INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Modelo de Cibersegurança Direcionado para o Setor Bancário, Baseado nas Boas Práticas dos Principais Quadros de Referência

Tiago Miguel Ramalho Batista

Mestrado em Informática e Gestão

Orientador:
Doutor Carlos José Corredoura Serrão, Professor Associado,
Iscte – Instituto Universitário de Lisboa

Setembro, 2025

Departamento de Ciências e Tecnologias de Informação

Modelo de Cibersegurança Direcionado para o Setor Bancário, Baseado nas Boas Práticas dos Principais Quadros de Referência

Tiago Miguel Ramalho Batista

Mestrado em Informática e Gestão

Orientador:
Doutor Carlos José Corredoura Serrão, Professor Associado,
Iscte – Instituto Universitário de Lisboa

Setembro, 2025

Agradecimentos

A realização desta dissertação só foi possível graças ao incentivo e apoio de todos os que me são mais próximos, à minha família, amigos e companheira, a quem expresso o meu mais profundo agradecimento.

Gostaria também de agradecer ao meu orientador, Carlos Serrão, pela disponibilidade, bem como pelas enriquecedoras sugestões e análises, que permitiram elevar a qualidade do trabalho desenvolvido.

Agradeço também aos especialistas que aceitaram participar nas entrevistas, disponibilizando o seu precioso tempo, partilhando o seu conhecimento, sem os quais a validação do modelo não teria sido possível.

Resumo

O crescente refinamento das ameaças cibernéticas representa atualmente um dos maiores desafios para o setor bancário, particularmente para as instituições bancárias, dada a criticidade dos ativos que tratam.

Este trabalho centra-se no desenvolvimento de um modelo robusto de práticas e configurações de cibersegurança, com o objetivo de reforçar a resiliência cibernética no setor bancário.

A investigação tem por base a Revisão Sistemática da Literatura (RSL) e a análise comparativa de modelos de referência reconhecidos internacionalmente, utilizando a *National Institute of Standards and Technology (NIST) - Cybersecurity Framework (CSF)* como alicerce do mo- delo e apoiando o mesmo com a *Center for Internet Security* (CIS), *Payment Card Industry - Data Security Standard (PCI-DSS)* e *Society for Worldwide Interbank Financial Telecommuni- cation (SWIFT) - Customer Security Controls Framework (CSCF)*.

Com base na abordagem metodológica *Design Science Research* (DSR), foi concebido e validado um modelo abrangente, estruturado segundo o ciclo de melhoria contínua *Plan, Do, Check, Act* (PDCA), e os núcleos funcionais do quadro normativo NIST - CSF.

A validação empírica do modelo foi realizada através de entrevistas a especialistas de cibersegurança do setor em análise, cujos contributos permitiram aferir a cobertura, aplicabilidade e clareza do modelo proposto.

Os resultados indicam que a integração criteriosa de requisitos técnicos, organizacionais e regulatórios permite mitigar de forma eficaz os riscos cibernéticos, promovendo uma postura de segurança congruente e resiliente nas instituições bancárias. Este trabalho contribui, assim, para o reforço da segurança da informação no setor bancário.

Palavras-Chave: Banco, Ciber, Práticas, Configuração, Fortalecimento, Resiliência

Abstract

The increasing sophistication of cyber threats currently represents one of the greatest challenges for the banking sector, particularly for banking institutions, given the critical nature of the assets they handle.

This project focuses on the development of a robust model of security practices and configurations, with the aim of strengthening cyber resilience in the financial sector.

The research is based on a Systematic Literature Review (SLR) and a comparative analysis of internationally recognised frameworks, using the National Institute of Standards and Technology (NIST) - Cybersecurity Framework (CSF) as the foundation of the model and supporting it with Center for Internet Security Controls (CIS), Payment Card Industry - Data Security Standard (PCI-DSS) and Society for Worldwide Interbank Financial Telecommunication (SWIFT) - Customer Security Controls Framework(CSCF).

Based on the DSR methodological approach, a comprehensive model was designed and validated, structured according to the PDCA continuous improvement cycle and the functional cores of the NIST - CSF framework.

The empirical validation of the model was carried out through interviews with industry experts, whose contributions allowed us to assess the model´s scope, usability, and clearness.

The results indicate that the careful integration of technical, organisational, and regulatory requirements effectively mitigates cyber risks, promoting a consistent and resilient security posture in banking institutions. This work thus contributes to strengthening information security in the banking sector.

Keywords: *Bank, Cyber, Practices, Configuration, Hardening, Resilience*

Conteúdo

Agradecimentos i

Resumo iii

Abstract v

Lista de Figuras ix

Lista de Tabelas xi

Lista de Siglas xiii

Capítulo 1. Introdução 1
1.1. Estrutura Dissertação 3

Capítulo 2. Revisão da Literatura 5
2.1. Enquadramento 5
2.2. Metodologia 6
2.3. Necessidade de Revisão 6
2.4. Conduzir Revisão 7
2.4.1. Protocolo de Revisão 7
2.4.2. Resultados Pesquisa 8
2.4.3. Extração e análise de dados 8
2.5. Discussão 9
2.5.1. Gestão de risco 11
2.5.2. Responsabilidade 11
2.5.3. Treino e Sensibilização 12
2.5.4. Fraude e Impacto 12
2.5.5. Medidas de Segurança no Setor Bancário 12
2.5.6. Conclusões 13

Capítulo 3. Desenvolvimento do Modelo Proposto 15
3.1. Introdução 15
3.2. Ciclo de Cibersegurança 16
3.3. Análise e comparação do modelo de referência NIST - CSF com os modelos de referência CIS, PCI-DSS e SWIFT CSCF 16
3.3.1. NIST - CSF 16
3.3.2. CIS 17
3.3.3. PCI-DSS 17
3.3.4. SWIFT CSCF 17
3.3.5. Comparação NIST - CSF / CIS 18

3.3.6. Comparação NIST - CSF / PCI-DSS 18
3.3.7. Comparação NIST - CSF / SWIFT CSCF 19
3.4. Exploração da NIST - CSF: Análise dos núcleos e integração com os requisitos da CIS, PCI-DSS e SWIFT CSCF 20
3.4.1. Núcleo: Governo 20
3.4.2. Núcleo: Identificar 23
3.4.3. Núcleo: Proteger 27
3.4.4. Núcleo: Detetar 36
3.4.5. Núcleo: Responder 39
3.4.6. Núcleo: Recuperar 41
3.5. Fundamentação e Estrutura do Modelo Proposto 42
3.6. Apresentação do Modelo Proposto 44
3.6.1. Conclusões 56

