de Cibersegurança	1	0
Information Security Officer	1	0
IT Risk	0	1
CIO	0	1
Total (percentagem)	**70,59%**	**29,41%**

Excertos dos participantes:

"Certificado de CISM da ISAC, CISA da ISAC, CCISO da EC-Council, Certified Penetration Testing Engineer da Mile2, certificado de CERT ORA, Certified Compliance Specialist da ICA e ICTTF, certificado da ISO/IEC 27001 Lead Implementer pela BSI" (E_12)

"CISA e CISSP" (E_11).

No terceiro subtema - Os participantes foram inquiridos sobre que *frameworks*, normas, guias e boas práticas, protocolos, modelos, procedimentos, plataformas, ferramentas e ciclos de CTI que usavam (Apêndice J). Muitos dos participantes portugueses desconheciam ou não usavam o que estava a ser questionado. Os dados deste tema estão apresentados nas tabelas 4.5, 4.6, 4.7 e 4.8.

Os participantes da UE relataram usar ferramentas que não são usadas por nenhum dos participantes de PT (*OpenCTI*, *AlienVault OTX* e CTM360) e ferramentas que não tinham sido identificadas no estudo (Tabela 4.5).

Tabela 4.5 – Plataformas/Ferramentas

Plataformas Ferramentas	**EU (n=8)**	**PT (n=20)**	**Total (n=28)**	**% Global**
MISP	1	6	7	25,00%
TheHive	0	0	0	0,00%
OpenCTI	2	0	2	7,14%
ThreatConnect	0	0	0	0,00%
IBM X-Force	0	3	3	10,71%
CTM360	1	0	1	3,57%
AlienVault OTX	2	0	2	7,14%
Anomali	0	1	1	3,57%
CIISI-PT	0	9	9	32,14%
FS-ISAC	2	1	3	10,71%

Opinião de um dos participantes:

"Em termos de ferramentas utilizam-se SIEM, EDR, cloud security, Web Applications by walls, sistemas de segurança de APIs, sistemas de orquestração, os chorus, endpoint management, entre outros" (E_08).

Pelo discurso dos participantes de PT, identificou-se que as plataformas/ferramentas mais usadas são a CIISI-PT (32.14%) e MISP (25%). De acordo com alguns participantes, apesar de usarem a CIISI-PT, praticamente não fazem partilha de informação:

"(…) Só partilhamos uma vez da CIISI-PT" (E_04)

"Temos acesso à CIISI-PT, mas não partilhamos" (E_15)

Os participantes da UE identificam que as plataformas usadas estão todas integradas umas com as outras.

"*Tudo automatizado e integrado, usamos SIEM e FS-ISAC, entre outros sistemas" (E_12)*

"Temos integração completa" (E_08)

De acordo com os participantes de PT, a integração só é feita por entidades bancárias que usam *Security Information and Event Management* (SIEM), mas essa integração é feita com as aplicações de SOC (algumas internas outras externas), sendo que a maior parte integra e não trata a informação. Nenhum entrevistado de PT falou de outro tipo de plataformas ou ferramentas. De acordo o discurso dos participantes as *frameworks* usadas na UE e PT são praticamente iguais, a divergência está no COBIT que só é usado por PT e na SWIFT que é usada pela UE (Tabela 4.6).

Tabela 4.6 – Frameworks

Frameworks	EU (n=8)	PT (n=14)	Total (n=22)	% Global
NIST Cybersecurity Framework	2	3	5	22,73%
MITRE ATT&CK	2	3	5	22,73%
CIS Controls (v8)	2	3	5	22,73%
COBIT 2019	0	5	5	22,73%
SWIFT	2	0	2	9,09%

Nas normas é convergente o uso da ISO/IEC 27001/27002, no entanto, na UE os participantes indicaram que são certificados nesta norma e as entidades bancárias também, enquanto em PT poucos participantes são certificados nesta norma e as entidades bancárias onde trabalham não são certificadas (Tabela 4.7).

Tabela 4.7 – Normas

Normas	UE (n=2)	PT (n=31)	Total (n=33)	% Global
ISO/IEC 27001/27002	2	10	12	36,36%
ISO/IEC 27010	0	0	0	0,00%
ISO/IEC 27035	0	5	5	15,15%
NIST SP 800-150	0	5	5	15,15%
NIST SP 800-53	0	5	5	15,15%
NIST SP 800-35	0	6	6	18,18%

Informação de alguns participantes:

"ISO/IEC 27001, até somos certificados" (E_08)

"O banco não é certificado" (E_04)

Tabela 4.8 – Protocolos, Guias, Modelos, Processos e Procedimentos

Protocolos, Guias, Modelos Processos e Procedimentos	EU (n=15)	PT (n=44)	Total (n=59)	% Global
ITIL 4	0	2	2	3,39%
ENISA Threat Intelligence Sharing Guide	2	4	6	10,17%
TLP (Traffic Light Protocol)	2	9	11	18,64%
STIX (Structured Threat Information eXpression)	1	2	3	5,08%
TAXII (Trusted Automated eXchange of Indicator Information)	0	1	1	1,69%
VERIS (Vocabulary for Event Recording and Incident Sharing)	0	0	0	0,05%
Ciclo de CTI	2	1	3	5,08%
NDAs (Non-Disclosure Agreements)	2	0	2	3,39%
Escalonamento	2	8	10	16,95%
Anonimização	2	9	11	18,64%
Planos de resposta	2	8	10	16,95%

Nos protocolos, guias, modelos, processos e procedimentos pelo discurso dos participantes pode-se inferir que existe convergência na maior parte dos aspetos. A divergência existe na ITIL 4 e TAXII, que só são usadas pelos participantes de PT, e no *Non-Disclosure Agreements* (NDAs) que é só usado pelos participantes da UE. Os ciclos de CTI (Apêndice J) são usados pelos participantes da EU, em PT só é usado por um dos participantes (Tabela 4.8).

No subtema – Dados a Partilhar, caso existisse uma partilha real, a tendência seria partilhar padrões de ataque, tipo de ataque, vetor de ataque, IoCs, alvos, agentes de ameaça, tipo de classificação e detalhe, indicadores de ataque e de exposição, informação sobre fraude. Opinião de alguns participantes (ver também Apêndice I – excerto 6):

"obrigatoriamente IoCs, mas para isso é necessário que as pessoas responsáveis queiram partilhar esses indicadores e situações que aconteçam na entidade bancária" (E_05)

"troca de informação sobre fraude, dados técnicos, IoCs" (E_17)

Por fim, no subtema – Informação Critica, foi possível identificar uma tendência para não partilha de informação critica, tais como vulnerabilidades, software utilizado para proteção, tudo que envolva clientes, o impacto do incidente e o impacto financeiro. Opinião de alguns participantes:

"As vulnerabilidades, porque são críticas, (…) o tipo de software que é o usado para a proteção do banco (…)" (E_04)

"Tudo que envolva clientes" (E_03)

"(…) quantos registos foram afetados, qual foi o impacto financeiro, que sistemas é que foram afetados, esta informação muito sensível" (E_08)

A análise do discurso dos participantes sugere que existem vários fatores considerados relevantes para fomentar uma maior colaboração entre instituições bancárias na partilha de informação de cibersegurança. Destaca-se a importância da construção de relações de confiança entre os bancos, apoiada pelo papel do BP enquanto entidade reguladora, promovendo uma mudança cultural que incentive a partilha pró-ativa. A nível organizacional, refere-se à necessidade de envolver os conselhos de administração com representantes especializados em cibersegurança, capazes de impulsionar políticas de partilha de informação. As plataformas e ferramentas revelaram diferenças entre os participantes da UE e de PT, a verificar-se maior integração e utilização diversificada nos participantes da UE, enquanto nos de PT sobressaem a CIISI-PT e o MISP, ainda que com uso limitado no que respeita à partilha.

Nas *frameworks*, há convergência no uso do NIST *Cybersecurity Framework*, MITRE ATT&CK e CIS *Controls*, mas com algumas especificidades regionais. Quanto às normas, é comum a adoção da ISO/IEC 27001/27002, o discurso dos participantes sugere que as entidades bancárias da UE também são certificadas. Já nos protocolos, guias, modelos e processos, observa-se grande alinhamento, com algumas diferenças pontuais.

A falta de formação em cibersegurança prejudica a colaboração na partilha de informação entre instituições bancárias.

Os participantes consideram que, caso a partilha fosse mais efetiva, deveria incidir sobretudo em indicadores técnicos de ataque (IoCs, TTPs, IoAs, vetores e padrões de ataque, bem como informações sobre fraude), enquanto dados mais sensíveis (v.g.: vulnerabilidades, software de proteção, impacto financeiro e dados de clientes) não deveriam ser partilhados. Por fim, foi ainda referido que a IA poderá assumir um papel central ao classificar, priorizar e filtrar informação, evitando sobrecarga e permitindo uma colaboração mais eficaz.

4.1.3. Incentivos à partilha de informação

Segundo o discurso dos participantes de uma forma geral, o incentivo para a partilha de informação no setor bancário não é eficiente (72.70% dos participantes diz que os incentivos não funcionam). Considerando que os incentivos regulatórios, económicos e tecnológicos não funcionam como incentivadores eficazes para a partilha de informação em cibersegurança (Tabela 4.9).

Tabela 4.9 – Incentivos à Partilha Informação

Incentivos	EU (n)	EU %	PT (n)	PT %	Total (n)	Total %
Funciona	1	33,30%	4	26,30%	5	27,30%
Não Funciona	2	66,70%	11	73,70%	13	72,70%

A não concordância com a existência de incentivos deve-se ao facto de que os mesmos poderiam ser incorretos. No sentido de, por exemplo, as pessoas partilharem informação errada para receberem o incentivo económico. Os participantes consideraram que o importante é alterar a cultura das pessoas, de forma que entendam que partilhar a informação de ciberataques e IoCs, por exemplo, não prejudica ao nível da concorrência, que a partilha é feita de forma segura e que em algumas plataformas está anonimizada. Deste modo, sugerem a criação de fóruns informais para as pessoas se conhecerem e passarem a ter confiança entre si, começando, assim, a fazer a partilha da informação de forma voluntária. Algumas opiniões de participantes (ver também Apêndice I – excerto 7):

"um banco que não partilhou nada e com os incentivos começa a partilhar é questionável, porque não o fazia antes" (E_04)

"não seria positivo porque estávamos a promover a partilha de informação sem ser muito fidedigna do partilhar só por partilhar. Não é uma boa estratégia" (E_08)

"o problema está na confiança e o poder existir fuga de informação. Acho que seria interessante é penalizações e multas grandes pela fuga de informação" (E_16)

Por outro lado, os participantes que defendem a utilidade dos incentivos (27.3%), afirmam que são essencialmente incentivos do tipo *Top/Down*, de penalizações para quem não partilha regularmente e de forma fidedigna, mas essencialmente incentivos positivos pelo elogio e pela demonstração dos benefícios da partilha em conferências e seminários. Opinião dos participantes (ver também Apêndice I – excerto 8):

"incentivo com base na regulação, o regulamento DORA mais a NIS 2, eles vão ser cumulativos" (E_17)

"eu partilho contigo porque a seguir vais partilhar comigo, ganhamos os dois. Isso já é por si um incentivo" (E_03)

Estes resultados sugerem que o tema gera perceções divergentes e que a confiança e a cultura organizacional são fatores centrais neste processo.

4.1.4. Métricas

Dentro deste grande tema foram identificados cinco subtemas: i) Méticas; ii) ENISA; iii) Integração; vi) Custo Estimado; v) Eficácia e Frequência.

Tabela 4.10 – Conceito de Métricas

Sigla	Nome completo	Objetivo principal	Tipo de informação	Exemplo prático (setor bancário)
KRI	Key Risk Indicator (Indicador-Chave de Risco)	Medir e monitorizar a exposição a riscos e sinalizar situações de alerta precoce.	Métrica de risco (tendencial /proativa).	% de sistemas críticos com vulnerabilidades não corrigidas
KPI	Key Performance Indicator (Indicador-Chave de Desempenho)	Avaliar o desempenho de processos ou controles de cibersegurança.	Métrica de desempenho (reativa/operacional).	Tempo médio de resposta a incidentes.
IoC	Indicator of Compromise (Indicador de Comprometimento)	Identificar sinais concretos de intrusão ou ataque em curso/concluído.	Evidência técnica de ataque.	Hash de ficheiro malicioso, IP de C2 (command & control).
IoA	Indicator of Attack (Indicador de Ataque)	Detetar táticas, técnicas e procedimentos (TTPs) que indicam que um ataque está a ser preparado ou executado.	Padrões de comportamento do atacante.	Sequência anómala de comandos PowerShell em vários endpoints.
IoOs	Indicators of Observation (Indicadores de Observação)	Registar dados observacionais que isoladamente não confirmam ataque, mas podem ser relevantes se correlacionados.	Informação contextual, ambígua.	Aumento súbito de tráfego numa porta não usual.
CTI	Cyber Threat Intelligence (Inteligência de Ameaças de Cibersegurança)	Recolher, analisar e partilhar informação sobre ameaças e atores maliciosos, para suportar decisões.	Conhecimento acionável sobre ameaças.	Relatório com TTPs de um grupo APT direcionado ao setor financeiro.

Estas métricas relacionam-se entre si num ciclo de integração. Primeiro, as métricas técnicas servem de input para CTI que as processa e consegue dar informação de métricas para gestão de risco e desempenho (KRI e KPI). A informação também circula no sentido contrário. Ou seja, no sentido ascendente (setas tracejadas) há a alimentação de informação e no sentido descente (setas pretas) o feedback de prioridades (Figura 4.2).

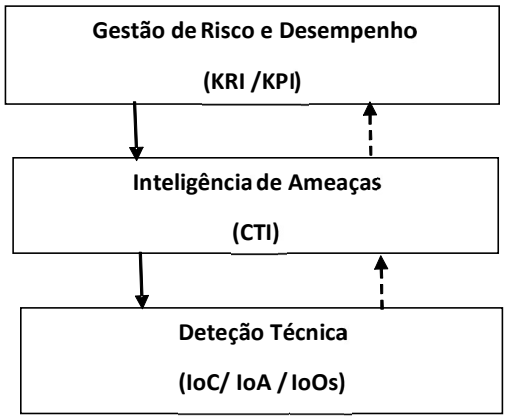


Figura 4.2 – Ciclo Integração IoAs/IoCs/IoOs, CTI, KPI/KRI

A analise do discurso dos participantes sugere que em PT, as métricas mais usadas são IoCs (37.00%), e nos bancos da UE as menos usadas são as KRI (9.10%), (Tabela 4.11).

Tabela 4.11 – Distribuição de Métricas por Região

Métrica	UE (n=2)	UE %	PT (n=15)	PT %	Total	Total %
IoAs	2	18,20%	0	0,00%	2	5,30%
IoOs	2	18,20%	0	0,00%	2	5,30%
IoCs	2	18,20%	10	37,00%	12	31,60%
CTI	2	18,20%	5	18,50%	7	18,40%
KRI	1	9,10%	6	22,20%	7	18,40%
KPI	2	18,20%	6	22,20%	8	21,10%

Na amostra, a tendência de utilização de métricas são os IoCs (31.60%), seguido dos KPI (21.10%). Apesar da dimensão da amostra em estudo, a analise do discurso dos participantes sugere que entre os participantes de PT e a UE existe uma convergência no uso de métricas de IoCs, KPI, KRI e CTI e uma divergência nas de IoAs e IoOs, apenas usadas pelos participantes dos bancos da EU. Também sugere que no setor bancário em PT se usam métricas para medir recursos, competências, políticas, percentagem de pessoas certificadas, auditorias e escalas ao nível dos riscos. Já no setor bancário na UE, além destas métricas, também são usadas métricas para medição da capacidade dos recursos do SOC e as suas competências. Nas tecnologias são feitas avaliações a cada porta de rede, a partir de *feeds* de CTI e de testes internos, serve para ver se o parque tecnológico continua a sustentar determinada função e se ainda está alinhado com os requisitos. Com isto conseguem medir os custos que teriam se não recebessem os *feeds* de CTI (seriam afetados *x* sistemas que têm *y* custo).