Capítulo 4. Validação do Modelo 57
4.1. Perfil dos entrevistados 57
4.2. Estrutura das entrevistas 57
4.3. Contributos das Entrevistas 58
4.3.1. Cobertura do modelo aos riscos das instituições bancárias 59
4.3.2. Adequação dos modelos de referência 59
4.3.3. Exequibilidade do Modelo no Contexto Organizacional 60
4.3.4. Equilíbrio e Abrangência do Modelo 62
4.3.5. Clareza e Acessibilidade do modelo para pessoas não especializadas na área 63
4.3.6. Simplicidade de Adoção 64
4.4. Resultados das Entrevistas 64
4.4.1. Cobertura do modelo aos riscos das instituições bancárias 65
4.4.2. Adequação das modelos de referência 65
4.4.3. Exequibilidade do Modelo no Contexto Organizacional 65
4.4.4. Equilíbrio e Abrangência do Modelo 66
4.4.5. Clareza e Acessibilidade do modelo para pessoas não especializadas na área 66
4.4.6. Simplicidade de Adoção 66
4.4.7. Síntese Final das Entrevistas 66
4.5. Alterações Sugeridas 67

Capítulo 5. Conclusões 71
5.1. Conclusões do Trabalho 71
5.2. Trabalho Futuro 72

Referências Bibliográficas 73

Apêndice A. Modelo 77

Lista de Figuras

Figura 1	Esquema *Design Science Research*	3
Figura 2	Distribuição dos artigos por tipo de publicação	9
Figura 3	Modelo PDCA	16
Figura 4	Ciclo Cibersegurança	17
Figura 5	Modelo desenvolvido	43
Figura 6	Secção do modelo: Identificar	47
Figura 7	Secção do modelo: Proteger	49
Figura 8	Secção do modelo: Detetar	52
Figura 9	Secção do modelo: Responder	53
Figura 10	Secção do modelo: Recuperar	55
Figura 11	Alteração sugerida: Identificação de Funções Críticas do Negócio e Classificação de Inventários	67
Figura 12	Alteração sugerida: Gestão de Vulnerabilidades e Sensibilização/Treino	68
Figura 13	Alteração sugerida: Processo de Gestão de Terceiras Partes	69
Figura 14	Modelo Parte 1	78
Figura 15	Modelo Parte 2	79

Lista de Tabelas

Tabela 1	Passos RSL	6
Tabela 2	Passos de Filtragem	8
Tabela 3	Distribuição artigos por ano de publicação	9
Tabela 4	Definições das áreas levantadas no estudo	10
Tabela 5	Distribuição artigos pelas questões e desafios identificados em cada área	10
Tabela 6	Definições das áreas levantadas no estudo	10
Tabela 7	Distribuição artigos pelas questões e desafios identificados em cada área	10
Tabela 8	Síntese comparativa entre os modelos NIST-CSF e CIS	18
Tabela 9	Síntese comparativa entre os modelos NIST-CSF e PCI-DSS	19
Tabela 10	Síntese comparativa entre os modelos NIST-CSF e SWIFT CSCF	20
Tabela 11	Mapeamento dos controlos do Núcleo Governo	21
Tabela 12	Mapeamento dos controlos do Núcleo Identificar	24
Tabela 13	Mapeamento dos controlos do Núcleo Proteger	28
Tabela 14	Mapeamento dos controlos do Núcleo Detetar	37
Tabela 15	Mapeamento dos controlos do Núcleo Responder	39
Tabela 16	Mapeamento dos controlos do Núcleo Recuperar	41
Tabela 17	Atividades, Entradas e Resultados - Governo	45
Tabela 18	Atividades, Entradas e Resultados - Identificar	47
Tabela 19	Atividades, Entradas e Resultados - Proteger	50
Tabela 20	Atividades, Entradas e Resultados - Detetar	52
Tabela 21	Atividades, Entradas e Resultados - Responder	54
Tabela 22	Atividades, Entradas e Resultados - Recuperar	56
Tabela 23	Perfil dos Especialistas Entrevistados	57
Tabela 24	Síntese Entrevistas	67

Lista de Siglas

AES: *Advanced Encryption Standard*

ASF: Autoridade de Supervisão de Seguros e Fundos de Pensões

ATM: *Automated Teller Machine*

BIA: *Business Impact Analysis*

BVN: *Bank Verification Number*

BYOD: *Bring Your Own Device*

CERT: *Computer Emergency Response Team*

CIA: *Confidentiality, Integrity, Availability*

CIS: *Center for Internet Security*

CNCS: Centro Nacional de Cibersegurança

COBIT: *Control Objectives for Information and Related Technologies*

CSCF: *Customer Security Controls Framework*

CSF: *Cybersecurity Framework*

DDoS: *Distributed Denial of Service*

DKIM: *DomainKeys Identified Mail*

DMARC: *Domain-based Message Authentication, Reporting and Conformance*

DORA: *Digital Operational Resilience Act*

DSR: *Design Science Research*

ECDHE: *Elliptic Curve Diffie-Hellman Ephemeral*

EDR: *Endpoint Detection and Response*

EPP: *Endpoint Protection Platform*

FIN: *Financial Information Network*

HIDS: *Host Intrusion Detection Systems*

HTTPS: *Hyper Text Transfer Protocol Secure*

ICIC: *Improving Critical Infrastructure Cybersecurity*

IDS: *Intrusion Detection System*

IPS: *Intrusion Prevention System*

ISO: *International Organization for Standardization*

KPIs: *Key Performance Indicators*

KRIs: *Key Risk Indicators*

MiCA: Markets in Crypto-Assets

NDAs: *Non-disclosure Agreements*

NIDS: *Network Intrusion Detection System*

NIST: *National Institute of Standards and Technology*

NIS2: *Network and Information Security Directive*

OSI: *Open Systems Interconnection*

OWASP: *Open Web Application Security Project*

PAM: *Privileged Access Management*

PAN: *Primary Account Number*

PCI-DSS: *Payment Card Industry-Data Security Standard*

PDCA: *Plan, Do, Check, Act*

PRISMA: *Preferred Reporting Items for Systematic Reviews and Meta-Analyses*

RMA: *Relationship Management Application*

RMF: *Risk Management Framework*

RSL: Revisão Sistemática da Literatura

SIEM: *Security Information and Event Management*

SIP: *Shared Infrastructure Programme*

SLA: *Service Level Agreement*

SOC: *Security Operation Center*

SPF: *Sender Policy Framework*

SSH: *Secure Shell*

SWIFT: *Society for Worldwide Interbank Financial Telecommunication*

TI: Tecnologia da Informação

URL: *Uniform Resource Locator*

WPA2: *Wi-Fi Protected Access 2*

XDR: *Extended Detection and Response*

CAPÍTULO 1

Introdução

A segurança da informação e cibersegurança deixaram de ser apenas questões meramente técnicas a serem resolvidas pelos departamentos de Tecnologia da Informação (TI) das organizações. Os requisitos de conformidade com regulamentos e legislação fizeram com que as consequências das infrações de cibersegurança e da exploração de potenciais vulnerabilidades se reflitam em todos os departamentos das organizações [1].