Na maturidade, foi analisado a maturidade da partilha de informação (Tabela 4.12) e a maturidade dos processos organizacionais em cibersegurança (Tabela 4.13). Na maioria, os níveis de maturidade da partilha de informação relatados pelos participantes de PT incidem no nível 1 e 2 (76.47%), não havendo maturidade de nível 4 e 5, e com alguns a não partilhar. Já pela UE, apenas foi relatado o nível de maturidade 4. No global, o nível 1 foi o com mais destaque (58.82%).

Tabela 4.12 – Maturidade da Partilha de Informação

Categoria	EU (n=2)	PT (n=15)	Total (n=17)	Total %
Não Partilham	0	1	1	5,88%
Partilham nível 1	0	10	10	58,82%
Partilham nível 2	0	3	3	17,65%
Partilham nível 3	0	1	1	5,88%
Partilham nível 4	2	0	2	11,76%
Partilham nível 5	0	0	0	0,00%

Opinião de participantes:

"(…) temos muita aderência a tudo o que é partilha de informação, nível partilha 4" (E_12)

"maturidade de partilha nível 1" (E_11)

"partilha de informação não existe" (E_10)

Apesar da dimensão da amostra em estudo, a análise dos discursos dos participantes sugere existir uma diferença na maturidade de partilha de informação entre instituições bancárias de PT e das duas instituições de outros países da UE em análise. Enquanto os participantes pertencentes a bancos portugueses reportaram uma maturidade média próxima do nível 1 (1,27), refletindo práticas iniciais e pouco estruturadas, os dois participantes de outros bancos da UE atingem uma média de nível 4 (4)

(conforme fórmula 4.1), sugerindo existir práticas mais consolidadas e colaborativas, numa escala de 1 a 5 (Apêndice F).

$$\text{Média} = (\sum (\text{nível} \times \text{nº participantes})) / \text{nº total de participantes} \quad (4.1)$$

Tabela 4.13 – Maturidade CMMI

Categoria	EU (n=2)	PT (n=15)	Total (n=17)	Total %
Partilham nível 1	0	2	2	11,76%
Partilham nível 2	0	3	3	17,65%
Partilham nível 3	0	7	7	41,18%
Partilham nível 4	2	3	5	29,41%
Partilham nível 5	0	0	0	0,00%

Na maioria, os níveis de CMMI, referentes maturidade organizacional em cibersegurança, relatados pelos participantes de PT incidem no nível 3 (41.18%). Já pela UE, apenas foi relatado o nível de maturidade 4. A análise dos discursos dos participantes sugere existir uma diferença na maturidade organizacional entre instituições bancárias de PT e da UE. Enquanto participantes dos bancos portugueses sugerem uma maturidade média próxima do nível 2,7 (2,73), aproximando-se do nível *Defined*, onde começa a refletir processos padronizados, institucionalizados e conhecidos em toda a organização, os dois participantes de outros bancos da UE atingem uma média de nível 4 (4) (conforme fórmula 4.1), onde a organização tem a análise de dados orientada a decisões de segurança. Numa escala de 1 a 5 (Apêndice E). Opinião de participantes:

"na gestão de risco em cibersegurança nível 3 (E_05)"

"Risco de Cibersegurança estamos no 4 (E_12)"

"Na gestão do risco nível 1 (E_10)"

No segundo subtema, a ENISA desenvolveu a métrica EU CSI com o objetivo de avaliar a postura de cibersegurança dos países membros da UE e da própria EU. Este índex segue uma estrutura hierárquica que inclui indicadores qualitativos e quantitativos distribuídos por áreas como política, operações, capacidade e mercado/indústria, que são agregados com base em pesos e escalados numa pontuação entre 0 e 100.

"EU Cybersecurity Index (EU CSI), desenvolvido pela agência da UE para a cibersegurança, ENISA. Este índice avalia e monitora a maturidade dos EM, incluindo recursos, competências, políticas, tecnologia e sensibilização em cibersegurança, que servem como ferramenta para diagnóstico, comparação e melhoria contínua" (E_17)

No terceiro subtema – Integração, sobre o nível da integração entre as atividades de cibersegurança e CTI, foram obtidas 16 respostas dos 17 participantes (Tabela 4.14). Pela analise dos discursos dos participantes, sugere que só nos dois bancos da UE é que é feita integração e medição, e em PT não integra ou desconhece o que é integração de atividades de cibersegurança com CTI (31.25%).

Tabela 4.14 – Integração de Atividades de Cibersegurança e CTI

Categoria	EU (n=2)	PT (n=14)	Total (n=16)	Total %
Integram e não medem	0	3	3	18,75%
Integram e medem	2	0	2	12,50%
Não Integram	0	6	6	37,50%
Desconhecem	0	5	5	31,25%

Os bancos que fazem integração e medição, obtêm *feeds* de CTI, e a cada trimestre fazem exercícios de *threat hunting*, usando um *Threat Actor* e *Tactics, Techniques and Procedures* (TTPS), são táticas onde definem o objetivo de alto nível do atacante em cada fase da intrusão (v.g.: ganhar acesso inicial, manter persistência, exfiltrar dados). Estas técnicas que são o método específico usado para atingir a tática (v.g.: *phishing* para acesso inicial, uso de *malware* para persistência), procedimentos que são o detalhe prático ou implementação concreta que o atacante usa (v.g.: envio de e-mails com anexos maliciosos, utilização de uma ferramenta específica para roubo de credenciais). Estas comparações normalmente são feitas usando *Threat Intelligence*, no MITRE ATT&CK e em *frameworks* de defesa, porque permitem às equipas de segurança mapear e antecipar como os atacantes atuam.

"(…), medimos, estamos continuamente a ingerir feets de CTI e depois a cada qourter fazemos um exercício de threat hunting que vai obter informação com base nas CTIs. Agarramos em Threat Actor, usamos TTPS, etc e executamos como se fossemos nós um atacante a replicar exatamente o que aconteceu. Depois emitimos um relatório para validar que o que nós estamos a receber destas feets é informação útil ou não" (E_08).

O subtema – Custo Estimado, foi questionado, se o custo estimado de não ter acesso à informação partilhada deveria ser ou não uma métrica, todos os participantes portugueses concordaram, acrescentando que seria uma métrica muito útil. Todavia, afirmam que não conseguem calcular esta métrica, pois ou não têm acesso à informação partilhada ou, tendo acesso, apenas integram a informação nos sistemas de SIEM.

"como se quantifica o benefício ou o prejuízo ou a partilha pela ausência da mesma" (E_03)

"Acho que é uma métrica difícil de fazer, porque não conseguimos saber qual a informação que

não foi partilhada, por isso não se pode medir" (E_5)

Os participantes dos dois bancos da UE também dizem que é uma métrica muito útil, mas que apenas conseguem calcular esta métrica ao nível de sistemas tecnológicos, a partir de informação de CTI que recebem e de testes internos que fazem. Com isto conseguem medir os custos que teriam se não recebessem os *feeds* de CTI (seriam afetados *x* sistemas que têm *y* custo). Mas não sabem como implementar uma métrica deste tipo porque é bastante complexo calcular globalmente o impacto na entidade bancária, dado que envolve variáveis qualitativas e quantitativas e depende do tipo de ataque.

"Eu acho que é relevante, mas não sei como calcular" (E_12)

"Eu acho que é relevante, não sei é como fazer, parece muito complicado, pois envolve muitas variáveis difíceis de medir" (E_08)

Por fim, o subtema – Eficácia e Frequência, a análise do discurso dos participantes sugere que na banca portuguesa não existem métricas ou indicadores para avaliar a eficácia e frequência da partilha de informação, devido a praticamente não existir partilha e, a que existe, ser informal ou entre SOC.

"Não existe" (E_04)

"Não temos métricas, pois não partilhamos com outras instituições e a partilha com o SOC não medimos" (E_11)

No entanto, um dos participantes portugueses indica qua a métrica poderia ser calculada desde que a informação fosse partilhada pelo setor bancário português.

"Sim, porque se a informação de ameaça fosse partilhada na banca. Por exemplo, com recurso a indicadores de comprometimento concretos, se depois se verifica um ataque que é barrado precisamente porque esses indicadores existirem. Podemos associar a ocorrência da defesa com a partilha de informação atempada" (E_17)

Contudo, os dois participantes de bancos da UE mencionam que usam métricas para avaliar a eficácia e a frequência de partilha de informação.

"Temos métricas para avaliar a eficácia e frequência de partilha, mas com FS-ISAC, pois não partilhamos diretamente com outros bancos." (E_12)

Em suma, a análise dos discursos dos participante sugere que as instituições bancárias portuguesas se encontram numa fase inicial em termos de métricas para avaliar a partilha de informação em cibersegurança (maturidade média de nível 1), na maturidade organizacional estão num nível 2,7. A maioria dos participantes de PT refere não utilizar métricas formais, limitando-se a práticas informais ou ligadas a fornecedores externos (SOC), o que compromete a medição da eficácia e frequência da partilha. Já da análise do discurso dos dois participantes de bancos da UE existe uma utilização estruturada de métricas como IoCs, KPI, KRI e CTI, e recorrem a exercícios de *threat hunting* e modelos como o *MITRE ATT&CK* para validar a utilidade da informação recebida (maturidade média de nível 4), na maturidade organizacional estão num nível 4. Verifica-se ainda que, tanto em PT como na UE, os participantes reconhecem a relevância de desenvolver uma métrica para estimar o custo de não ter acesso à informação partilhada, embora a sua implementação seja considerada difícil devido à natureza qualitativa e quantitativa das variáveis envolvidas. Existe uma diferença entre a realidade dos participantes portugueses e os dois da UE, onde sugerem que os bancos nacionais a dependem sobretudo de abordagens *ad-hoc*, enquanto os bancos europeus integram métricas em processos de melhoria contínua e alinhamento regulatório.

4.1.5. Conclusão

Em síntese, apesar da dimensão da amostra em estudo, a análise dos discursos dos participantes sugere identificar diferentes perceções dos participantes. O resultado da análise dos discursos sugere que a partilha de informação em cibersegurança no setor bancário continua a ser limitada, sobretudo em PT, onde predominam barreiras culturais, associadas à falta de confiança e à visão de concorrência, já os dois participantes dos bancos da UE, que está é mais condicionada por barreiras legais e regulamentares. Estas barreiras traduzem-se numa partilha pouco estruturada, frequentemente informal e motivada apenas por exigências regulatórias, o que reduz a eficácia da resposta coletiva às ameaças cibernéticas.

Apesar destas limitações, foram identificados fatores potenciadores da colaboração, nomeadamente, o papel do BP enquanto regulador imparcial, a integração de representantes especializados em cibersegurança nos conselhos de administração e o recurso a plataformas como o CIISI-PT ou FS-ISAC, ainda que estas apresentem diferentes níveis de utilização e integração entre PT e a UE. Quanto ao tipo de informação a partilhar, existe consenso sobre a relevância de indicadores técnicos (IoCs; CTI e KPI) e dados relacionados com fraude, excluindo informação sensível como vulnerabilidades, software de proteção e impacto financeiro. O BCE alterar regulamentos ou diretrizes de forma a que os bancos entendem-se que a partilha em um bem comum e não concorrencial de

forma a começarem proactivamente a partilhar mais.

Verificou-se ainda que os incentivos regulatórios, económicos ou tecnológicos são percecionados como pouco eficazes por grande parte dos participantes, sendo a mudança cultural e o reforço da confiança apontados como elementos essenciais para uma partilha sustentável e voluntária. No que respeita a métricas, os entrevistados indicam que os bancos portugueses se encontram numa fase embrionária, com práticas pouco estruturadas e maturidade média de nível 1 na partilha de informação, ao passo que os bancos da UE apresentam maturidade próxima do nível 4, integrando métricas como IoAs, IoOs, IoCs, CTI e KPI em processos de melhoria contínua. Quanto a maturidade organizacional PT, está num nível de 2,7, e da UE com um nível 4.

Em suma, a análise dos discursos dos participantes sugere uma diferença entre realidade portuguesa e realidade dos participantes dos dois bancos da UE, na maturidade da partilha de informação em cibersegurança, refletindo sobretudo diferenças culturais, regulatórias e organizacionais. A superação destes desafios passará pela criação de uma cultura de confiança e cooperação, suportada por regulação clara, integração tecnológica e utilização de métricas que permitam avaliar de forma objetiva a eficácia da partilha.

4.2. Discussão dos resultados

Nesta seção, discutem-se os principais resultados obtidos, relacionando-os com a literatura existente e com o quadro teórico adotado. O objetivo é compreender em que medida os achados confirmam, ampliam ou desafiam estudos anteriores.

Questão Q1 – Quais as medidas que podem incentivar a uma maior colaboração na partilha de informação sobre cibersegurança entre as instituições bancárias e que tipo de dados podem ser relevantes partilhar? foi analisada à luz da hipótese H1 – "existem barreiras significativas que dificultam a partilha de informação sobre cibersegurança entre instituições bancárias, sendo as barreiras legais e de concorrência as mais determinantes". A análise empírica realizada confirma parcialmente esta hipótese, mas revela dimensões adicionais que permitem complexificar a compreensão do problema e relativizar o peso das diferentes barreiras.

Convergências entre literatura e dados empíricos

A revisão da literatura mostrou que as barreiras legais e regulatórias são amplamente destacadas como limitadoras da partilha de informação. Instrumentos como o RGPD [47], a Lei do Sigilo Bancário [51] e o Regulamento DORA [18] estabelecem restrições claras quanto ao tipo de informação que pode ser partilhada e em que condições. Estudos como [59] [61] e [62] sublinham ainda a sobreposição de normas, a burocracia e a falta de harmonização regulatória, que criam incertezas jurídicas e bloqueiam iniciativas de cooperação entre instituições financeiras. Os participantes corroboram estas conclusões,

destacando as dificuldades práticas resultantes da complexidade normativa: "*demasiadas leis, regulamentos, diretivas e frameworks, muito complexas de interpretação, além de alguns contraditórios entre si*" (E_14; E_17). Este alinhamento confirma que as barreiras legais e regulamentares constituem, de facto, um entrave transversal e estrutural à partilha de informação em cibersegurança.

Divergências entre teoria e prática

Apesar do peso das barreiras legais, a análise dos dados empíricos revela que, no contexto português, as barreiras culturais assumem maior relevância do que inicialmente previsto na hipótese H1. Os participantes destacam uma cultura organizacional de "*security by obscurity*", marcada pelo receio de exposição pública, pelo medo da perda de vantagem competitiva e pela resistência interna à cooperação (E_02, E_05, E_09, E_13). Expressões como: "*alterar a mente dos portugueses*" (E_13) ou "*na banca a partilha não é fácil, devido a serem muito fechados*" (E_05) evidenciam a dimensão cultural como barreira mais crítica no caso português. Esta constatação vai além do que a literatura normativa costuma enfatizar. Enquanto os regulamentos e as diretivas europeias sublinham a importância da partilha (v.g.: DORA, NIS 2), estudos como [55] [57] e [60] já alertavam que fatores de confiança, reputação e cultura interorganizacional são frequentemente negligenciados, mas constituem determinantes centrais para a efetividade da cooperação em cibersegurança. Assim, a análise empírica amplia a visão da literatura ao colocar a dimensão cultural no centro da discussão.

Outra dimensão crítica revelada pelos dados é a barreira de confiança. Embora a literatura refira a necessidade de mecanismos técnicos que garantam a interoperabilidade e a confidencialidade [60], os participantes enfatizam a confiança interpessoal e interorganizacional: receio de que a informação partilhada seja usada de forma inadequada, falta de reciprocidade na troca e medo de perda reputacional. Na prática, isso resulta numa preferência por partilhas informais (bilaterais, em fóruns restritos ou via fornecedores externos) em detrimento de mecanismos estruturados e oficiais (E_03, E_04, E_05, E_17). Este fenómeno sugere que, para além de clarificações normativas, é necessária uma mudança cultural sustentada em mecanismos de confiança e na criação de redes de colaboração estáveis.

Divergência Portugal vs. União Europeia

Um aspeto particularmente relevante é a diferença observada entre PT e outros países da UE. Em PT, predomina a partilha reativa, limitada e muitas vezes apenas por obrigação regulatória (BP, CNCS, CNPD). A cultura de protecionismo e a interpretação restritiva do RGPD inibem partilhas proativas, nomeadamente no combate à fraude. Na UE (em outros Estados-Membros), foram mencionadas práticas mais abertas, com recurso a plataformas colaborativas como a FS-ISAC, que permitem uma partilha estruturada de indicadores de compromisso (IoCs) e inteligência de ameaças (E_08, E_12). Esta comparação evidencia que, apesar de existirem enquadramentos regulatórios comuns (RGPD,

DORA, NIS 2), a aplicação prática varia substancialmente entre países, influenciada por fatores culturais, institucionais e de maturidade tecnológica.

Fraude, um caso paradigmático de divergência regulatória

O problema da fraude bancária é paradigmático. Enquanto países como a Itália criaram plataformas específicas para partilha de informação sobre fraude, envolvendo até autoridades policiais e regulatórias, em PT o BP bloqueia tal partilha com base no RGPD. Os participantes foram unânimes em considerar esta prática contraproducente, uma vez que favorece a propagação da fraude, sobretudo em contextos de criminalidade organizada (*malware* bancário, redes ilícitas) (E_10; E_17). Esta divergência intra-UE demonstra que a interpretação restritiva da legislação nacional fragiliza a resposta coletiva e evidencia a necessidade de harmonização prática, não apenas legal.

Em suma, a análise permite afirmar que a hipótese H1 é parcialmente confirmada: as barreiras legais/regulatórias são determinantes, mas não exclusivas e nem sempre as mais relevantes. Pois as barreiras culturais emergem como fator dominante no contexto português, ampliando as conclusões da literatura. A confiança interorganizacional é um elemento central que articula as dimensões cultural e institucional. Existe uma assimetria entre práticas em PT e em outros países da UE, com os primeiros a privilegiarem uma abordagem restritiva e os segundos a adotarem mecanismos colaborativos mais maduros. A ausência de partilha estruturada, especialmente no combate à fraude, tem impactos negativos diretos na resiliência coletiva e na segurança do setor financeiro nacional.

Implicações práticas e teóricas

Do ponto de vista prático, os resultados apontam para a necessidade de: (i) clarificação regulatória - harmonizar normas europeias e nacionais, eliminando contradições e interpretações restritivas; (ii) transformação cultural - promover iniciativas que fomentem a confiança e a colaboração, como fóruns de partilha, exercícios conjuntos e mecanismos de incentivo positivo; (iii) institucionalização de plataformas seguras - desenvolver ambientes de partilha com garantias de anonimização e de confidencialidade que possam reduzir o medo de exposição e reforçar a reciprocidade.

Do ponto de vista teórico, o estudo mostra que a literatura deve evoluir de uma visão predominantemente normativa para uma análise mais integrada que contemple a dimensão cultural e relacional como fatores críticos da cooperação em cibersegurança.

Questão Q2 – Quais as medidas que podem incentivar a uma maior colaboração na partilha de informação sobre cibersegurança entre as instituições bancárias e que tipo de dados podem ser relevantes partilhar? foi analisada à luz da hipótese H2 – "a adoção de medidas específicas, como plataformas seguras de partilha e quadros legais mais claros, pode aumentar significativamente a

colaboração entre instituições bancárias, especialmente quando acompanhada da definição clara dos tipos de dados a partilhar".

Validação parcial da hipótese

A análise dos resultados sugere que a hipótese H2 é parcialmente confirmada. Tanto a literatura como os dados empíricos apontam que plataformas seguras e quadros normativos mais claros são elementos essenciais, mas insuficientes por si só. Os participantes destacam que a principal barreira não é apenas tecnológica ou regulatória, mas cultural: a ausência de confiança entre instituições, a perceção de risco competitivo e a falta de liderança regulatória tornam a partilha ainda limitada, sobretudo em PT. Assim, a hipótese confirma-se no sentido em que medidas estruturadas (plataformas, enquadramento legal, definição clara dos dados a partilhar) são condições necessárias. Contudo, não são condições suficientes para garantir a colaboração, que exige também mudança cultural, liderança regulatória e alinhamento estratégico ao nível dos conselhos de administração.

A literatura [83] destaca que as TISPs, como STIX/TAXII, FS-ISAC, CIRAS e CIISI-EU, representam um avanço importante, mas carecem de padronização, interoperabilidade e confiança. Os dados empíricos confirmam esta lacuna em PT, embora exista a CIISI-PT e o MISP, os participantes admitem que a participação é limitada e a partilha efetiva quase inexistente. Este contraste é evidente quando comparado com a UE, onde os bancos relatam integração total entre plataformas e uso de ferramentas mais diversificadas (v.g.: *OpenCTI*, *AlienVault* OTX). As instituições da EU usam a plataforma FS-ISAC, ao contrário das instituições de PT, que a maior parte desconhece. O acesso à plataforma não é barato, mas não é por isso que as instituições financeiras PT, não usam, mas sim por falta de conhecimento da plataforma ou não quererem partilhar. A discrepância evidencia uma assimetria de maturidade tecnológica e colaborativa, sugerindo que o problema em PT não está na ausência de plataformas, mas na sua subutilização, consequência da falta de confiança e cultura colaborativa.

A revisão de literatura salienta a importância do DORA, NIS2 e iniciativas regulatórias europeias como catalisadores da partilha [18]. Os participantes confirmam que o BP pode desempenhar um papel central na promoção da colaboração, seja através de instruções mais específicas, seja promovendo fóruns de confiança entre bancos. A análise mostra que, embora exista enquadramento legal, este ainda não é percecionado como suficiente para quebrar as barreiras culturais e organizacionais. A recomendação crítica que emerge é que o regulador não se limite a impor obrigações formais, mas atue também como facilitador cultural, criando espaços de partilha informal e assegurando a proteção contra riscos legais e concorrenciais.

Uma das descobertas mais relevantes da análise é a ênfase dada pelos participantes à falta de confiança como obstáculo central. Muitos referem que a colaboração só pode avançar se houver uma mudança cultural liderada pelo regulador e pela própria administração dos bancos. A sugestão de incluir membros especializados em cibersegurança nos conselhos de administração é particularmente

relevante, pois evidencia que a partilha de informação não pode ser vista como uma função operacional, mas como uma decisão estratégica de gestão. A comparação com outros países, como o modelo italiano citado pelos participantes, reforça que o sucesso da colaboração depende de uma comunidade de confiança, onde os bancos compreendem que a partilha fortalece a segurança coletiva sem comprometer vantagens competitivas.

Tipos de dados a partilhar

A hipótese H2 também pressupõe que a definição clara dos dados a partilhar aumenta a colaboração. Os dados confirmam esse ponto, existe consenso de que a partilha deve incidir em indicadores técnicos (IoCs, TTPs, IoAs, padrões e vetores de ataque, informação sobre fraude). Estes dados são considerados de alto valor coletivo e relativamente menos sensíveis do ponto de vista competitivo. Em contrapartida, há convergência na recusa em partilhar informações mais críticas, como vulnerabilidades específicas, software de proteção, dados de clientes, impacto financeiro ou número de registos afetados. Esta fronteira entre dados partilháveis e não partilháveis revela um equilíbrio entre necessidade de colaboração e proteção da confidencialidade, e confirma a relevância da definição clara de tipologias de dados como condição para aumentar a confiança no processo de partilha.

Inteligência Artificial

Um ponto inovador trazido pelos participantes é o papel da IA na priorização da informação partilhada. Ao classificar indicadores (malicioso, suspeito, benigno) e filtrar o que é mais crítico, a IA poderia reduzir a sobrecarga de informação e aumentar a relevância da partilha. Este ponto complementa a literatura, que se concentra mais em taxonomias e padrões de interoperabilidade [83] [84], sugerindo que a próxima evolução das plataformas de partilha poderá passar pela integração de mecanismos de IA para triagem e validação de dados.

Implicações práticas e teóricas

A análise evidencia que a colaboração na partilha de informação no setor bancário é um desafio multifacetado. A hipótese H2 é validada no sentido de que plataformas seguras e quadros legais claros são essenciais, mas os dados demonstram que a verdadeira barreira é de natureza cultural e relacional. Assim, para aumentar significativamente a colaboração, são necessárias medidas complementares: (i) liderança regulatória ativa (v.g.: BP como facilitador da confiança, à semelhança da ENISA na UE); (ii) mudança cultural *top-down*, com envolvimento dos conselhos de administração e consciencialização dos benefícios coletivos; (iii) definição clara dos tipos de dados a partilhar, privilegiando indicadores técnicos de ataque e fraude; (iv) adoção de tecnologias avançadas (IA, interoperabilidade STIX/TAXII, integração de plataformas) para reduzir riscos e aumentar eficiência; (v) comunidades de confiança que combinem fóruns formais e informais, permitindo que a colaboração evolua gradualmente.

Portanto, mais do que criar plataformas ou normas, o setor bancário necessita de um ecossistema colaborativo sustentado em confiança, regulação clara e inovação tecnológica, capaz de transformar a partilha de informação numa prática estratégica e sustentável para a resiliência coletiva do sistema bancário.

Questão Q3 – Como os incentivos regulatórios, económicos e tecnológicos podem ser usados para promover a partilha de informação sobre cibersegurança entre as instituições bancárias e qual o seu impacto na segurança coletiva do setor? foi investigada à luz da hipótese H3 – "os incentivos regulatórios, económicos e tecnológicos (alinhados com os requisitos legais e de *compliance)* têm um papel positivo na promoção da partilha de informação sobre cibersegurança".

Confirmação parcial e nuances da hipótese

Os dados empíricos revelam uma divergência significativa entre a literatura e a perceção prática dos participantes. Enquanto a revisão teórica aponta para o papel positivo dos incentivos como catalisadores da partilha [93] [96], 72,7% dos participantes consideram-nos ineficazes ou até contraproducentes. Esse resultado sugere que a hipótese H3 não é validada de forma linear: embora os incentivos possam desempenhar um papel positivo, a sua eficácia depende fortemente de confiança, cultura organizacional e desenho do mecanismo de incentivo. A crítica mais frequente diz respeito ao risco de incentivos económicos distorcerem o processo, levando a práticas como a partilha de informação pouco fidedigna apenas para obter benefícios. Nesse sentido, os dados convergem com a literatura que destaca os problemas de confiança e falta de padronização como obstáculos centrais à colaboração em cibersegurança [96]. Assim, verifica-se que o incentivo por si só não resolve a barreira cultural e organizacional existente, e pode até gerar efeitos indesejados.

Os resultados apontam que os incentivos percebidos como mais eficazes são os de carácter regulatório, sobretudo aqueles associados a diretivas como a NIS2 e o Regulamento DORA, que introduzem sanções e penalizações para o incumprimento. Essa visão alinha-se com modelos *top-down,* nos quais a pressão normativa atua como catalisador da mudança organizacional. No entanto, embora a regulação seja reconhecida como necessária, vários participantes sublinham que a partilha espontânea e voluntária deveria ser o objetivo final, sob pena de se criar uma cultura de *compliance* mínimo, em vez de uma cultura de confiança e colaboração genuína. Aqui, verifica-se uma tensão crítica entre regulação formal e iniciativas informais. Enquanto a regulação garante padronização e cumprimento mínimo, a literatura destaca que soluções descentralizadas baseadas em confiança, como fóruns colaborativos ou tecnologias emergentes (*Blockchain*, contratos inteligentes), podem mitigar problemas de privacidade e interoperabilidade [96]. Este contraste sugere que uma abordagem híbrida – combinando regulação clara com mecanismos tecnológicos inovadores – pode ser mais eficaz.

Embora teoricamente os incentivos económicos possam aumentar a adesão à partilha, os participantes consideraram-nos problemáticos, pois poderiam gerar oportunismo e partilha sem qualidade ("partilhar só por partilhar"). Essa crítica reforça a ideia de que, no setor bancário, onde a confiança e a precisão da informação são vitais, incentivos monetários não substituem a necessidade de confiança institucional. Além disso, a dependência de incentivos externos pode minar a construção de uma cultura organizacional que valorize a partilha como um bem coletivo. Em contraste, exemplos europeus sugerem que a demonstração de benefícios tangíveis (como a melhoria na deteção de incidentes ou a redução de perdas financeiras) pode ser um incentivo mais sustentável do que recompensas diretas.

A literatura sugere que o uso de tecnologias como STIX™, OWL e Blockchain pode fornecer incentivos indiretos, ao garantir interoperabilidade, anonimato e confiança descentralizada [96]. Contudo, nenhum dos participantes referiu explicitamente a adoção destas soluções, indicando que o potencial tecnológico ainda está pouco explorado no setor bancário português. Essa ausência revela uma lacuna entre teoria e prática, embora haja propostas robustas em termos tecnológicos, faltam estudos de caso e implementações concretas em contextos regulados, como o setor bancário. Assim, verifica-se uma oportunidade de investigação aplicada que explore como estas soluções podem ser integradas em ecossistemas financeiros já regidos por normas estritas.

Um consenso emergente entre os participantes é que confiança e cultura organizacional são fatores mais decisivos do que os incentivos em si. A desconfiança quanto ao uso da informação partilhada, aliada ao receio de fuga de dados sensíveis, compromete a adesão às práticas de colaboração. Alguns participantes defendem a criação de fóruns informais para fortalecer a confiança entre profissionais antes da institucionalização da partilha. Esse resultado dialoga com a literatura, que reconhece que, sem confiança, até mesmo plataformas bem desenhadas podem falhar na promoção da colaboração [93]. Portanto, o impacto positivo dos incentivos na segurança coletiva só se materializa se acompanhado por mecanismos de construção de confiança interorganizacional, que permitam que a partilha deixe de ser percebida como um risco competitivo e passe a ser entendida como um bem coletivo para a resiliência do setor.

Em suma, a análise mostra que a hipótese H3 é confirmada apenas parcialmente. Os incentivos regulatórios, económicos e tecnológicos têm potencial para promover a partilha de informação, mas a sua eficácia está condicionada a três fatores críticos: (i) confiança interorganizacional - que não pode ser substituída por incentivos externos; (ii) cultura organizacional - que deve valorizar a partilha como prática intrínseca e não apenas como requisito legal; (iii) integração de incentivos regulatórios e tecnológicos - de forma a garantir simultaneamente padronização, segurança e inovação. Assim, enquanto a regulação (v.g.: NIS2, DORA) pode servir como gatilho inicial, a verdadeira maturidade na

partilha de informação só será alcançada com incentivos positivos baseados em benefícios coletivos, reforço de confiança e soluções tecnológicas que assegurem anonimato e interoperabilidade. Esta visão crítica indica que, no setor bancário, a simples existência de incentivos não é suficiente, é necessário um ecossistema que combine normas, cultura e tecnologia para transformar a partilha de informação numa prática consolidada e sustentável.

Questão Q4 – Que métricas existem, ou poderiam ser desenvolvidas, para avaliar o nível de maturidade na partilha de informação sobre cibersegurança no setor bancário? à luz da hipótese H4 – "não existem métricas padronizadas para avaliar a maturidade da partilha de informação em cibersegurança no setor bancário".

Confirmação parcial da hipótese e realidade portuguesa

A análise dos dados confirma que, em PT, não existem métricas formalizadas ou padronizadas para avaliar a maturidade da partilha de informação. Os participantes portugueses relataram níveis de maturidade predominantemente baixos (níveis 1 e 2), refletindo práticas incipientes, informais e em muitos casos restritas ao relacionamento com fornecedores externos (SOC). Esse cenário compromete a capacidade de monitorizar a eficácia e frequência do impacto da partilha de informação, alinhando-se com as conclusões da ENISA, que identificou limitações significativas de recursos humanos, financeiros e tecnológicos no contexto nacional [103].

Esta ausência de métricas robustas em PT reforça a hipótese H4, mas de forma parcial: não se trata da inexistência absoluta de métricas de cibersegurança, já que algumas instituições reportam o uso de KPI, KRI e IoCs, mas sim da inexistência de métricas aplicadas especificamente à maturidade da partilha de informação. Assim, verifica-se um vazio metodológico que fragiliza a capacidade nacional de diagnóstico e melhoria contínua.