À medida que as organizações embarcam em processos de transição e transformação digital, a garantia de princípios de *Confidentiality, Integrity, Availability* (CIA) dos seus ativos digitais torna-se essencial. Enfrentar as ameaças a que estes ativos se encontram expostos exige uma abordagem séria e integrada e medidas preventivas que contemplem a defesa de sistemas de acordo com as exigências e campos de atuação de cada entidade [2].

O panorama atual do ciberespaço engloba atividades criminosas que afetam muitas unidades e funções organizacionais distintas, mas especialmente o setor bancário [1]. Este é frequentemente o alvo mais tentador e recorrente, visto ser o mais recompensador, financeiramente, para os atacantes, mas não só [1]. Muitas vezes, os atacantes podem ter outras intenções, como meramente afetar a imagem do banco ou marcar uma posição política [3]. As intrusões cibernéticas representam um dos desafios mais críticos para as instituições financeiras [4].

A questão da cibersegurança é principalmente importante no setor bancário, visto que as instituições bancárias controlam praticamente todo o fluxo monetário em todos os setores de atividade da sociedade, sendo responsáveis por manter seguros os ativos financeiros e as informações dos clientes [1].

A atenção voltou-se para as ameaças cibernéticas e as estratégias correspondentes para as mitigar. Nos últimos anos, testemunhou-se uma série de ataques elaborados e um aumento na cobertura oferecida pelos meios de comunicação social, aumentando a sensibilização de que estes incidentes estão cada vez mais a crescer em termos de frequência, custo, planeamento e gravidade [5].

De entre os setores mais afetados com ciberataques, como a saúde, educação e transportes, está também presente a banca, maioritariamente através de ataques de *phishing* contra os clientes. Dados estatísticos por parte do Centro Nacional de Cibersegurança (CNCS) revelam que os clientes das instituições bancárias são alvo de 59% da totalidade dos ataques de *phishing* e *smishing* [6].

Também o número de ataques de *ransomware* aumentou em quase 100% de 2022 para 2023 [6].

O risco cibernético foi outrora tratado como secundário em relação a outros, aparentemente, mais importantes para o balanço do banco, como o risco de crédito ou de liquidez. O surgimento de riscos mais graves veio alterar esta situação [4]. As instituições financeiras devem reconhecer que os invasores conseguem ultrapassar as suas medidas de segurança e, por isso, não as podem considerar infalíveis [7].

Uma das principais formas de ataque é através do lado humano, que continua a ser a principal fraqueza a nível de segurança. Recomendam-se então formações especializadas para os trabalhadores de todas as áreas, com foco na cibersegurança. Como boa prática, a maior parte das instituições financeiras exige que certos colaboradores sejam certificados nesta temática, e que consigam apoiar o resto dos colaboradores nesta matéria.

Especialistas financeiros propõem a realização de seminários de sensibilização sobre a matéria de cibersegurança, o reforço do acesso dos utilizadores, a encriptação e as *firewalls*, a avaliação regular das vulnerabilidades, a realização de testes de intrusão, a revisão e atualização frequentes das infraestruturas e dos sistemas, a cooperação entre os operadores bancários e as autoridades reguladoras e a sensibilização do público [8].

Para fazer face a estes riscos emergentes, os reguladores e supervisores financeiros lançaram várias iniciativas para reforçar a resiliência cibernética dos sistemas financeiros [7].

No que toca à mitigação, é necessário o reforço das medidas de segurança através de uma série de requisitos [7]. Um sistema organizacional, complexo e multifacetado, para ser considerado resiliente, deve conseguir manter as operações sob ataque ou falha, sendo capaz de reconfigurar/recuperar as suas funções e, eventualmente, restabelecer o estado original [9].

A colaboração entre instituições financeiras, auditores externos e empresas do setor da segurança aumenta o nível de segurança e resiliência cibernética. O que pode ser alcançado estabelecendo parcerias com empresas com experiência internacional, ou aproveitando o conhecimento e perspetivas fornecidas por auditores independentes [10]. As instituições financeiras devem desenvolver um plano abrangente para controlo de segurança e integrar o mesmo na sua arquitetura e sistemas de informação [11].

É importante que as organizações monitorizem e reavaliem continuamente a eficácia dos controlos de segurança implementados [11].

A implementação de medidas de cibersegurança é necessária devido à crescente complexidade e digitalização das operações comerciais, que expõe as organizações a ameaças e ataques cibernéticos [9]. Além disso, a natureza evolutiva das ameaças à cibersegurança, como os ataques de *malware*, realça a necessidade de existência de processos de recuperação robustos e a adoção de melhores práticas de segurança [12]. Ao implementar estas medidas, as organizações podem atenuar os riscos e garantir a resiliência dos seus sistemas de informação [8].

O principal objetivo deste trabalho é desenvolver um modelo, baseado no quadro normativo da *National Institute of Standards and Technology* (NIST) - *Cybersecurity Framework* (CSF) e agregando controlos e recomendações de outros modelos reconhecidos na área, tendo em consideração as boas práticas e procedimentos recomendados. Pretende-se igualmente identificar vulnerabilidades e os seus respetivos tratamentos, sugerindo melhorias/alterações a ter em conta de forma a mitigar o risco o máximo possível e garantir a segurança do sistema, ativos, dados sensíveis e recursos críticos contra ameaças de segurança.

Para este trabalho foi elaborada a seguinte questão de investigação: **Será possível conceber um modelo que indique quais as boas práticas de segurança fundamentais a implementar numa instituição bancária, tendo em conta os desafios e adversidades da área, proporcionando mitigação para os riscos específicos?**

A metodologia de investigação utilizada no âmbito deste trabalho foi o *Design Science Research* (DSR). O modelo é cíclico, onde, no final da quinta etapa, caso haja necessidade de

melhoria, regressa-se até à segunda etapa, repetindo o processo até que as especificações definidas sejam atingidas. O número de iterações não é fixo e apenas se avança para o último passo quando o modelo cumprir todos os requisitos definidos [13].