Cenário europeu, métricas estruturadas e alinhamento regulatório

Em contraste, as instituições bancárias da UE demonstram uma realidade mais avançada, reportando níveis médios de maturidade de nível 4. As práticas identificadas incluem o uso de métricas técnicas (IoCs, IoAs, IoOs), métricas de gestão (KRI, KPI) e a integração com CTI. Estas práticas não só permitem medir a eficácia e a frequência da partilha, mas também criar ciclos de retroalimentação entre operações técnicas e decisões estratégicas, o que está em linha com os níveis de maturidade com base nas recomendações do NIST [94] e metodologias como o MITRE ATT&CK. Este alinhamento entre métricas técnicas e de gestão reflete um modelo de maturidade baseado em colaboração estruturada, regulação europeia (NIS2) e inovação tecnológica, demonstrando que a medição da partilha de informação é viável quando integrada em ecossistemas de confiança como os ISACs [102]. As métricas organizações de cibersegurança, estão alinhadas com *frameworks* como o CMMI [100].

Cenário europeu vs. Cenário português

Na amostra, métricas técnicas (IoCs) foram as mais usadas (v.g.: ≈ 31.6% no conjunto; 37% em PT), seguidas por KPI (≈21.1%). Bancos da UE demonstraram maior integração entre métricas técnicas e de gestão; em PT a utilização é mais fragmentada e, muitas vezes, limitada ao fluxo entre SOCs ou a reportes obrigatórios. Esta heterogeneidade confirma que, apesar de existirem medidores úteis, a ausência de harmonização impede comparações credíveis e avaliações de maturidade entre organizações e jurisdições.

Lacunas e oportunidades, a métrica do custo da não partilha

Um dos pontos mais relevantes emergentes das entrevistas foi a sugestão de desenvolver uma métrica que quantifique o custo de não ter acesso à informação partilhada. Tanto os participantes portugueses quanto os europeus reconheceram o valor desta métrica, mas salientaram a sua complexidade de implementação, já que envolve variáveis qualitativas (impacto reputacional, confiança interinstitucional) e quantitativas (número de sistemas afetados, custos de mitigação). Esta dificuldade está alinhada com a literatura, que aponta para a necessidade de combinar métricas tradicionais (KPI, KRI, IoCs) com indicadores inovadores capazes de capturar impactos indiretos e intangíveis [99] [101]. A crítica aqui reside no facto de o setor bancário português não possuir sequer a infraestrutura básica para iniciar tais medições, enquanto a UE já experimenta metodologias avançadas, como simulações de *threat hunting* baseadas em CTI e TTPS, com capacidade de validar se a informação partilhada foi efetivamente útil para prevenir incidentes.

Proposta teórica — um Índice de Maturidade de Partilha (IMP)

Para operacionalizar e padronizar a avaliação, é proposto um índice híbrido e sustentável — IMP.

Metodologia do índice proposto: o IMP é um índice composto que quantifica a maturidade da partilha de informação de cibersegurança no setor bancário através de sete sub-métricas normalizadas: Frequência (F), Qualidade (Q), Tempestividade (T), Reciprocidade (R), Integração tecnológica (I), Adoção de standards (S) e Impacto mensurável (IM). Cada sub-métrica é transformada para o intervalo [0,1] por funções de normalização com limites regulatórios e técnicas de robustez (*winsorization*; uso de medianas). O IMP é a soma ponderada $\sum w_i X_i$ com $\sum w_i = 1$, onde os pesos são determinados por consenso regulatório e revisão anual. O impacto (IM) combina evidência operacional (redução de MTTD/MTTR por *Difference-in-Differences*) e económica (Custo da Não-Partilha em modelos contrafactuais), com intervalos de confiança por *bootstrap*. O modelo inclui gestão de dados, auditoria independente e medidas anti-incentivos. Resultados são apresentados em *dashboards* com *trending*, radar por sub-métrica e análises de sensibilidade a pesos e limites.

$$IMP = w_1 \cdot F + w_2 \cdot Q + w_3 \cdot T + w_4 \cdot R + w_5 \cdot I + w_6 \cdot S + w_7 \cdot IM \quad (4.2)$$

onde: (i) F (Frequência) - número de eventos/indicadores partilhados por período normalizado por

número de incidentes relevantes; (ii) Q (Qualidade/Relevância) - percentagem de indicadores validados que geraram ação (v.g.: bloqueio, correção); (iii) T (Tempestividade) - média do tempo entre deteção e partilha (invertida/normalizada — menor tempo = melhor pontuação); (iv) R (Reciprocidade) - relação entre aquilo que uma entidade partilha e aquilo que recebe de pares (score de bilateralidade); (v) I (Integração CTI/Tecnológica) - percentagem de sistemas (SIEM/CTI) integrados e capazes de consumir *feeds*; (vi) S (Adoção de Standards) - conformidade com taxonomias e protocolos (STIX/TAXII, MISP, MITRE *mappings*); (viii) IM (Impacto Mensurável) - incidência de eventos evitados ou mitigados graças à informação partilhada (ver sugestão abaixo para o cálculo de IM).

Sugestão de pesos feita pelos participantes: w_1=0.15, w_2=0.20, w_3=0.15, w_4=0.15, w_5=0.15, w_6=0.10, w_7=0.10 (somam 1). Os pesos devem ser ajustados por consenso entre regulador e setor bancário.

Como medir o "IM — impacto" (métrica mais complexa) : (i) abordagem prática - calcular variação no MTTD/MTTR (*mean time to detect/resolve*) associada à entrada de *feeds* externos; usar exercícios controlados (*threat hunting* simulado) para validar que um IoC partilhado reduziu o tempo de deteção e/ou evitou comprometimentos; (ii) método económico - estimar Custo da Não-Partilha por cenário — comparar custo médio por incidente (dados históricos) com o número estimado de incidentes que seriam evitados com partilha atempada (modelos contrafactuais ou experiências de piloto). Reconhece-se que este cálculo é complexo, mas viável em pilotos coordenados.

Implicações práticas e administrativas: (i) regulação e padronização - BP (autoridade competente), iniciativas como CIISI-PT deveriam liderar a definição de um IMP mínimo, com taxonomia comum e requisitos de *logging* de partilha; (ii) pilotos e validação - Executar pilotos nacionais/europeus que recolham dados de plataformas (*logs* STIX/TAXII, SIEM, MISP) para calibrar pesos e validar a relação entre pontuação IMP e resultados operacionais; (iii) transparência controlada - Exigir metadados de partilha (sem expor conteúdo sensível) para alimentar métricas sem violar o RGPD ou o sigilo bancário.

A ausência de métricas de partilha em PT compromete: (i) capacidade de *benchmarking* entre instituições; (ii) identificação de lacunas sistémicas; (iii) integração com iniciativas regulatórias europeias, como a NIS2.

Em síntese, os dados confirmam que o setor bancário português se encontra numa fase incipiente e pouco estruturada, dependente de práticas *ad-hoc* e com ausência de métricas para partilha de informação, o que valida a hipótese H4. Em contrapartida, o setor bancário europeu revela práticas avançadas de medição e integração de métricas, sustentadas por estruturas colaborativas, exercícios de CTI e regulação comunitária. Esta disparidade sugere que a adoção de métricas padronizadas não é apenas uma questão de capacidade técnica, mas também de cultura organizacional e alinhamento

político-regulatório. O futuro da investigação e da prática aponta para a necessidade de desenvolver modelos híbridos de medição, capazes de quantificar tanto os benefícios diretos (redução de incidentes) quanto os custos da ausência de partilha, fornecendo uma base mais robusta para a evolução da maturidade no setor bancário.

A formulação rígida de H4 (“Não existem métricas padronizadas…”) é em grande parte verdadeira no sentido de ausência de um índice consensual e específico para maturidade de partilha. Porém, a afirmação carece de nuance - existem métricas e indicadores relevantes que constituem blocos de construção (IoCs, KPI, KRI, EU-CSI, integração CTI), e esses blocos permitem — com coordenação regulatória e técnica — a criação de um padrão operacionalizável (v.g.: IMP). Assim, H4 deve ser considerada confirmada parcialmente, não existem hoje métricas padronizadas, mas existem bases técnicas e métricas parciais suficientes para desenvolver e pilotar um padrão sectorial.

CAPÍTULO 5

Conclusão, Limitações do Estudo e Recomendações

5.1. Conclusão

A presente investigação teve como objetivo analisar os fatores que condicionam a partilha de informação sobre cibersegurança no setor bancário, explorando barreiras, colaboração à partilha, incentivos e métricas. O estudo baseou-se em quatro questões de investigação (Q1–Q4) e as respetivas hipóteses, analisadas criticamente através da combinação entre revisão de literatura e dados empíricos recolhidos junto de profissionais de cibersegurança do setor bancário em PT e em bancos da UE.

Q1 – Barreiras à partilha de informação

A hipótese H1 foi parcialmente confirmada. Embora as barreiras legais, regulatórias e de concorrência sejam relevantes, a análise empírica revelou que, no caso português, as barreiras culturais (resistência à cooperação, protecionismo, receio de exposição pública) são as mais determinantes. Acresce ainda a barreira da confiança, raramente destacada na literatura, mas central na prática, refletindo a ausência de reciprocidade e o medo do uso indevido da informação. Verificou-se também uma divergência relevante entre PT (predomínio de práticas restritivas e partilha reativa) e outros países da UE (mecanismos colaborativos mais estruturados, v.g.: FS-ISAC).

Q2 – Medidas que podem incentivar a uma maior colaboração na partilha de informação

A hipótese H2 foi confirmada. A confiança interpessoal, interorganizacional e institucional é um fator crítico para viabilizar a partilha de informação. No entanto, a confiança não emerge espontaneamente, depende da criação de redes formais e informais, de mecanismos de anonimização e da perceção de benefícios mútuos. A cultura de "*security by obscurity*" ainda prevalece em PT, mas experiências internacionais mostram que plataformas estruturadas podem atenuar o problema. A partilha de informação em cibersegurança tem um impacto direto e positivo na capacidade coletiva de prevenção, deteção, resposta e recuperação de incidentes. Contudo, o impacto depende da qualidade, tempestividade e fidedignidade da informação partilhada. Observou-se que, em PT, a partilha é predominantemente reativa e regulatória, limitando o seu valor estratégico, enquanto em alguns países da UE existem práticas mais maduras e colaborativas que aumentam a eficácia na luta contra o cibercrime e a fraude.

Q3 – Incentivos regulatórios, económicos e tecnológicos

A hipótese H3 foi confirmada apenas parcialmente. Apesar de os incentivos regulatórios e tecnológicos serem importantes, a maioria dos participantes considera que incentivos económicos

diretos podem ser contraproducentes, levando à partilha de informação de baixa qualidade ou meramente instrumental. O que se destaca é a necessidade de incentivos de natureza cultural e institucional, como a valorização pública das boas práticas, conferências e demonstração dos benefícios da partilha. A legislação europeia (v.g.: DORA, NIS 2) desempenha um papel relevante, mas só terá impacto real quando acompanhada por mecanismos de confiança e mudança cultural.

Q4 – Métricas para avaliar a maturidade da partilha de informação

A hipótese H4 afirmava a inexistência de métricas padronizadas. A análise integrada da literatura e dos dados empíricos permite tirar as seguintes conclusões: (i) nas práticas observadas, existem métricas consolidadas que medem aspetos relevantes, concretamente, métricas técnicas (IoCs, IoAs, IoOs); métricas de gestão (KPI, KRI); e indicadores derivados de CTI (qualidade e integração de *feeds*). Há também índices institucionais (v.g.: EU-CSI) que avaliam a postura global de cibersegurança; (ii) existência de métricas parciais, mas ausência de um padrão específico para "maturidade de partilha". Contudo, existem métricas parciais e complementares (IoCs, KPI, KRI, EU-CSI, integração CTI), que podem servir de base ao desenvolvimento de um Índice de Maturidade de Partilha (IMP), conforme proposto pelo investigador.

A hipótese H4 deve, portanto, ser entendida como parcialmente confirmada, não há uma métrica consolidada, mas existem blocos técnicos e conceptuais suficientes para a construção de um modelo robusto.

De forma global, a investigação demonstra que a partilha de informação em cibersegurança no setor bancário é uma necessidade inadiável, mas que permanece limitada por barreiras culturais, legislativas, normativa e regulamentar. A realidade portuguesa caracteriza-se por uma partilha reduzida, predominantemente informal e reativa (limitada ao reporte obrigatório a reguladores), medo da perda de competitividade, no entanto pela análise do discurso dos dois participantes dos bancos da UE têm práticas mais estruturadas. A superação deste bloqueio exige clareza regulatória, mecanismos de confiança institucional, adoção de métricas objetivas que permitam medir, comparar e melhorar continuamente o nível de colaboração e, sobretudo, uma mudança cultural e organizacional profunda que reconheça a cibersegurança como um bem comum. Os resultados permitem concluir que a partilha de informação em cibersegurança no setor bancário é uma necessidade reconhecida, mas ainda longe de ser uma prática consolidada.

5.2. Contributos da Investigação

A investigação produziu contributos em três planos distintos: teórico-científico, prático-operacional e metodológico.

Teórico-Científico – (i) avança na compreensão académica sobre as barreiras culturais, organizacionais e legais que limitam a partilha de informação, aprofundando a discussão existente na literatura; (ii) propõe uma tipologia clara de dados partilháveis vs. não partilháveis, apoiada em evidência empírica, que pode ser replicada noutras jurisdições; (iii) introduz o conceito de um Índice de Maturidade de Partilha (IMP), combinando métricas técnicas, de gestão e de impacto, representando um contributo inovador para futuras abordagens de avaliação da maturidade colaborativa.

Prático-operacional - Identifica medidas concretas para incentivar a colaboração, incluindo: (i) plataformas seguras de partilha interoperáveis; (ii) envolvimento dos Conselhos de Administração; (iii) papel regulador ativo do BP; (iv) utilização de IA na gestão de informação partilhada; (v) fornece aos decisores institucionais e reguladores um quadro estruturado de dados prioritários para partilha (IoCs, TTPs, fraude) e dados a excluir da partilha (vulnerabilidades críticas, dados de clientes).

Metodológico - apresenta uma aplicação robusta da análise qualitativa, cruzando entrevistas com literatura, o que reforça a validade dos resultados. E oferece um caminho prático para a construção de métricas, integrando dimensões técnicas e organizacionais, permitindo replicação em estudos futuros.

5.3. Limitações do Estudo

Nenhum estudo está isento de limitações e o presente não é exceção. As principais limitações desta dissertação têm de ser reconhecidas e tidas em conta, e incidem essencialmente ao nível da revisão de literatura e dos dados obtidos.

Na revisão de literatura pode ter existido: (i) uma definição errada de palavras-chave e dos critérios de inclusão/exclusão; (ii) uma análise incompleta devido ao estudo ter incidido em dados essencialmente posteriores a 2020; (iii) défice de estudos académicos específicos que analisem a partilha de informação em cibersegurança no setor bancário, especialmente em contexto europeu e português; (iv) falta de dados empíricos e estudos de caso que demonstrem a eficácia real de práticas colaborativas no combate a ciberameaças. Para contrariar a alínea (i) e (ii) foram feitas pesquisas cinzentas sem datas, por *snowball* e a partir de conversas/reuniões com o orientador.

Ao nível dos dados: (i) amostra limitada – o estudo baseou-se em 17 entrevistas obtidas por conveniência, o que não permite generalizar resultados para todo o setor bancário; (ii) viés de perceção – as respostas refletem opiniões subjetivas, podendo estar influenciadas por experiências pessoais, posição hierárquica ou contexto institucional dos participantes; (iii) a natureza exploratória

e qualitativa privilegiou a profundidade em detrimento da amplitude. A ausência de dados quantitativos limita a possibilidade de medir estatisticamente o impacto das barreiras ou a efetividade das práticas de partilha (iv) falta de diversidade geográfica e institucional – a análise pode não captar diferenças relevantes entre bancos de diferentes dimensões e geografias, restringindo a comparabilidade global; (v) carência de dados quantitativos objetivos – a análise foca-se em perceções, não incluindo métricas empíricas sobre efetividade das questões a responder; (vi) o enquadramento regulatório europeu em cibersegurança (v.g.: DORA, NIS2) encontra-se em constante atualização. Algumas conclusões poderão ser afetadas por alterações futuras na legislação ou pela criação de novos mecanismos de partilha obrigatória; (vii) embora se tenha proposto a construção do IMP, este não foi implementado ou testado empiricamente, permanecendo como contributo conceptual.