O DSR está estruturado em 6 fases:

(1) Identificação do problema;
(2) Definição dos objetivos da solução;
(3) Desenho da metodologia de desenvolvimento;
(4) Demonstração;
(5) Avaliação;
(6) Comunicação

Na figura 1 encontra-se o modelo de investigação que foi aplicado:

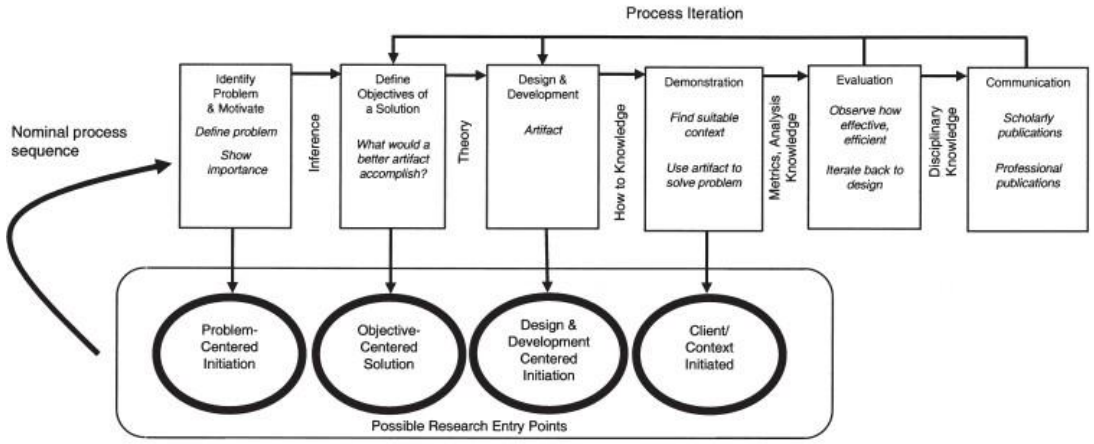


Figura 1. Esquema *Design Science Research* [13]

A aplicação desta metodologia neste trabalho inicia-se com a **identificação do problema**, a questão dos crescentes riscos cibernéticos, referidos no capítulo inicial. De seguida, na fase de **definição dos objetivos**, o foco deste trabalho é conseguir recomendar novas práticas e configurações de segurança, bem como identificar vulnerabilidades e os seus respetivos tratamentos [13].

A terceira fase desta metodologia está demonstrada no terceiro capítulo deste trabalho, através da **análise comparativa** dos vários modelos de referência, e do consequente trabalho de conjunção de requisitos. Seguidamente, as fases 4 e 5, são implementadas através de entrevistas realizadas com especialistas da área, quer para **demonstração** como para **validação** do modelo desenvolvido.

Por fim, na última fase desta metodologia, e caso as fases anteriores tenham sido concluídas com sucesso, procede-se à comunicação e divulgação dos resultados alcançados, através da **escrita da dissertação** e da elaboração de um artigo científico [13].

1.1. Estrutura Dissertação

No capítulo 2 será apresentada a revisão sistemática da literatura, cujo objetivo é compreender o estado da arte em torno da cibersegurança no que diz respeito ao setor bancário. São analisados os principais riscos e ameaças, bem como modelos de referência e medidas de proteção. Por fim,

aborda-se ainda o papel do fator humano, sensibilização e treino, os impactos das ameaças e as boas práticas adotadas pelo setor.

No capítulo 3 é explicado o modelo proposto. São realizadas análises comparativas entre os quadros normativos selecionados para complementar o modelo. Por fim, são agregados e complementados os controlos do modelo de referência da NIST CSF, usado como alicerce do modelo, com os vários controlos das restantes.

O capítulo 4 aborda a validação do modelo, através da apresentação do conteúdo das entrevistas com os especialistas do setor. Estes contributos permitiram avaliar a relevância e aplicabilidade prática do modelo, bem como identificar pontos de melhoria. Com base nas opiniões recolhidas, foram implementadas alterações ao modelo.

Por fim, no capítulo 5, serão apresentadas as conclusões do trabalho desenvolvido, em conjunto com a retrospetiva dos resultados alcançados e limitações encontradas ao longo da investigação. É também feita a resposta à questão de investigação. Por fim, são identificados possíveis caminhos para trabalho futuro.

CAPÍTULO 2

Revisão da Literatura

Neste capítulo foi realizada uma revisão sistemática da literatura com o objetivo de compreender o atual estado da arte sobre o tema da investigação.

Para a realização da Revisão Sistemática da Literatura (RSL) recorreu-se ao método *Preferred Reporting Items for Systematic Reviews and Meta-Analyses* (PRISMA).

2.1. Enquadramento

O risco cibernético é frequentemente identificado como uma das maiores ameaças ao funcionamento eficaz do sistema financeiro. Na última década, tem-se verificado um aumento constante dos incidentes cibernéticos e das perdas associadas [14].

Devido à crescente complexidade das redes, e com as empresas a rentabilizarem-se com as suas expansões, surgiram novas ameaças, tendo vindo desde então a existir uma crescente evolução nas medidas de cibersegurança [15].

O conceito de cibersegurança evoluiu para resiliência cibernética, que se refere à capacidade de uma organização se adaptar à mudança, suportar ataques e recuperar-se após os mesmos [9]. O estudo da cibersegurança é essencial em todas as organizações, não só as envolvidas no mercado financeiro, mas também com as que lidam com fluxos de informação sensíveis. É responsabilidade dos gestores promover a sensibilização para a cibersegurança nas suas organizações [12].

A cibersegurança pode ser definida como um conjunto de ações com vista à proteção dos ativos de uma organização, com foco nas ameaças e ataques à informação [16]. Este conjunto contempla medidas a aplicar de forma a proteger os sistemas contra acessos não autorizados, no qual estão inseridos diferentes protocolos, procedimentos, ferramentas, diretrizes e modelos de referência [5].

No setor bancário são usados modelos de referência para controlo de riscos, avaliação ou medição, como os da NIST - CSF [1] ou *Control Objectives for Information and Related Technologies* (COBIT) [17].

Alguns tipos de ataques mais comuns que afetam o setor bancário, e não só, são ataques de *phishing*, roubo de cartões bancários, roubo de identidade, *malware*, fraude bancária e esquemas fraudulentos que envolvem o *Bank Verification Number* (BVN), um sistema de identificação biométrica que utiliza um número de 11 dígitos como identificador universal em todos os bancos do país, e outros números usados para o mesmo efeito [18].

Em situações de ciberataques, a capacidade de reação imediata é fundamental para diminuir os possíveis danos. Por isso, é determinante que os bancos disponham de um processo de resposta rápida após um ataque e mecanismos de resolução para mitigar ao máximo possível as suas consequências, principalmente durante o período em que os pagamentos sofrem interrupções [19]. No que diz respeito ao desenvolvimento futuro, são dois os caminhos mais prováveis a tomar: inteligência artificial e modelos de aprendizagem automática [9].

2.2. Metodologia

De forma a compreender melhor estas ameaças e as suas possíveis formas de mitigação, foi utilizada uma metodologia de análise rigorosa do estado da arte, a RSL

É um tipo de investigação científica que tem como objetivo reunir, avaliar e resumir os resultados de múltiplos estudos [20]. Procura tratar toda a documentação disponível sobre uma(s) determinada(s) questão(ões) de investigação ou tópico, utilizando métodos sistemáticos e explícitos para identificar, selecionar e avaliar a investigação relevante [21].

Tem como principal objetivo providenciar um resumo de informação sobre um tema, identificando falhas e percebendo em que áreas é necessário aprofundar o estudo [21].

É essencial para garantir que todas as decisões/recomendações a seguir são fundamentadas com a melhor base possível [21].

Este método apresenta várias vantagens, como a identificação de falhas, sintetização de evidências, compreensão da literatura disponível e minimização da imparcialidade [21].

Deste modo, foi a metodologia escolhida para o trabalho desenvolvido, visto que apresenta uma cobertura bastante ampla e exaustiva da literatura existente, prevenindo a omissão de estudos importantes que possam impactar o modelo proposto, na identificação de pontos fortes e falhas dos vários modelos de referência, crucial para atingir os objetivos do trabalho a desenvolver e a tomar decisões fundamentadas sobre os vários pontos de cada modelo com base em evidências. Esta metodologia oferece também uma abordagem de recolha e análise da informação que complementa a natureza estruturante dos quadros normativos.

De seguida, apresenta-se, na Tabela 1, a estrutura da revisão.

Tabela 1. Passos RSL

Planeamento da Revisão	Realização da Revisão	Relatório da Revisão
Necessidade de revisão	Resultados da pesquisa	Resumo dos dados extraídos
Objetivo	Extração e análise de dados	Relatório das conclusões
Protocolo de revisão		

2.3. Necessidade de Revisão

Desde golpes a *Automated Teller Machine* (ATM) na Índia, ataques ao banco central do Bangladesh [14], ataques de *Distributed Denial of Service* (DDoS) aos principais bancos norte-americanos resultando em perdas na ordem dos milhões de dólares [22], e a fugas de informações bancárias, como no caso de um dos maiores bancos do mundo, *JPMorgan Chase*, sediado nos Estados Unidos da América, onde foram comprometidos dados de aproximadamente 76 milhões de famílias e 7 milhões de pequenos negócios [1], o risco cibernético tem vindo a tornar-se um dos problemas mais complexos de todo o sistema financeiro [14].

A segurança da informação do próprio banco e dos seus clientes é difícil de alcançar, devido à exposição de que são alvo e, por causa dos múltiplos intervenientes no processo, como o fator humano, tecnológico ou físico [23]. A fraude bancária é um problema que impacta todos, sendo cada vez mais difícil de detetar. As organizações criminosas estão cada vez mais bem preparadas e estruturadas, para poderem operar praticamente a partir de todo o mundo [23].

A resiliência dos sistemas é um processo contínuo de melhoramento e adaptação no combate aos ataques sofridos, de forma a evoluir [23]. Os bancos devem procurar reavaliar os seus mecanismos de defesa continuamente [23].

Esta investigação torna-se assim necessária na procura destes processos de evolução e adaptação contínuos, de modo a encontrar potenciais falhas e vulnerabilidades, e novos mecanismos de segurança com vista à proteção do setor bancário.

2.4. Condução da revisão

Consiste na segunda fase da RSL, e contém a aplicação do protocolo de revisão e a análise dos dados extraídos. O principal objetivo desta fase é garantir que o processo de seleção, extração e avaliação da literatura seja conduzido de forma rigorosa.

2.4.1. Protocolo de Revisão

O protocolo usado foi o PRISMA. Esta metodologia foi desenvolvida de modo a facilitar a comunicação transparente e completa de revisões sistemáticas. É uma diretriz para a elaboração de documentos/relatórios pensada de modo a resolver a má execução de relatórios de revisões sistemáticas [24].

Inclui uma lista de controlos de 27 itens recomendados para a apresentação de relatórios em revisões sistemáticas e um documento explicativo com orientações adicionais [24].

As recomendações foram adotadas mundialmente, evidenciado pela sua co-publicação em várias revistas, citação em mais de 60 000 relatórios (Scopus, agosto de 2020), aprovação de quase 200 revistas e organizações de revisões sistemáticas, e a adoção em várias disciplinas [24].

As evidências de estudos observacionais sugerem que a utilização do PRISMA está associada ao desenvolvimento mais completo das revisões sistemáticas [24].

Usaram-se alguns dos pontos da lista de controlos do PRISMA nos vários aspetos de desenvolvimento do trabalho, como na introdução, pontos 3 e 4 da lista, descrevendo o racional da revisão com base no conhecimento existente e fornecendo uma declaração explícita dos objetivos que a revisão aborda, nos métodos usados na revisão de literatura, como a especificação dos critérios de inclusão e exclusão na seleção de artigos (ponto 5) e das bases de dados e sites utilizados para a sua recolha (ponto 6) e os filtros utilizados (ponto 7).

Na discussão foram descritos os resultados dos processos de pesquisa e seleção (ponto 16a) e foi apresentada uma interpretação geral dos resultados (ponto 23a) [25].

O trabalho inicia-se com a revisão sistemática da literatura, sendo seguido de comparação e análises dos modelos de referências escolhidas e consequente agregação de requisitos. Posteriormente, foram conduzidas entrevistas a especialistas da área de modo a validar o modelo apresentado. Foram efetuadas as alterações sugeridas pelos especialistas, aquando das entrevistas, e, por fim, termina-se o trabalho com as conclusões obtidas.