Estas lacunas oferecem oportunidades valiosas para futuras investigações académicas, sobretudo em estudos que aliem a análise teórica à aplicação prática em ambientes bancários reais.

5.4. Recomendações para futuras Investigações

Para investigações futuras, sugere-se: (i) utilização de outros métodos de investigação, como métodos mistos com o objetivo de combinar entrevistas qualitativas com inquéritos quantitativos, e métodos probabilísticos para reduzir viés; (ii) incluir mais instituições bancárias e de diferentes geografias e atores regulatórios; (iii) fazer estudos comparativos com outros setores críticos para analisar se o nível de partilha de informação sobre cibersegurança sofre os mesmos problemas que no setor bancário, ou se existe boas práticas para replicar no setor bancário; (iv) investigar se a introdução de novos regulamentos que não sejam contraditórios entre si e de plataformas seguras com anonimização, aumentam a confiança e a qualidade da informação partilhada ao longo do tempo; (v) validação empírica do IMP – desenvolver e testar empiricamente um índice de maturidade em colaboração com bancos portugueses e de outros países; (vi) investigar como a IA pode classificar, filtrar e priorizar informação partilhada, reduzindo falsos positivos e maximizando valor operacional e estudar os riscos associados à IA na partilha (viés algorítmico, risco de manipulação); (vii) desenvolver *frameworks* que quantifiquem o impacto económico da partilha (custos de não partilhar vs. benefícios da cooperação), apoiando decisões de investimento em cibersegurança colaborativa; (Viii) avaliar de que forma a implementação plena do DORA e da NIS 2 irá transformar a partilha de informação em cibersegurança no setor bancário europeu.

5.5. Implicações práticas para o Setor Bancário

Os resultados obtidos permitem identificar um conjunto de recomendações práticas para o setor bancário, de forma a melhorar a partilha de informação em cibersegurança e, consequentemente, a resiliência coletiva do setor.

É necessário ir além dos incentivos formais e apostar numa combinação equilibrada de mecanismos regulatórios, tecnológicos e, sobretudo, de confiança e cultura organizacional. Elenquem-se as seguintes recomendações: (i) necessidade de fomentar a confiança entre os diferentes atores do setor; (ii) criar fóruns informais, grupos de trabalho e redes colaborativas que aproximem os profissionais, permitindo o desenvolvimento de relações de confiança interpessoal (esta aproximação favorece uma partilha mais espontânea, transparente e de maior valor acrescentado); (iii) importa salientar a relevância de uma abordagem integrada entre incentivos formais e culturais; (iv) Se, por um lado, os incentivos regulatórios e até penalizações podem assegurar um nível mínimo de conformidade, por outro lado, devem ser complementados por incentivos positivos, como o reconhecimento público, o benchmarking setorial e a valorização em conferências e seminários; (v) reforço da literacia e cultura de cibersegurança; (vi) investir na sensibilização e formação contínua dos colaboradores (para que compreendam o valor estratégico da partilha e percebam que esta não representa uma ameaça à competitividade, mas sim um benefício coletivo para o setor bancário); (vii) as instituições devem procurar inovar de forma cautelosa, explorando soluções novas, contratos inteligentes e padrões de interoperabilidade (v.g.: STIX™, OWL) que possam aumentar a confiança e reduzir barreiras técnicas à partilha de informação. Contudo, a adoção destas tecnologias deve ser cuidadosamente avaliada em termos de viabilidade prática, custos e alinhamento com requisitos regulatórios; (viii) reforço da cooperação com reguladores e entidades supervisoras.

Referências Bibliográficas

[1] "Cybersecurity in finance is critical to safeguarding economic resilience." Accessed: Jan. 04, 2025. [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-of-critical-sectors/finance

[2] B. Portugal, "Relatório de Estabilidade Financeira - Banco de Portugal - GEE," Nov. 2022. Accessed: Jan. 04, 2025. [Online]. Available: https://www.gee.gov.pt/pt/indicadores-diarios/ultimos-indicadores/32498-relatorio-de-estabilidade-financeira-banco-de-portugal-6

[3] European Central Bank, "Cyber Resilience for Financial Market Infrastructures." Accessed: Jan. 04, 2025. [Online]. Available: https://figi.itu.int/wp-content/uploads/2021/05/FIGIECBOperationalCyberFinalWeb1213.pdf

[4] R. Levine, "Chapter 12 Finance and Growth: Theory and Evidence," in *Handbook of Economic Growth*, vol. 1, no. SUPPL. PART A, Elsevier, 2005, pp. 865–934. doi: 10.1016/S1574-0684(05)01012-9.

[5] M. Ebrahimi Kahou and A. Lehar, "Macroprudential policy: A review," *Journal of Financial Stability*, vol. 29, pp. 92–105, Apr. 2017, doi: 10.1016/j.jfs.2016.12.005.

[6] E. Meuleman and R. Vander Vennet, "Macroprudential policy and bank systemic risk," *Journal of Financial Stability*, vol. 47, p. 100724, Apr. 2020, doi: 10.1016/j.jfs.2020.100724.

[7] R. Zhang and S. Ben Naceur, "Financial development, inequality, and poverty: Some international evidence," *International Review of Economics & Finance*, vol. 61, pp. 1–16, May 2019, doi: 10.1016/j.iref.2018.12.015.

[8] D. Hu and C. Gan, "Green finance development and its origin, motives, and barriers: an exploratory study," *Environ Dev Sustain*, Jan. 2025, doi: 10.1007/s10668-024-05570-w.

[9] J. Yang, D. Lu, and J. Shi, "Does digital financial inclusion promote intergenerational income mobility? Evidence from China," *Financ Res Lett*, vol. 82, p. 107637, Sep. 2025, doi: 10.1016/j.frl.2025.107637.

[10] D. M. Carvalho, "O sistema financeiro e o crescimento económico," Universidade do Minho, 2019. Accessed: Sep. 28, 2025. [Online]. Available: https://1library.org/article/o-sistema-financeiro-e-o-crescimento-econ%C3%B3mico.yjdmlxmy

[11] E. Teixeira and T. Filho, "O Sistema Financeiro Globalizado Contemporâneo: Estrutura e Perspetivas," Jan. 2015. Accessed: Sep. 28, 2025. [Online]. Available: https://repositorio.ipea.gov.br/server/api/core/bitstreams/264ebcbd-bc39-4f43-81cd-f1d1d8a44af2/content

[12] World Economic Forum, "The Global Risk Report 2024," Jan. 2024. Accessed: Nov. 06, 2024. [Online]. Available: https://www.weforum.org/publications/global-risks-report-2024/

[13] L. Ponemon and K. Bissell, “The Cost of Cybercrime,” 2019. Accessed: Nov. 06, 2024. [Online]. Available: https://iapp.org/media/pdf/resource_center/accenture_cost_of_cybercrime_study_2019.pdf

[14] “Decreto-Lei n.o 22/2025 | DR.” Accessed: Aug. 18, 2025. [Online]. Available: https://diariodarepublica.pt/dr/detalhe/decreto-lei/22-2025-911488699

[15] I. Lella, “Enisa Threat Landscape 2024,” Sep. 2024. doi: 10.2824/0710888.

[16] “Annual report NIS Directive incidents 2024 CG Publication,” Aug. 2025. Accessed: Aug. 18, 2025. [Online]. Available: https://ec.europa.eu/newsroom/repository/document/2025-31/Annual_Report_NISD_Security_Incidents_2024_lLl8Yt8at5UKGOymYgsc0rxZrpQ_118680.pdf?

[17] “Digital Operational Resilience Act | Advisory | Serviços | PwC Portugal.” Accessed: Feb. 06, 2025. [Online]. Available: https://www.pwc.pt/pt/servicos/advisory/digital-operational-resilience-act.html

[18] União Europeia, “Regulamento - 2022/2554 - EN - EUR-Lex,” Dec. 2022. Accessed: Feb. 08, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022R2554

[19] K. Chamberlain, “Cyber Threats: How Banks Can Share Information Effectively | ABA Banking Journal,” *ABA Banking Journal*, Nov. 2018, Accessed: Feb. 12, 2025. [Online]. Available: https://bankingjournal.aba.com/2018/11/cyber-threats-how-banks-can-share-information-effectively/?

[20] “The cyber clock is ticking: Derisking emerging technologies in financial services,” Mar. 2024. Accessed: Jan. 04, 2025. [Online]. Available: https://www.mckinsey.com/capabilities/risk-and-resilience/our-insights/the-cyber-clock-is-ticking-derisking-emerging-technologies-in-financial-services#/

[21] Â. Maia and E. Fernandes, “Grounded Theory.” Accessed: Feb. 09, 2025. [Online]. Available: https://repositorium.uminho.pt/bitstream/1822/4209/1/Grounded%20Theory.pdf

[22] K. Krippendorff, *Content Analysis: An Introduction to Its Methodology*. 2455 Teller Road, Thousand Oaks California 91320 : SAGE Publications, Inc., 2019. doi: 10.4135/9781071878781.

[23] L. Bardin, *Analise_de_conteudo_Lisboa*. France, 1977. Accessed: Sep. 24, 2025. [Online]. Available: https://www.academia.edu/40820250/BARDlN_L_1977_An%C3%A1lise_de_conte%C3%BAdo_Lisboa_edi%C3%A7%C3%B5es_70_225

[24] M. Page, J. Mckenzie, and K. Shing, “Declaração PRISMA 2020: uma Diretriz Atualizada para Publicação de Revisões Sistemáticas,” Aug. 2024. doi: https://doi.org/10.5281/zenodo.13271469.

[25] “Scopus - Document search.” Accessed: Mar. 09, 2025. [Online]. Available: https://www.scopus.com/search/form.uri?display=basic&zone=header&origin=#basic

[26] “Document Search - Web of Science Core Collection.” Accessed: Mar. 09, 2025. [Online]. Available: https://www.webofscience.com/wos/woscc/basic-search

[27] “EBSCOhost Research Databases.” Accessed: Apr. 20, 2025. [Online]. Available: https://research.ebsco.com/c/htqn2w/search/advanced/filters?autocorrect=y

[28] M. Visser, N. J. van Eck, and L. Waltman, “Large-scale comparison of bibliographic data sources: Scopus, Web of Science, Dimensions, Crossref, and Microsoft Academic,” *Quantitative Science Studies*, vol. 2, no. 1, pp. 20–41, Apr. 2021, doi: 10.1162/qss_a_00112.

[29] C. Wohlin, “Guidelines for snowballing in systematic literature studies and a replication in software engineering,” in *Proceedings of the 18th International Conference on Evaluation and Assessment in Software Engineering*, New York, NY, USA: ACM, May 2014, pp. 1–10. doi: 10.1145/2601248.2601268.

[30] E. J. do Nascimento and F. K. de Oliveira, “Análise Comparativa entre as Técnicas Tradicional e Snowbolling da revisão Sistemática da literatura acerca dos recursos educacionais abertos,” *Jornada de Iniciação Científica e Extensão*, vol. 14, no. 1, p. 99, Sep. 2019, Accessed: Mar. 09, 2025. [Online]. Available: https://periodicos.ifsertao-pe.edu.br/ojs2/index.php/jince/article/view/749

[31] V. Garousi, M. Felderer, and M. V. Mäntylä, “Guidelines for including grey literature and conducting multivocal literature reviews in software engineering,” *Inf Softw Technol*, vol. 106, pp. 101–121, Feb. 2019, doi: 10.1016/j.infsof.2018.09.006.

[32] CNSS, “Committee on National Security Systems Committee on National Security Systems (CNSS) Glossary,” Apr. 2015. Accessed: Dec. 28, 2024. [Online]. Available: http://www.cnss.gov.

[33] “O que é gerenciamento de riscos cibernéticos?,” IBM. Accessed: Dec. 28, 2024. [Online]. Available: https://www.ibm.com/br-pt/topics/cyber-risk-management?utm_source=chatgpt.com

[34] CNCS, “Quadro Nacional de Referência para a Cibersegurança,” *CNCS*. Accessed: Feb. 05, 2025. [Online]. Available: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

[35] “Estratégia Nacional de Segurança Cibernética-e-Ciber,” Feb. 2020. Accessed: Dec. 28, 2024. [Online]. Available: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Decreto/D9637.htm

[36] CNCS, “Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança v1.1,” Dec. 2022, Accessed: Dec. 31, 2024. [Online]. Available: https://www.cncs.gov.pt/docs/guia-de-gestao-dos-riscos11.pdf

[37] “Cibersegurança no setor bancário é crítica para a confiança - TV Europa.” Accessed: Jan. 05, 2025. [Online]. Available: https://www.tveuropa.pt/noticias/ciberseguranca-no-setor-bancario-e-critica-para-a-confianca/?utm_source=chatgpt.com

[38] “Cibersegurança - Banca - ABM | Axians PT.” Accessed: Jan. 05, 2025. [Online]. Available: https://www.axians.pt/cybersecurity/banking/?utm_source=chatgpt.com

[39] “Tenchi | Third-Party Cyber Risk Reduction.” Accessed: Jan. 05, 2025. [Online]. Available: https://www.tenchisecurity.com/br/insights-news/desafios-e-recomendacoes-na-gestao-de-risco-de-terceiros-no-setor-bancario-e-financeiro?utm_source=chatgpt.com

[40] “10 Casos de Uso de Inteligência Artificial na Segurança Cibernética - Data Science Academy.” Accessed: Aug. 18, 2025. [Online]. Available: https://blog.dsacademy.com.br/10-casos-de-uso-de-inteligencia-artificial-na-seguranca-cibernetica/

[41] M. Flinders, I. Smalley, and J. Schneider, “Detecção de fraudes com IA no setor bancário.” Accessed: Aug. 18, 2025. [Online]. Available: https://www.ibm.com/br-pt/think/topics/ai-fraud-detection-in-banking

[42] “Regime Juridico Segurança Ciberespaço,” Diário da República. Accessed: Feb. 05, 2025. [Online]. Available: https://www.cncs.gov.pt/docs/regime-jurdico-da-segurana-do-ciberespao.pdf

[43] J. C. Crisanto and J. Prenio, “Emerging Prudential Approaches to Enhance Banks’ Cyber Resilience,” in *The Palgrave Handbook of FinTech and Blockchain*, M. Pompella and R. Matousek, Eds., Cham: Springer International Publishing, 2021, pp. 285–306. doi: 10.1007/978-3-030-66433-6_13.

[44] A. Augusto and R. Carvalho, “A Importância das Informações para a Segurança no Ciberespaço,” Técnico Lisboa, 2021. Accessed: Feb. 12, 2025. [Online]. Available: https://fenix.tecnico.ulisboa.pt/downloadFile/1126295043839208/Tese%20de%20Mestrado%20Antonio%20Carvalho_A%20importanica%20das%20informacoes%20para%20a%20seguranca%20no%20ciberespaco_22012021.pdf

[45] S. Abu Sayeed, N. Kshetri, M. Mehedi Rahman, and S. Alam, “FSCsec: Collaboration in Financial Sector Cybersecurity-Exploring the Impact of Resource Sharing on IT Security”, doi: https://doi.org/10.48550/arXiv.2410.15194.

[46] “ISO/IEC 27001:2022(en), Information security, cybersecurity and privacy protection — Information security management systems — Requirements.” Accessed: Feb. 09, 2025. [Online]. Available: https://www.iso.org/obp/ui/en/#iso:std:iso-iec:27001:ed-3:v1:en

[47] “ISO/IEC 27035-1:2023 - Information technology — Information security incident management — Part 1: Principles and process.” Accessed: May 26, 2025. [Online]. Available: https://www.iso.org/standard/78973.html

[48] “REGULAMENTO
(UE) 2016/ 679 do Parlamento Europeu e do Conselho - de 27 de abril de 2016 - relat ivo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pes

soais e à livre circulação desses dados e que revoga a Diretiva 95/ 46/ CE (Regulament o Geral sobre a Proteção de Dados),” Apr. 2016. Accessed: Feb. 08, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/PL/TXT/PDF/?uri=CELEX:32016R0679

[49] “Diretiva - 2022/2555 - EN - EUR-Lex.” Accessed: Feb. 08, 2025. [Online]. Available: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32022L2555

[50] “Guidelines on ICT and security risk management | European Banking Authority.” Accessed: Feb. 09, 2025. [Online]. Available: https://www.eba.europa.eu/guidelines-ict-and-security-risk-management

[51] “Guidelines, Recommendations and Technical Standards.” Accessed: Feb. 09, 2025. [Online]. Available: https://www.esma.europa.eu/publications-and-data/guidelines-recommendations-and-technical-standards?