As bases de dados científicas consideradas para a pesquisa bibliográfica foram as seguintes:

- ACM Digital Library
- EBSCO
- IEE Xplore Digital Library
- Scopus
- Web of Science

Primeiramente, fez-se a pesquisa sem qualquer tipo de filtragem (*Full Text).* O primeiro filtro aplicado foi ao resumo, que reduziu substancialmente o número de resultados obtidos. De seguida, foram selecionados apenas artigos publicados em revistas e conferências.

O terceiro filtro foi a data, onde se consideraram apenas artigos após 2004. Esta data foi escolhida visto que o tema da cibersegurança começou a ser estudado mais seriamente no início da década de 2000. O quarto filtro foi a linguagem de escrita dos artigos, apenas em inglês.

Por fim, o quinto e sexto filtros foram filtros manuais, primeiramente na verificação de artigos duplicados e, de seguida, uma verificação manual de todos os artigos de modo a garantir a sua adequação ao tema.

Critérios de inclusão:

- Conferências e Revistas
- Escritos em inglês
- Título relevante

Critérios de exclusão:

- Redigidos num idioma diferente do inglês
- Título não relevante
- Textos não científicos

2.4.2. Resultados Pesquisa

A pesquisa efetuada nas bases de dados bibliográficas foi a seguinte: (*Bank* AND Cyber**) *AND* (*Practices* OR Configuration* OR Hardening* OR Resilience**)

Apresenta-se na tabela 2 o processo de filtragem e os produtos finais dos artigos reunidos.

Tabela 2. Passos de Filtragem

Base de dados	Inicial	1ºFiltro	2ºFiltro	3ºFiltro	4ºFiltro	5ºFiltro	6ºFiltro
ACM Digital Library	3652	5	4	4	4	4	1
EBSCO	1350991	3102	452	433	333	163	18
IEE Xplore Digital Library	73	24	20	20	20	20	5
Scopus	25664	144	121	120	113	106	12
Web of science	221	68	42	42	39	4	0
Total	1380601	3343	639	619	509	297	36

2.4.3. Extração e análise de dados

Depois de feita a aplicação dos filtros, todos os artigos foram analisados individualmente, sendo extraídos os domínios de cada um, o ano de publicação e características. Na figura 2 apresenta-se a distribuição dos artigos reunidos em conferências e revistas.

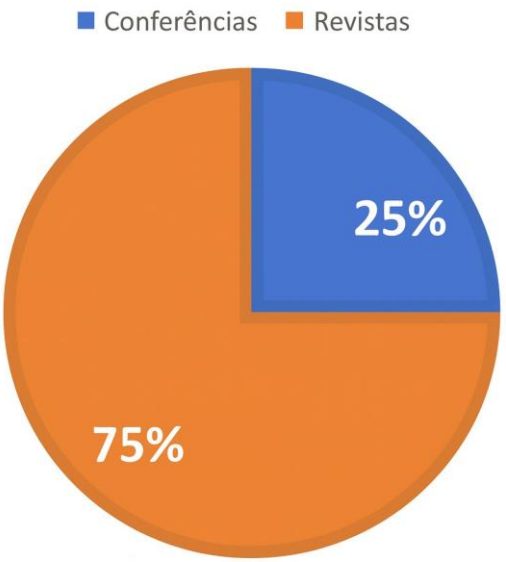


Figura 2. Distribuição dos artigos por tipo de publicação

Na tabela 3 verificam-se as distribuições dos artigos levantados por ano de publicação.

Tabela 3. Distribuição artigos por ano de publicação

Ano	NºArtigos	Percentagem (%)
2023	4	11,11
2022	6	16,67
2021	3	8,33
2020	4	11,11
2019	4	11,11
2018	2	5,56
2017	4	11,11
2016	4	11,11
2015	2	5,56
2014	1	2,78
2013	1	2,78
2012	0	0
2011	1	2,78
Total	**36**	**100%**

2.5. Discussão

A Tabela 4 apresenta as definições associadas a cada uma das áreas identificadas, gestão do risco, fraude e impacto social, e responsabilidade. Estas definições constituem a base para a identificação dos principais desafios e questões abordados na literatura.

Tabela 4. Definições das áreas levantadas no estudo

Área	**Definição**
Gestão do risco	Identificação, avaliação e mitigação de potenciais ameaças e vulnerabilidades, que podem comprometer a integridade da organização
Fraude e impacto social	Atividades ou eventos maliciosos que resultam num acesso não autorizado a informação confidencial, dando origem a danos por vezes incalculáveis
Responsabilidade	Responsabilidade ética das organizações e indivíduos.

De seguida, a Tabela 5 sistematiza a distribuição dos artigos pelas questões e desafios identificados em cada uma dessas áreas. Observa-se que a área de gestão de risco concentra o maior número de publicações, evidenciando um interesse significativo na identificação e mitigação de ameaças e vulnerabilidades. As áreas de fraude e impacto social, e responsabilidade também se destacam, embora com menor representatividade.

Tabela 5. Distribuição artigos pelas questões e desafios identificados em cada área

Área	Total	Referências
Gestão do risco	18	[4], [2], [10], [12], [26], [27], [7], [9],[11], [15], [20], [19], [14], [28], [17], [29], [30], [22]
Fraude e impacto social	6	[8], [26], [23], [18], [31], [32]
Responsabilidade	8	[1], [33], [5], [15], [16], [34], [30], [22]

Prosseguindo a análise, a Tabela 6 introduz um novo tema, focado nas medidas adotadas para enfrentar os desafios anteriormente descritos. As áreas de medidas humanas, tecnológicas e regulamentação traduzem diferentes abordagens, desde ações de sensibilização e formação, à implementação de soluções tecnológicas, como autenticação multi-fator, e à criação de normas e políticas formais.

Tabela 6. Definições das áreas levantadas no estudo

Área	Definição
Medidas humanas	Conjunto de medidas de modo a aumentar a consciencialização e instrução.
Medidas tecnológicas	Conjunto de medidas implementadas (*software*, modelos de referência, etc.) destinadas a proteger dados e sistemas.
Regulamentação	Normas e diretrizes estabelecidas para garantir a proteção e integridade dos dados e sistemas.

Por fim, a Tabela 7 apresenta a distribuição dos artigos pelas medidas identificadas, revelando uma preponderância das medidas humanas e tecnológicas. Este resultado sugere que a literatura tende a privilegiar estratégias operacionais e comportamentais na mitigação de riscos, apesar de os aspetos regulatórios serem também fundamentais. A articulação entre estas dimensões evidencia a importância de uma abordagem multidisciplinar para enfrentar os desafios associados à segurança e à responsabilidade organizacional.

Tabela 7. Distribuição artigos pelas questões e desafios identificados em cada área

Área	Total	Referências
Medidas humanas	12	[33], [5], [8], [10], [12], [26], [27], [7], [16], [18], [31], [34]
Medidas tecnológicas	11	[1], [2], [33], [8], [10], [26], [9], [11], [15], [18], [17]
Regulamentação	3	[4], [14], [29]

Em síntese, a análise das tabelas apresentadas permitiu obter uma visão geral das principais áreas temáticas e das abordagens identificadas na literatura. Verificou-se que os estudos tendem a concentrar-se sobretudo na gestão do risco, refletindo a relevância desta dimensão na mitigação de ameaças e vulnerabilidades organizacionais. Paralelamente, as temáticas de fraude e impacto social e responsabilidade surgem como complementares, evidenciando preocupações éticas, legais e de segurança que atravessam o contexto organizacional.

No que respeita às medidas de atuação, observa-se um maior enfoque nas dimensões humanas e tecnológicas, com a regulamentação a ocupar um papel menos expressivo, ainda que essencial.

Assim, esta primeira análise fornece uma base sólida para a compreensão das tendências e lacunas existentes, servindo de ponto de partida para o aprofundamento de cada uma das áreas, seguidamente.

2.5.1. Gestão de risco

Muitos dos modelos de referência tradicionais não conseguem dar resposta às ameaças emergentes no mundo da cibersegurança. Os incidentes nesta área são bastante diferentes das demais, visto que muitas vezes não é possível dar resposta com base nas medidas usadas em ataques anteriores, devido à natureza dos mesmos, que estão em constante evolução [14]. É fundamental a utilização destes modelos por parte dos bancos, principalmente aqueles orientados para a gestão de risco [30].

Outro modelo é o *Improving Critical Infrastructure Cybersecurity* (ICIC), cujo objetivo é ajudar os responsáveis pelas infraestruturas críticas, que dizem respeito a ativos e sistemas, quer virtuais quer físicos, cuja falha teria um impacto catastrófico, a identificar, avaliar e gerir o risco cibernético [30].

Um dos principais problemas da segurança cibernética é o pensamento de que investir em segurança é um investimento sem retorno financeiro [9]. Gerir e supervisionar o risco é uma das principais responsabilidades dos gestores do setor bancário, e embora os bancos sempre tenham tido processos de gestão de risco, a crise global financeira de 2008 destacou a importância destes processos. Desde então, muitos bancos reformularam e repensaram os seus processos e procedimentos de gestão de risco [4].

Existe bastante pressão para que as instituições bancárias adotem uma postura virada para a gestão de risco. Um modelo também bastante recomendado para uma instituição bancária é a *Risk Management Framework* (RMF), integrada na NIST - CSF [11].

Passou a ser obrigatório, a partir de 2009, ser exposto publicamente de que forma a gerência da organização vê a gestão de risco e como age para monitorizar o risco [4].

2.5.2. Responsabilidade

O lado humano continua a ser o principal fator comprometedor na área da cibersegurança, principalmente através de ataques de *phishing*, *vishing* e *smishing*, onde o intuito é enganar a pessoa de forma a aceder a informação confidencial [10]. Cerca de 95% dos ataques de *malware* e *ransomware* foram causados por falhas humanas, maioritariamente não intencionais [12].

No setor bancário, a avaliação das características comportamentais dos colaboradores, de forma a mitigar o risco, continua a ser uma área pouco explorada. A personalidade pode ajudar a perceber os aspetos mentais das pessoas e as respetivas associações a atividades ilegais [31]. As organizações dispõem de poucos recursos na promoção de comportamentos éticos [31].

É necessária uma mudança de paradigma nos valores sociais e éticos [10]. Uma hipótese para atingir este objetivo passa pelas instituições financeiras disponibilizarem ferramentas para a tomada de decisões éticas [31]. Começa a ser obrigatório, como no caso da Hungria, a existência de treino específico para os trabalhadores da área financeira [10].

Também os utilizadores, que têm um papel importante no combate às ameaças emergentes no mundo digital, devem estar conscientes dos perigos e alertar a quem de direito, ao detetarem atividades suspeitas [28]. Muitos clientes, normalmente com idades mais avançadas, continuam a desconhecer a maior parte das ameaças [23]. Cerca de 95% das pessoas estão informadas sobre ataques provenientes de vírus, no entanto apenas 36% estão sensibilizadas sobre os ataques de *phishing* [23]. Muitas vezes, basta um simples clique para comprometer informação confidencial, através de uma mensagem de correio eletrónico recebida, aparentemente pelo banco de confiança, com a solicitação de dados confidenciais [23]. Isto acontece muitas vezes por fraca sensibilização para este tipo de problemas [23].

Uma medida de proteção bastante importante é no processo de definição de palavras-passe, através da utilização de autenticação multifator, cujo principal objetivo é dificultar o acesso indevido aos dados e sistemas por parte dos atacantes cibernéticos [22]. A autenticação multifator é obrigatória na grande maioria das empresas de nível global, como o caso da *Intel*, *American Express* ou *MasterCard* [22]. Já se começa a observar uma tendência para a substituição das palavras-passe de forma definitiva em detrimento da utilização de dados biométricos, como impressões digitais, leitura da íris ou reconhecimento de voz [22].

2.5.3. Treino e Sensibilização

Deste modo é essencial o investimento das organizações em planos de treino e sensibilização social quer para os trabalhadores da área de cibersegurança, quer para os do setor bancário, como dos clientes [9]. Estes planos de treino podem incluir simulações de cibersegurança, que já se revelaram bastante eficazes, requerendo que a equipa de TI prepare e crie um ataque simulado, de forma que os colaboradores tenham de responder de acordo com os procedimentos necessários [22].

Nunca irá ser possível eliminar o erro humano na sua totalidade, mas se estes planos forem desenvolvidos corretamente e aplicados de forma contínua, a probabilidade de ocorrência de incidentes de segurança deste género irá diminuir consideravelmente [9]. Além disso, é importante a identificação e prevenção antecipada de vulnerabilidades nas fases iniciais do ciclo de desenvolvimento de *software* [29].