[52] “Decreto-Lei no 298/92 de 31 de Dezembro”, Accessed: Feb. 08, 2025. [Online]. Available: https://www.bportugal.pt/sites/default/files/anexos/legislacoes//dl298ano92.PDF

[53] “Temas Supervisão :: Elementos de Informação”, Accessed: Feb. 09, 2025. [Online]. Available: https://www.bportugal.pt/sites/default/files/anexos/instrucoes//396809213_1.docx.pdf

[54] R. Naydenov and M. Theocharidou, “EU Cybersegurity Iniciatives in the Finance Sector,” Mar. 2021. doi: 10.2824/15644.

[55] C. Calliess and A. Baumgarten, “Cybersecurity in the EU The Example of the Financial Sector: A Legal Perspective,” *German Law Journal*, vol. 21, no. 6, pp. 1149–1179, Sep. 2020, doi: 10.1017/glj.2020.67.

[56] K. Murphy, “Central Bank Digital Currency Data Use and Privacy Protection,” *Fintech Notes*, vol. 2024, no. 004, p. 1, Aug. 2024, doi: 10.5089/9798400286971.063.

[57] S. Wang, M. Asif, M. F. Shahzad, and M. Ashfaq, “Data privacy and cybersecurity challenges in the digital transformation of the banking sector,” *Comput Secur*, vol. 147, p. 104051, Dec. 2024, doi: 10.1016/j.cose.2024.104051.

[58] “Cibersegurança: as lições aprendidas ficam para quem as pratica.” Accessed: Feb. 08, 2025. [Online]. Available: https://dinheirovivo.dn.pt/opiniao/ciberseguranca-as-licoes-aprendidas-ficam-para-quem-as-pratica-17017961.html/?

[59] “Cibersegurança no setor financeiro | Deloitte Portugal.” Accessed: Feb. 08, 2025. [Online]. Available: https://www.deloitte.com/pt/pt/services/risk-advisory/perspectives/ciberseguranca-no-setor-financeiro.html?

[60] P. Chatzigiannis, C. Gu, S. Raghuraman, P. Rindal, and M. Zamani, “Privacy-Enhancing Technologies for Financial Data Sharing,” Mar. 2023, doi: https://doi.org/10.48550/arXiv.2306.10200.

[61] T. D. Wagner, K. Mahbub, E. Palomar, and A. E. Abdallah, “Cyber threat intelligence sharing: Survey and research directions,” *Comput Secur*, vol. 87, p. 101589, Nov. 2019, doi: 10.1016/j.cose.2019.101589.

[62] J. Ruohonen, K. Rindell, and S. Busetti, “From cyber security incident management to cyber security crisis management in the European Union,” *Comput Secur*, vol. 159, p. 104689, Dec. 2025, doi: 10.1016/j.cose.2025.104689.

[63] ESMA, “Final Report draft_RTS_and_ITS_on_incident,” 2024, Accessed: Aug. 28, 2025. [Online]. Available: https://www.esma.europa.eu/sites/default/files/2024-07/JC_2024-33_-_Final_report_on_the_draft_RTS_and_ITS_on_incident_reporting.pdf

[64] “Supervisão Bancária do BCE –Prioridades prudenciais a nível do MUS no período de 2023 a 2025.” Accessed: Feb. 08, 2025. [Online]. Available: https://www.bankingsupervision.europa.eu/framework/priorities/html/ssm.supervisory_priorities202212~3a1e609cf8.pt.html

[65] “Fórum com a Indústria para a Cibersegurança e Resiliência Operacional | Banco de Portugal.” Accessed: Feb. 06, 2025. [Online]. Available: https://www.bportugal.pt/page/forum-com-industria-para-ciberseguranca-e-resiliencia-operacional?

[66] C. Lambrinoudakis, S. Gritzalis, C. Xenakis, S. Katsikas, M. Karyda, and A. Tsochou, “Compendium of Risk Management Frameworks with potencial Interoperability,” Jan. 2022. doi: 10.2824/75906.

[67] “Os 5 Principais Frameworks de Cibersegurança para Proteger Ambientes Digitais.” Accessed: Feb. 09, 2025. [Online]. Available: https://www.dio.me/articles/os-5-principais-frameworks-de-ciberseguranca-para-proteger-ambientes-digitais?

[68] S. Paz, “Cybersecurity Standards and Frameworks,” in *IEEE Technology and Engineering Management Society Body of Knowledge (TEMSBOK)*, Wiley, 2023, pp. 397–416. doi: 10.1002/9781119987635.ch23.

[69] Crossmark, “The NIST Cybersecurity Framework (CSF) 2.0,” Feb. 2024. doi: 10.6028/NIST.CSWP.29.

[70] “COBIT | Control Objectives for Information Technologies | ISACA.” Accessed: Feb. 09, 2025. [Online]. Available: https://www.isaca.org/resources/cobit#1

[71] V. Stocchett, “A Roadmap to the CIS Critical Security Controls,” Nov. 2024. Accessed: Feb. 09, 2025. [Online]. Available: https://www.cisecurity.org/insights/white-papers/roadmap-cis-critical-security-controls

[72] “MITRE ATT&CK®.” Accessed: Feb. 09, 2025. [Online]. Available: https://attack.mitre.org/

[73] “Cyber resilience oversight expectations for financial market infrastructures Cyber resilience oversight expectations for financial market infrastructures-Contents,” 2018, Accessed: Feb. 09, 2025. [Online]. Available: https://www.ecb.europa.eu/paym/pdf/cons/cyberresilience/Cyber_resilience_oversight_expectations_for_financial_market_infrastructures.pdf

[74] C. on Payments, M. Infrastructures, and B. of the International Organization of Securities Commissions, “Committee on Payments and Market Infrastructures Board of the International

Organization of Securities Commissions Guidance on cyber resilience for financial market infrastructures," 2016, Accessed: Feb. 09, 2025. [Online]. Available: www.bis.org

[75] "Measuring and Managing Information Risk: A FAIR Approach - Jack Freund, Jack Jones - Google Books." Accessed: Feb. 09, 2025. [Online]. Available: https://books.google.pt/books?hl=en&lr=&id=oAR0AwAAQBAJ&oi=fnd&pg=PP1&ots=8m0qOwKCFg&sig=SfokvD2zwM_zlkuOERSkUTnmqmc&redir_esc=y#v=onepage&q&f=false

[76] "The Importance and Effectiveness of Cyber Risk Quantification." Accessed: Feb. 09, 2025. [Online]. Available: https://www.fairinstitute.org/what-is-fair

[77] C. Alberts, A. Dorofee, and J. Stevens, "Introduction to the OCTAVE ® Approach," 2003, Accessed: Feb. 09, 2025. [Online]. Available: https://www.itgovernance.co.uk/files/Octave.pdf

[78] "SEI Releases OCTAVE FORTE Model for Enterprise Risk Management." Accessed: Feb. 09, 2025. [Online]. Available: https://insights.sei.cmu.edu/news/sei-releases-octave-forte-model-for-enterprise-risk-management/

[79] "The STRIDE Threat Model | Microsoft Learn." Accessed: Feb. 09, 2025. [Online]. Available: https://learn.microsoft.com/en-us/previous-versions/commerce-server/ee823878(v=cs.20)?redirectedfrom=MSDN

[80] N. R. Mead, F. Shull, and K. Vemuru, "A Hybrid Threat Modeling Method," 2018, Accessed: Feb. 09, 2025. [Online]. Available: http://www.sei.cmu.edu

[81] "O tema da Cibersegurança", Accessed: Feb. 08, 2025. [Online]. Available: www.bportugal.pt

[82] T. Ongun *et al.*, "Collaborative Information Sharing for ML-Based Threat Detection," 2021, Accessed: Feb. 09, 2025. [Online]. Available: https://arxiv.org/abs/2104.11636

[83] "Banco de Portugal avança na cooperação para a cibersegurança | Banco de Portugal." Accessed: Jan. 05, 2025. [Online]. Available: https://www.bportugal.pt/comunicado/banco-de-portugal-avanca-na-cooperacao-para-ciberseguranca?

[84] C. Sauerwein, C. Sillaber, A. Mussmann, and R. Breu, "Threat Intelligence Sharing Platforms: An Exploratory Study of Software Vendors and Research Perspectives", Accessed: Mar. 29, 2025. [Online]. Available: https://www.wi2017.ch/images/wi2017-0188.pdf

[85] "Introduction to STIX." Accessed: Aug. 19, 2025. [Online]. Available: https://oasis-open.github.io/cti-documentation/stix/intro

[86] "Financial Services Information Sharing and Analysis Center." Accessed: Feb. 08, 2025. [Online]. Available: https://www.fsisac.com/

[87] "Incident reporting — CIRAS." Accessed: Feb. 09, 2025. [Online]. Available: https://ciras.enisa.europa.eu/

[88] "Nova iniciativa reúne as autoridades policiais e as maiores infraestruturas financeiras da Europa | Europol." Accessed: Sep. 28, 2025. [Online]. Available:

https://www.europol.europa.eu/media-press/newsroom/news/new-initiative-brings-together-law-enforcement-and-europe%E2%80%99s-largest-financial-infrastructures

[89] "Protecting the European financial sector: the Cyber Information and Intelligence Sharing Initiative." Accessed: Feb. 09, 2025. [Online]. Available: https://www.ecb.europa.eu/press/key/date/2020/html/ecb.sp200227~7aae128657.en.html?

[90] R. S. Teopisto, J. Lupi, and D. P. Duarte, "DORA." Accessed: Feb. 08, 2025. [Online]. Available: https://abreuadvogados.com/wp-content/uploads/2023/01/DORA.pdf

[91] CNCS, "Coordenação da resposta a incidentes." Accessed: Feb. 09, 2025. [Online]. Available: https://www.cncs.gov.pt/pt/certpt/coordenacao-da-resposta-a-incidentes/

[92] CNCS, "Taxonomia." Accessed: Aug. 30, 2025. [Online]. Available: https://www.cncs.gov.pt/pt/certpt/taxonomia/?

[93] "Taxonomia Comum da Rede Nacional de CSIRT Dezembro 2023", Accessed: Aug. 30, 2025. [Online]. Available: https://www.redecsirt.pt/files/RNCSIRT_Taxonomia_v3.3.pdf

[94] C. S. Johnson, M. L. Badger, D. A. Waltermire, J. Snyder, and C. Skorupka, "Guide to Cyber Threat Information Sharing," Gaithersburg, MD, Oct. 2016. doi: 10.6028/NIST.SP.800-150.

[95] "Challenges and Opportunities of Enabling Information Sharing," Jan. 2024. Accessed: Dec. 18, 2025. [Online]. Available: https://www.insaonline.org/docs/default-source/uploadedfiles/2024/insa_cyber_information_sharing.pdf

[96] N. Alexopoulos, E. Vasilomanolakis, S. Le Roux, S. Rowe, and M. Mühlhäuser, "TRIDEnT: Building Decentralized Incentives for Collaborative Security," May 2019, Accessed: Feb. 09, 2025. [Online]. Available: http://arxiv.org/abs/1905.03571

[97] R. Riesco, X. Larriva-Novo, and V. A. Villagra, "Cybersecurity threat intelligence knowledge exchange based on blockchain," *Telecommun Syst*, vol. 73, no. 2, pp. 259–288, Feb. 2020, doi: 10.1007/s11235-019-00613-4.

[98] "2020 Volume 6 Key Performance Indicators for Security Governance Part 1." Accessed: Sep. 28, 2025. [Online]. Available: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/key-performance-indicators-for-security-governance-part-1

[99] "12 principais métricas e KPIs de segurança cibernética que as empresas devem monitorar | Computer Weekly." Accessed: May 03, 2025. [Online]. Available: https://www.computerweekly.com/br/tip/12-principais-metricas-e-KPIs-de-seguranca-cibernetica-que-as-empresas-devem-monitorar?

[100] "CMMI Cybermaturity Platform | ISACA." Accessed: May 03, 2025. [Online]. Available: https://www.isaca.org/enterprise/cmmi-cybermaturity-platform

[101] A. A. Darem, A. A. Alhashmi, T. M. Alkhaldi, A. M. Alashjaee, S. M. Alanazi, and S. A. Ebad, "Cyber Threats Classifications and Countermeasures in Banking and Financial Sector," *IEEE Access*, vol. 11, pp. 125138–125158, 2023, doi: 10.1109/ACCESS.2023.3327016.

[102] K. Anastasakis and A. Rashid, “Towards Linking Indicators of Compromise to Operational Resilience and Safety Requirements,” in *Proceedings of the Sixth Workshop on CPS&IoT Security and Privacy*, New York, NY, USA: ACM, Nov. 2024, pp. 104–110. doi: 10.1145/3690134.3694827.

[103] ENISA, “EU-Cybersecurity EU-level insights and next steps,” 2024. doi: 10.2824/7714867.

[104] A. Drougkas, U. Komzaite, E. Philippou, P. Abe, G. François, and E. Maaskant, “NIS Investments, Cybersegurity Policy Assessment,” Nov. 2024. doi: 10.2824/5220134.

[105] U. Flick, “Uma Introdução à Pesquisa Qualitativa, 2a ed. Porto Alegre, Artmed.” Accessed: Sep. 24, 2025. [Online]. Available: https://ia800103.us.archive.org/34/items/ParaCompreenderACiencia/3.%20FLICK%2C%20UWE.%20Introdu%C3%A7%C3%A3o%20%C3%A0%20pesquisa%20qualitativa.pdf

[106] B. G. Glaser and A. L. Strauss, “The Discovery of Grounded Theory: Strategies for Qualitative Research. Chicago, IL, USA,” Aldine Publishing Company. Accessed: Sep. 23, 2025. [Online]. Available: http://www.sxf.uevora.pt/wp-content/uploads/2013/03/Glaser_1967.pdf

[107] C. Robson and McCartan Kieran, “A Resource for Social Scientists and Practitioner-Researchers, 2nd ed. Oxford: Blackwell.” Accessed: Sep. 24, 2025. [Online]. Available: https://www.academia.edu/86033008/Real_World_Research

[108] M. LÜDKE and M. ANDRÉ, “E. D. A. Pesquisa em educação: abordagens qualitativas.” Accessed: Sep. 24, 2025. [Online]. Available: https://www.academia.edu/43066896/Pesquisa_em_Educa%C3%A7%C3%A3o_Abordagens_Qualitativas_vf

[109] Lessa De Oliveira; and Cristiano, “Um Apanhado Teórico - Conceptual sobre a Pesquisa Qualitativa: Tipos, Técnicas e Características,” vol. 2, núm. 3, 2008, Accessed: Mar. 09, 2025. [Online]. Available: https://www.redalyc.org/articulo.oa?id=702078545001

[110] D. MOREIRA, “ O método fenomenológico na pesquisa. São Paulo: Pioneira Thomson.” Accessed: Sep. 24, 2025. [Online]. Available: https://toaz.info/doc-view-3

[111] D. L. Morgan, “Focus Groups,” *Annu Rev Sociol*, vol. 22, no. 1, pp. 129–152, Aug. 1996, doi: 10.1146/annurev.soc.22.1.129.

[112] D. Morgan, *Focus Groups as Qualitative Research*. 2455 Teller Road, Thousand Oaks California 91320 United States of America : SAGE Publications, Inc., 1997. doi: 10.4135/9781412984287.

[113] A. Strauss and J. Corbin, “Basics of qualitative research : grounded theory procedures and techniques : Strauss, Anselm L : Free Download, Borrow, and Streaming : Internet Archive.” Accessed: Apr. 20, 2025. [Online]. Available: https://archive.org/details/basicsofqualitat0000stra/page/n5/mode/2up

[114] S. Rädiker and U. Kuckartz, *Focused Analysis of Qualitative Interviews with MAXQDA*. MAXQDA Press, 2020. doi: 10.36192/978-3-948768072.

[115] J. Corbin and A. Strauss, *Basics of Qualitative Research (3rd ed.): Techniques and Procedures for Developing Grounded Theory*. 2455 Teller Road, Thousand Oaks California 91320 United States : SAGE Publications, Inc., 2008. doi: 10.4135/9781452230153.

[116] R. S. Santos, C. Pimenta do Vale, B. Bogoni, and P. H. Kirkegaard, "Abordagem, projeto e métodos de investigação qualitativa em contexto educacional," in *New Trends in Qualitative Research*, vol. 7, Ludomedia, 2021, pp. 181–189. doi: 10.36367/ntqr.7.2021.181-189.

[117] Z. M. M. B. Alves and M. H. G. F. D. da Silva, "Análise qualitativa de dados de entrevista: uma proposta," *Paidéia (Ribeirão Preto)*, no. 2, pp. 61–69, Jul. 1992, doi: 10.1590/S0103-863X1992000200007.

[118] "MAXQDA em Português." Accessed: May 26, 2025. [Online]. Available: https://www.maxqda.com/pt?

[119] "Bryman: Social Research Methods, 4 th edition," Oxford University Press. Accessed: Jul. 27, 2025. [Online]. Available: https://inee.org/sites/default/files/resources/Bryman__A._2012_Social_research_methods.pdf?

[120] "Inteligência artificial no setor bancário: aplicações e chaves para adotá-la - Stefanini Brasil." Accessed: Sep. 27, 2025. [Online]. Available: https://stefanini.com/pt-br/insights/inteligencia-artificial-no-setor-bancario-aplicacoes

Apêndices

Apêndice A - Processo de Seleção de Palavras-Chave no Web of Science

Tabela 6.1 – Processo de Seleção de Palavras-Chave no Web of Science

Conceitos	População	Critérios Inclusão
Cybersecurity	Banking Sector	Palavaras Chave, no Título e Resumo
Risk Management	Banking Risk Legal Standards	Data: > 2019
Cyber Security Metrics	Risk management metrics for banking	Lingua : Português e Inglês
Cybersecurity risk phases	Information sharing in banking	Tipo Documento: Artigo Revisão, Artigo Conferência
CyberSecurity Metrics		Tipo de Fonte: Journal
Risk Management		Acesso Aberto
Risk Management Metrics		Area Pesquisa: Business, Economic, Finance, Sistemas de Informação
Risk Management Framework		
Cyber Threat Intelligence		
66763 documentos		
	27.951 documentos	
		43 documentos

Apêndice B - Processo de Seleção de Palavras-Chave no SCOPUS

Tabela 6.2 – Processo de Seleção de Palavras-Chave no SCOPUS

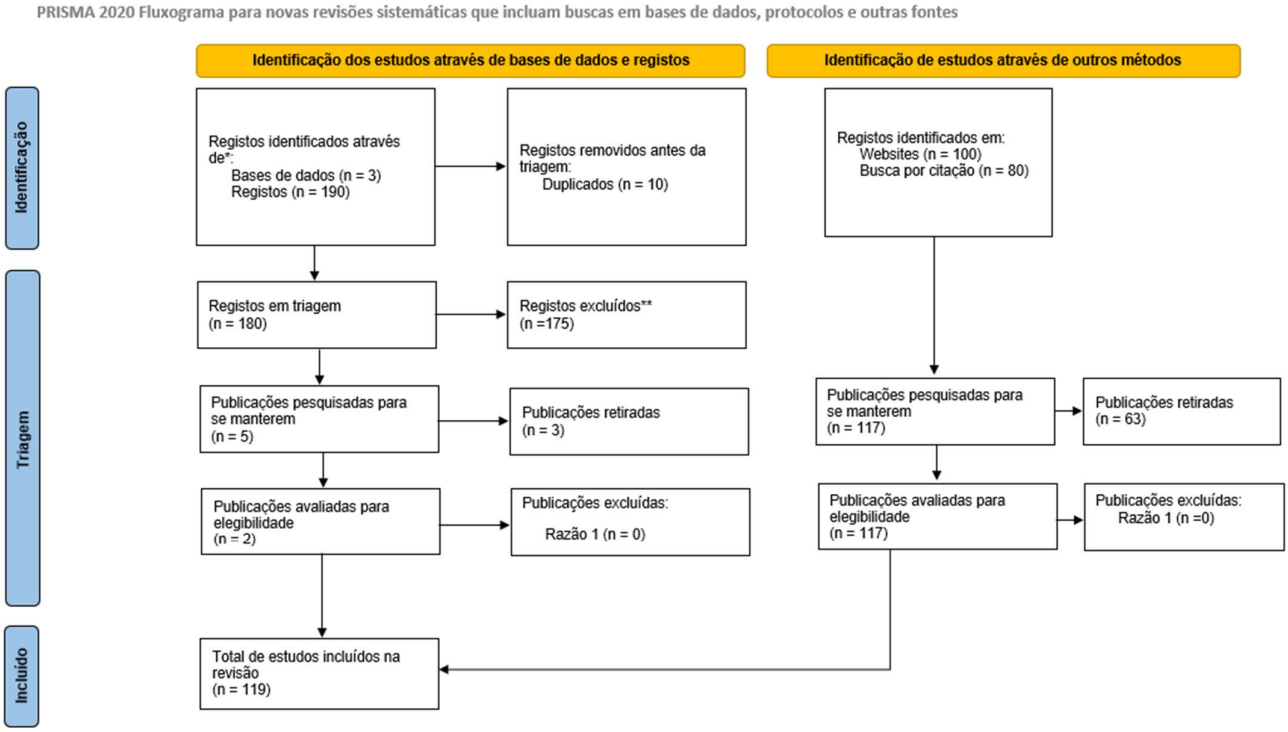
Conceitos	População	Critérios Inclusão
Cybersecurity	Banking Sector	Palavaras Chave, no Título e Resumo
	Banking Risk Legal Standards	Data: > 2019
Cyber Security Metrics	Risk management metrics for banking	Lingua : Português e Inglês
Cybersecurity risk phases	Information sharing in banking	Tipo Documento: Artigo Revisão, Artigo Conferência
CyberSecurity Metrics		Tipo de Fonte: Journal
		Acesso Aberto
Risk Management Metrics		Area Pesquisa: Business, Economic, Finance, Sistemas de Informação
Risk Management Framework		
Cyber Threat Intelligence		
206917 documentos		
	653 documentos	
		100 documentos

Apêndice C - Processo de Seleção de Palavras-Chave no EBSCO

Tabela 6.3 – Processo de Seleção de Palavras-Chave no EBSCO

Conceitos	População	Critérios Inclusão
Cybersecurity	Banking Sector	Palavaras Chave, no Título e Resumo
	Banking Risk Legal Standards	Data: > 2019
Cyber Security Metrics	Risk management metrics for banking	Lingua : Português e Inglês
Cybersecurity risk phases	Information sharing in banking	Tipo Documento: Artigo Revisão, Artigo Conferência
CyberSecurity Metrics		Tipo de Fonte: Journal
		Acesso Aberto
Risk Management Metrics		Area Pesquisa: Business, Economic, Finance, Sistemas de Informação
Risk Management Framework		
Cyber Threat Intelligence		
125541 documentos		
	349 documentos	
		47 documentos

Apêndice D – PRISMA



Traduzido por: Verónica Abreu, Sónia Gonçalves-Lopes*, José Luís Sousa* e Verónica Oliveira / *ESS Jean Piaget - Vila Nova de Gaia - Portugal*
de: Page MJ, McKenzie JE, Bossuyt PM, Boutron I, Hoffmann TC, Mulrow CD, et al. The PRISMA 2020 statement: an updated guideline for reporting systematic reviews. BMJ 2021;372:n71. doi: 10.1136/bmj.n71

Figura 6.1 – PRISMA

Apêndice E - Níveis de maturidade CMMI

Nível 1 – *Initial*

Processos são *ad-hoc* e caóticos.

A organização reage a incidentes, mas não tem práticas consistentes.

Pouca ou nenhuma documentação ou repetibilidade.

Nível 2 – *Managed*

Processos são planeados e executados de forma controlada.

Existe documentação básica, mas ainda limitada.

A organização começa a monitorizar e medir resultados.

Nível 3 – *Defined*

Processos são padronizados e documentados em toda a organização.

Existe formação, comunicação e alinhamento organizacional.

A cibersegurança é integrada na estratégia empresarial.

Nível 4 –*Quantitatively Managed*

A organização usa métricas e KPIs para gerir e melhorar processos.

A análise de dados orienta decisões de segurança.

Existe previsibilidade e controlo estatístico.

Nível 5 –*Optimizing*

Foco na melhoria contínua com base em feedback e inovação.

A organização é proativa, antecipando ameaças e adaptando-se rapidamente.

A cibersegurança é uma vantagem competitiva.

Apêndice F - Níveis de maturidade com base nas recomendações do NIST

Nível 1 – Inicial

A organização realiza partilhas de forma *ad-hoc*, sem processos definidos ou objetivos claros. A informação é ocasionalmente recebida ou enviada, mas sem integração sistemática.

Nível 2 – Básico

Existem processos básicos de partilha com parceiros selecionados. A organização começa a definir critérios para o tipo de informação partilhada e os canais utilizados.

Nível 3 – Intermédio

A partilha de informação é estruturada e regular. A organização participa em comunidades formais (ex. ISACs ou CIISI-EU), com políticas internas que regulam o fluxo de dados e a proteção da confidencialidade.

Nível 4 – Avançado

A organização integra a partilha de informação nos seus processos de gestão de risco e resposta a incidentes. Utiliza ferramentas automatizadas para recolha, análise e disseminação de inteligência cibernética.

Nível 5 – Otimizado

A partilha é proativa, colaborativa e estratégica. A organização contribui ativamente para ecossistemas de cibersegurança, influenciando padrões e políticas, e utiliza métricas para avaliar o impacto da partilha na sua postura de segurança.

Apêndice G – Questões Entrevistas

Entrevista Individual

1- Que idade tem?
2- Em quantas instituições do setor bancário já trabalhou?
3- Quantos anos tem de experiência no setor bancário?
4- Qual o cargo que tem na empresa? Qual a dimensão da sua equipa?
5- Qual a função na área de segurança de Informação? (Tabela 4)
6- Que funções ligadas à área de Cibersegurança existem na sua empresa? (Tabela4)
7- Quantos anos de experiência tem na área da cibersegurança?
8- Tem alguma certificação profissional ou académica na área da cibersegurança?
9- Como descreve a abordagem atual à gestão de risco em cibersegurança no setor bancário em geral? E na sua instituição?
10- Na sua opinião, quais os principais desafios ou lacunas existentes?
11- Que fatores, atores ou instrumentos considera mais relevantes para influenciar positivamente a gestão do risco de cibersegurança no setor bancário?
12- Existem boas práticas ou lições aprendidas noutros setores que possam ser aplicadas?
13- Que iniciativas de colaboração entre agentes do setor bancário conhece neste domínio?
14- Que melhorias considera essenciais para reforçar a cooperação na gestão do risco de cibersegurança?
15- Como funciona a articulação da partilha de informação entre a ENISA, FISAC, BCE, CERT-EU, CIISI-EU, FS-ISAC? Existem mais entidades a partilhar informação?
16- Que tipos de informação sobre cibersegurança considera mais relevantes para serem partilhados entre instituições do setor bancário?
17- E em que fases da cibersegurança (prevenção, deteção, resposta ou recuperação) essa informação é mais útil?
18- Que tipo de informação é considerada mais sensível ou crítica para partilhar, e porquê?
19- Que valor atribui à informação partilhada em cibersegurança?
20- Quem são os principais interessados e qual o racional que deve orientar essa partilha?
21- Está familiarizado com os objetos definidos no modelo STIX (ex: Indicator, Malware, Threat Actor)?
22- Quais destes objetos são mais utilizados ou relevantes na partilha de informação?
23- Que tipo de indicadores de compromisso (IoCs) costumam partilhar?
24- A sua instituição partilha informação nas diferentes fases de um incidente (prevenção,

deteção, resposta e recuperação) com outras entidades bancárias ou apenas com autoridades de controlo?

25- Que plataformas, normas, ferramentas, processos a sua instituição usa (v.g.: CIISI-PT, ISACs, FICRO) para a partilha de informação? (Tabela1)

26- Qual é o grau de adesão e participação das entidades bancárias?

27- Que tipo de informação é partilhada nestas plataformas?

28- Existem normas, taxonomias ou critérios específicos para a gestão e acesso à informação?

29- A informação é partilhada com outras entidades (outros bancos, Banco de Portugal, centro nacional de cibersegurança).

30- Como é feito o acesso, atualização e gestão da informação nas plataformas de partilha?

31- Existe integração com o sistema de informação interno e com as plataformas de gestão de cibersegurança (por ex: SIEM - *Security Information and Event Management* e CIISI-PT)?

32- Na sua opinião, qual o nível de compreensão e mobilização que a sua instituição tem em relação aos riscos de cibersegurança, nomeadamente, ameaças, vulnerabilidades e potencial impacto dos ciber-incidentes?

33- A sua instituição adota frameworks ou certificações como Information Security Management System (ISMS)? Se sim, quais? (Tabela 2) e o setor bancário em geral?

34- Como classificaria o nível de maturidade da sua instituição na partilha de informação e na gestão de risco em cibersegurança? (Tabela 3) E o restante setor bancário?

35- A sua instituição utiliza métricas (KPIs) para avaliar a gestão do risco em cibersegurança e atividades de *Cyber Threat Intelligence* (CTI)?

36- Quais são os principais indicadores utilizados?

37- Existem métricas ou escalas usadas para medir recursos, competências, políticas, tecnologias e sensibilização na área da cibersegurança?

38- Como é avaliada, por exemplo, a maturidade dos processos, a existência de papéis definidos ou o funcionamento do SOC?

39- Que ferramentas e métricas de CTI são usadas pela equipa do SOC?

40- A equipa de SOC partilha informações e métricas sobre ciberameaças? Se sim, com quem?

41- É feito algum tipo de medição sobre o grau de integração entre as atividades de cibersegurança e as de CTI, nomeadamente nas fases de prevenção, deteção, resposta e recuperação de incidentes?

42- Que métricas ou indicadores são usados (ou seriam relevantes) para avaliar a eficácia e frequência da partilha de informação sobre cibersegurança com outras instituições ou entidades de controlo?

43- Na sua opinião, o custo estimado de não ter acesso à informação partilhada pode ou deve ser

considerado uma métrica relevante?

44- De que forma esse impacto pode ser avaliado?

45- Na sua opinião, por que a partilha de informação sobre cibersegurança ainda é limitada no setor bancário? Se sim, que fatores legais, regulamentares, normativos, técnico, concorrenciais, culturais, segurança dos dados partilhados, mais contribuem para essa limitação?

46- Que soluções concretas propõe para ultrapassar as barreiras à partilha de informação em cibersegurança no setor bancário?

47- Que práticas seriam beneficiadas se essas barreiras fossem ultrapassadas?

48- Que tipos de incentivos (regulatórios, económicos, reputacionais, tecnológicos) poderiam ser implementados para promover a partilha de informação entre instituições?

49- Como avalia o impacto que esses incentivos teriam na cibersegurança das instituições individualmente e no setor bancário como um todo?

50- Poderão os bancos beneficiar financeiramente ou estrategicamente com essa colaboração?

51- Quais são, na sua opinião, os principais recursos, competências e capacidades essenciais para que a partilha de informação em cibersegurança funcione de forma eficaz entre instituições do setor financeiro?

52- Conhece modelos internacionais de partilha de informação que poderiam ser adaptados e adotados no contexto do setor bancário português?

53- Conhece algum plano Estratégico definido pelo BP para a partilha de Informação em Cibersegurança? Se sim, quais os aspetos que considera mais relevantes do plano? Quais os mais realistas/viáveis e inviáveis?

54- Há alguma outra questão relevante sobre partilha de informação em cibersegurança que não foi abordada? Gostaria de sugerir algo mais para a investigação?

Apêndice H – Regras Entrevistas

Foi solicitado o parecer da Comissão de Ética da ISTA/ISCTE para a elaboração das entrevistas. Para o parecer foram entregues os seguintes documentos:

- FormularioComissaoEtica;
- Debriefing_CE_ISTA;
- ConsentimentoInformado_DadosPessoais_CE_ISTA;
- TermoResponsabilidadeConfindencialidade_CE_ISTA;
- TratamentoDadosPessoais_Questionario_CE_ISTA;
- Guião das Entrevistas.

Apêndice I - Excertos dos Discursos dos Participantes

Excerto 1: Barreiras

"Na banca a partilha não é fácil, devido a serem muito fechados" (E_05)

"(…) tudo o que tem a ver com partilha não é fácil de ser feito de forma natural" (E_09)

"Se partilhar ajudo os outros a evoluir e passo a ter problemas concorrenciais" (E_02)

Excerto 2: Partilha PT

"há muito tempo que fazemos partilha entre os bancos de forma informal" (E_03).

"Fazem-se partilhas ao nível do CIISI-PT que é uma plataforma MISP e tem algumas taxinomias para a informação a partilhar, mas na prática não se partilha" (E_04)

Excerto 3: Não Partilha

"poderia ser deselegante em termos de mercado que é partilharem experiências sobre soluções que tenham sido implementadas ao nível das organizações" (E_01)

Excerto 4: Cibercrime

"(…) a cibersegurança é a outra face da moeda no combate ao cibercrime. Num documento que todos os Cibercentros da Europa têm, que a ENISA tem, que a Europol tem, que a Interpol tem, que a judiciária tem, chamado de taxonomia. Temos uma taxonomia que será talvez a mais rigorosa e a mais abrangente no site da Europol. Estas taxonomias quando são vistas, quando são analisadas, não há dúvida nenhuma que 90% dos eventos que lá vêm descritos correspondem a cibercrime" (E_17).

Excerto 5: Colaboração

"Cultural, tem o peso maior, pois vamos utilizar a justificação concorrencial e regulamentar para não fazer partilha. Tem de ser o regulador a puxar para mudar a cultura, e tem de ser top down, (…) a missão do BP é zelar pela estabilidade do sistema financeiro português (…)" (E_16)

"Banco de Portugal podia ajudar com algumas instruções de trabalho mais específicas" (E_17)

Excerto 6: Dados a Partilhar

"Perceber quais é que são os alvos, agentes de ameaça que estão mais ativos e se são para determinadas entidades bancárias e com que especificidades. Um ator que ataca um banco que é muito forte em B2C não é o mesmo que ataca um banco que é mais virado para ver B2B, os TTP, IoA que estão a ser utilizados, controlos que estão implementados, que eram supostos prevenir aqueles tipos de ataques que foram ineficazes, e porque é que foram ineficazes. O objetivo é esta informação, ser consumida pelas outras entidades para conseguirem afinar os seus controlos, porque muitas vezes pode haver um ator que se especializou em fazer by pass a um DF muito famoso ao crowd strike, e assim já se sabe que quem tiver o crowd strike tem de alterar as configurações. Mas de facto o uso de indicadores de ataque e os indicadores de exposição são os as informações mais importantes a serem partilhadas" (E_08)

Excerto 7: Incentivos a Partilha de Informação

"Não acho uma boa ideia, para funcionar bem teria de ser regulatório. Mas as pessoas deviam partilhar espontaneamente sem ter de existir qualquer incentivo" (E_12)

"as pessoas têm de sentir isto como sendo um benefício" (E_11)

Excerto 8: Incentivos

"a legislação tem trazido incentivos negativos, baseados na contraordenação, na sanção. Devia existir mais incentivos positivos, pelo elogio, pela demonstração, conferências, seminários para explicar os benefícios da partilha. E o melhor incentivo era de cima para baixo, vir do regulador" (E_17)

Apêndice J – *Frameworks*, Normas, Guias, Boas Práticas, Protocolos, Modelos, Procedimentos, Plataformas, Ferramentas e Ciclos

Breve explicação das *Frameworks*, Normas, Guias e Boas Práticas, Protocolos, Modelos, Procedimentos, Plataformas, Ferramentas e Ciclos

Frameworks

- *NIST Cybersecurity Framework* → *Framework* de cibersegurança para gestão de riscos;
- MITRE ATT&CK → *Framework* de conhecimento sobre táticas e técnicas de adversários;
- CIS *Controls* (v8) → *Framework* de boas práticas em segurança da informação;
- SWIFT *Customer Security Controls Framework* (CSCF) → *Framework* de controlos de segurança;
- COBIT 2019 → *Framework* de governo e gestão de TI.

Normas

- ISO/IEC 27001 / 27002 → Normas internacionais de gestão da segurança da informação;
- ISO/IEC 27010 → Norma para comunicação e troca de informações seguras entre organizações;
- ISO/IEC 27035 → Norma para gestão de incidentes de segurança.

Guias e Boas Práticas

- ENISA *Threat Intelligence Sharing Guide* → Guia da ENISA para partilha de inteligência de ameaças;
- *Information Technology Infrastructure Library* (ITIL 4) → Conjunto de boas práticas para gestão de serviços de TI;
- NIST SP 800-150 → Guia para partilha de informação de ameaças;
- NIST SP 800-35 → Guia de migração tecnológica;
- NIST SP 800-53 → Controlo de segurança e privacidade.

Protocolos/Modelos/Procedimentos

- *Traffic Light Protocol* (TLP) → Protocolo de classificação e partilha de informação sensível;
- TAXII → Protocolo para troca automatizada de CTI;
- *Vocabulary for Event Recording and Incident Sharing* (VERIS) → Modelo para registo e partilha de incidentes;

- STIX → Linguagem padrão para partilha de CTI;
- *Non-Disclosure Agreements* (NDAs) → Acordos de confidencialidade;
- Escalonamento → Procedimento de encaminhamento de incidentes;
- Anonimização → Técnica para proteger identidade de fontes/dados;
- Planos de resposta → Conjunto de ações a executar perante incidentes.

Plataformas/Ferramentas

- MISP → Plataforma *open-source* para partilha de indicadores de ameaça;
- TheHive → Plataforma para gestão de incidentes;
- OpenCTI → Plataforma *open-source* para gestão de inteligência de ameaças;
- ThreatConnect, IBM X-Force, Anomali, AlienVault OTX → Plataformas comerciais/de comunidade para *Threat Intelligence*;
- CIISI-PT → Centro de partilha de informação de cibersegurança em PT;
- CTM360 → Plataforma consolidada de proteção contra riscos digitais
- FS-ISAC → Centros de Análise e Partilha de Informação.

Ciclos de CTI

- Ciclo de CTI → Deteção → Validação → Classificação → Anonimização → Partilha → Resposta coordenada.

O Ciclo de CTI, é o processo estruturado que orienta a forma como a inteligência de ciberameaças é recolhida, analisada, partilhada e utilizada. Serve para garantir que a informação sobre ameaças é útil, validada e acionável, ajudando na tomada de decisão e na resposta a incidentes.

Fases típicas do ciclo de CTI:

- Planeamento e Direção
    - Definição de objetivos, que tipo de ameaças queremos monitorizar.
    - Identificação de necessidades de inteligência (por exemplo, ataques a bancos, *ransomware, phishing*).
- Recolha
    - Obtenção de dados de diferentes fontes, logs de SIEM, *feeds* de CTI, *honeypots*, MISP, OSINT, ISACs.
- Processamento
    - Normalização, filtragem e organização dos dados (v.g.: converter indicadores para formatos como STIX/TAXII).

- Análise
    - Transformação dos dados em inteligência acionável (v.g.: identificar padrões, atribuir ameaças a grupos conhecidos, prever movimentos de atacantes).
- Disseminação / Partilha
    - Distribuição da inteligência para as equipas certas: SOC, gestão de risco, outras organizações (via TLP, ISACs, CIISI-PT).
- Feedback / Lições Aprendidas
    - Avaliar se a inteligência foi útil.
    - Ajustar necessidades e reiniciar o ciclo.

Anexos

Anexo A – Conceitos de Segurança e suas relações

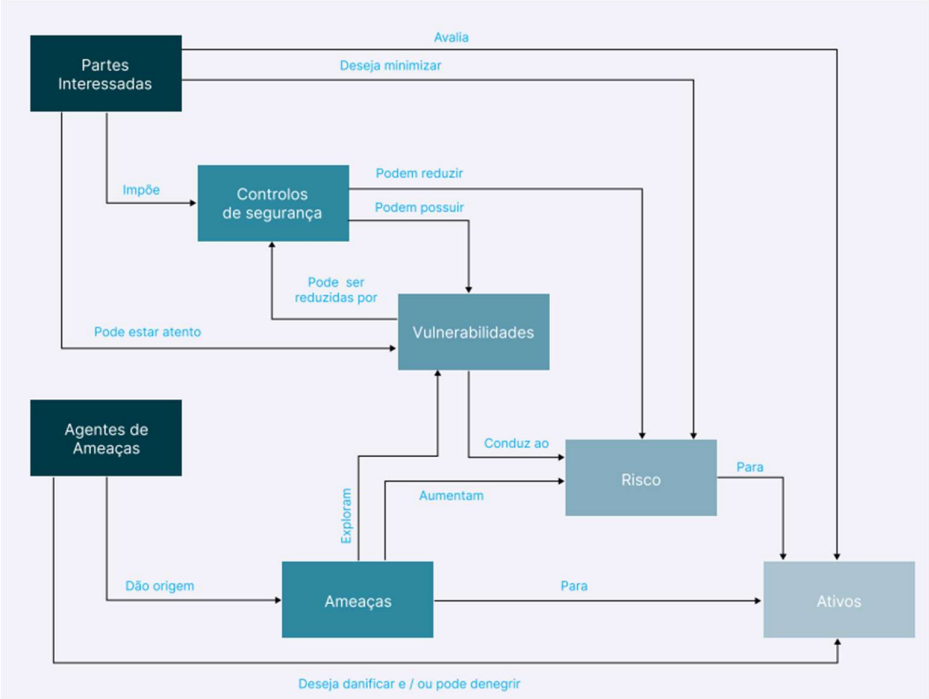


Figura 7.1 – Conceitos de segurança e as suas relações; Fonte:CNCS, adaptação da Norma ISO/ IEC

Anexo B – Processo Gestão de Risco

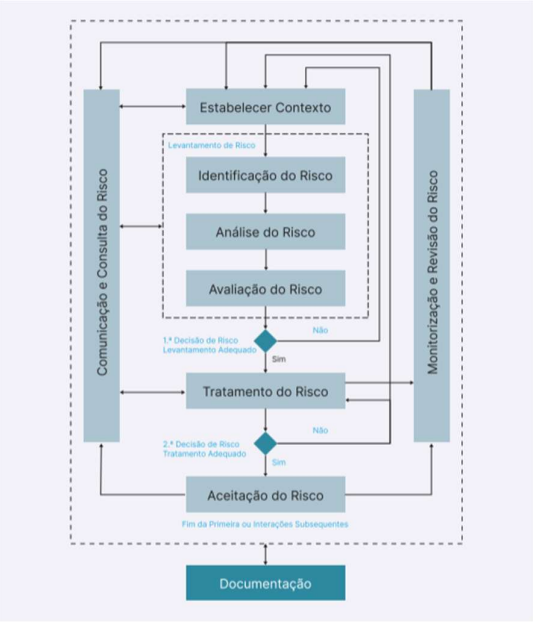


Figura 7.2 – Processo Gestão de Risco; Fonte: ISO/IEC 27500

Anexo C – Objetivos de Segurança

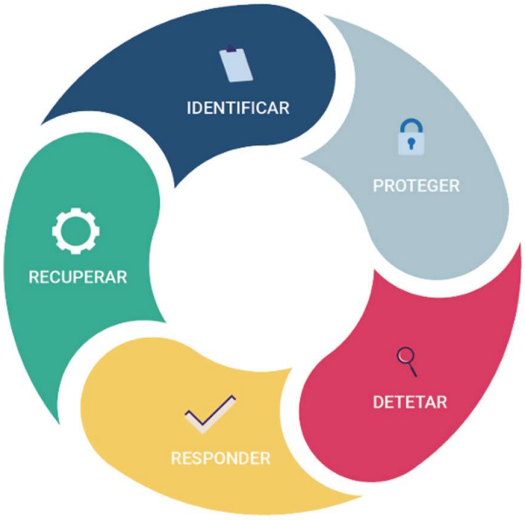


Figura 7.3 – Objetivos de Segurança, Fonte: QNRCS

Anexo D – Arquitetura STIX

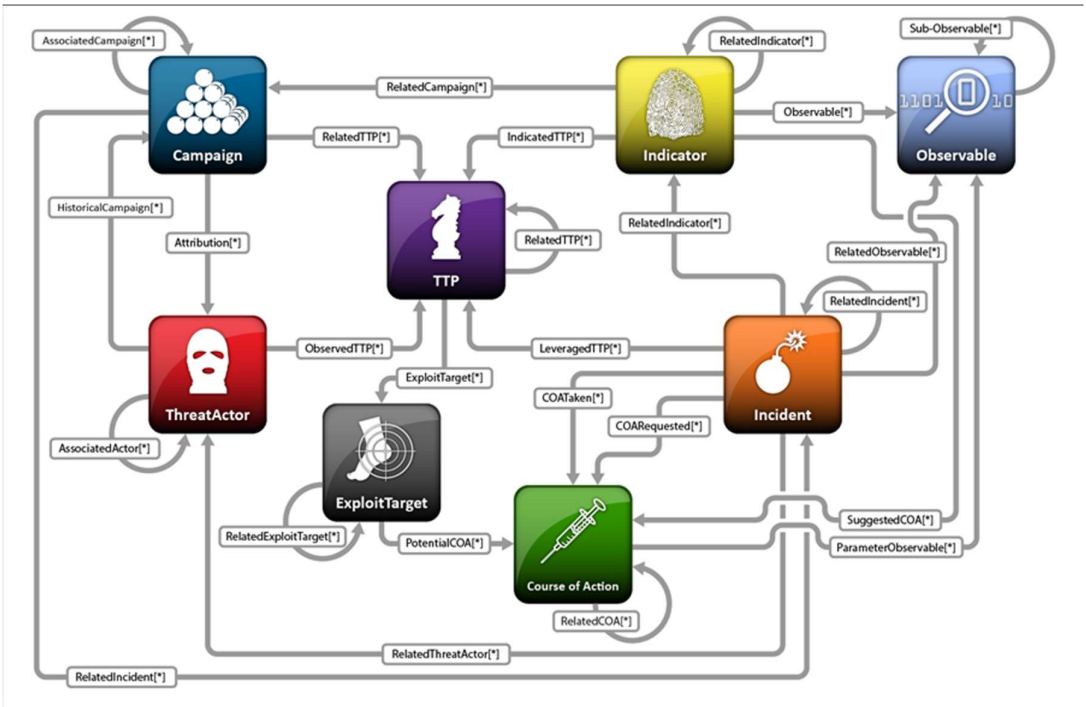


Figura 7.4 – Arquitetura STIX. Fonte: MITRE

Anexo E – Taxonomia CNCS

Classe Incidente	Tipo Incidente
Código Malicioso	Sistema Infetado
	Distribuição de Malware
	Servidor C2
	Configuração de Malware
Disponibilidade	Negação de Serviço
	Negação de Serviço Distribuída
	Configuração incorreta
	Sabotagem
	Interrupção
Recolha de Informação	Scanning
	Sniffing
	Engenharia Social
Intrusão	Comprometimento de Conta Privilegiada
	Comprometimento de Conta Não Privilegiada
	Comprometimento de Aplicação
	Comprometimento de Sistema
	Arrombamento
Tentativa de Intrusão	Exploração de Vulnerabilidade
	Tentativa de Login
	Nova assinatura de ataque
Segurança da Informação	Acesso não autorizado
	Modificação não autorizada
	Perda de dados
	Exfiltração de Informação
Fraude	Utilização indevida ou não autorizada de recursos
	Direitos de autor
	Utilização ilegítima de nome de terceiros
	Phishing
Conteúdo Abusivo	SPAM
	Discurso Nocivo
	Exploração sexual de menores, racismo e apologia da violência
Vulnerabilidade	Criptografia fraca
	Amplificador DDoS
	Serviços acessíveis potencialmente indesejados
	Revelação de informação
	Sistema vulnerável
Outro	Sem tipo
	Indeterminado

Figura 7.5 – Taxonomia CNCS