2.5.4. Fraude e Impacto Social

As instituições bancárias são as organizações que mais sofrem com ataques cibernéticos, devido

à motivação económica existente por parte dos atacantes [7]. Casos como o ataque cibernético de 2017 ao banco central do Bangladesh, onde mais de 100 milhões de dólares foram roubados, são, infelizmente, mais frequentes do que possam parecer [32].

Os clientes esperam do banco a máxima segurança, protegendo os seus ativos. Para tal, os bancos têm vindo a investir cada vez mais em medidas de segurança. A queda de uma instituição bancária traria consequências avassaladoras para toda a rede financeira da sociedade, como nos mostram vários casos ao longo das últimas décadas [1]. Por exemplo, num cenário de ataque que impeça um banco de realizar pagamentos, outros bancos podem depender desses pagamentos como fonte de liquidez, fazendo com que toda a rede bancária entre em colapso, com origem num ataque direcionado a um único banco [19].

2.5.5. Medidas de Segurança no Setor Bancário

De modo a complementar a questão de investigação, foi possível recolher várias medidas de segurança indispensáveis no setor bancário, e como estas contribuem para a mitigação do risco. Os bancos são obrigados a cumprir com várias normas de requisitos mínimos de segurança, exigidos pela superintendência dos bancos [23].

No caso do banco digital, a segurança deve também considerar aspetos relacionados com a utilização dos clientes, como a personalização da aplicação, a integração de serviços de terceiros, a utilização de janelas de multi-serviço, a usabilidade, o suporte e acessibilidade da aplicação, mas também potenciais pontos de risco que necessitam de avaliação e proteção adequada [26].

Além disso, verificações de rotina de rede para dispositivos não autorizados e *malware* são recomendadas para detetar e mitigar ataques cibernéticos [22]. Os dispositivos móveis também devem ser analisados regularmente, mesmo os que estejam devidamente autorizados a utilizar recursos e informação da organização [15].

A existência de um plano de ação bem definido e praticado pelos colaboradores no banco é fundamental, visto que o tempo de resposta a um incidente é de elevada importância de modo a reduzir ao máximo os possíveis danos e impactos [18].

Atualizar regularmente o *software* e *hardware* dos sistemas de TI do banco, de forma a estarem em conformidade com as normas de segurança, e deste modo a seguirem as melhores práticas [15]. A segmentação da rede é uma boa prática a seguir, de forma a restringir certos departamentos do banco de aceder a informação confidencial, sendo preciso, no entanto, que haja troca de informação entre as segmentações criadas, através de *firewalls*, por exemplo [15]. Uma boa prática é também a separação de segmentos confiáveis na camada física do modelo *Open Systems Interconnection* (OSI) [15].

Outra medida indispensável é a utilização de indicadores, e a sua respetiva análise, como a verificação interna da segurança do próprio banco. Uma forma de o fazer é através do quadro normativo da NIST - CSF, que permite não só fazer a averiguação da segurança como avaliar outros pontos críticos de todo o ecossistema da instituição bancária [1]. A análise de incidentes de segurança exige que as instituições recolham, monitorizem, avaliem e partilhem informações para identificar e prevenir as ameaças cibernéticas no setor. Esta cooperação é de facto importante, como é possível perceber pelo exemplo da resposta aos ataques de DDoS de 2012 a alguns bancos americanos [22]. Foram ataques sem precedentes em termos de volume.

Na tentativa de mitigar as ameaças, as instituições financeiras visadas começaram a com-partilhar informação entre elas e com o governo federal [22]. Os bancos atacados de seguida utilizaram a informação partilhada proveniente dos bancos que sofreram os incidentes para se precaverem da melhor forma possível, de tal forma que a recuperação pós-ataque foi muito mais

rápida e eficaz do que nas primeiras instituições afetadas, o que demonstra o valor da colaboração e partilha de informação [22].

Devem ser implementados procedimentos com o objetivo de bloquear o acesso não autorizado aos sistemas de informação, ferramentas e software do banco. Um possível exemplo é a implementação de regulamentos no que diz respeito à criação e utilização de palavras-passe, que devem cumprir parâmetros específicos [10].

Vários mecanismos e ferramentas de defesa devem ser utilizados, como sistemas de prevenção e deteção de intrusões, sistemas de gestão de incidentes ou software para gestão de cópias de segurança [10]. Estes mecanismos servem de apoio à estrutura de segurança e defesa do banco [10].

Devem também ser criadas equipas especializadas na resposta ao risco, como por exemplo *Computer Emergency Response Team* (CERT) [9]. Dentro desta equipa existe o *Security Operation Center* (SOC), responsável pela monitorização e supervisão [9].

2.5.6. Conclusões

O RSL permitiu consolidar uma visão abrangente sobre os riscos cibernéticos e os meios de proteção utilizados no setor bancário. Foi possível apurar que este setor é dos mais afetados pelos atacantes cibernéticos, devido à natureza sensível dos dados, informação e ativos que tratam, exigindo fortes medidas de gestão de risco, treino e sensibilização dos colaboradores e clientes, e a implementação de planos de contingência bem estruturados.

Entre os tópicos estudados, foi possível apontar os que se destacaram do ponto de vista da importância, como a necessidade de modelos de referência adequados às ameaças constantes, investimento em formação contínua, aplicação de medidas de proteção (autenticação multifator), indicadores de segurança e atualização regular dos sistemas.

Outro ponto abordado foi a importância da cooperação entre as instituições, sendo a partilha de informação um fator-chave no combate às ameaças. Observa-se também a adoção das novas tecnologias como a inteligência artificial e a aprendizagem automática, com o mesmo objetivo, e não só.

Deste modo, foi possível entender as bases e práticas necessárias para a investigação, identificando quer os atuais desafios, como as medidas prioritárias a tomar. As conclusões retiradas deste capítulo servem, assim, de ponto de partida para as análises comparativas dos modelos de referência e para a proposta de um modelo mais robusto e adaptado às necessidades do setor.

CAPÍTULO 3

Desenvolvimento do Modelo Proposto

Neste capítulo foi realizada uma análise e comparação detalhadas dos modelos de referência NIST - CSF, *Center for Internet Security* (CIS), *Payment Card Industry-Data Security Standard* (PCI-DSS) e *Society for Worldwide Interbank Financial Telecommunication* (SWIFT) *Customer Security Controls Framework* (CSCF). De seguida, foi realizada uma análise conjunta com o objetivo de agregar e complementar o modelo da NIST - CSF com requisitos dos modelos de referência anteriormente analisados, sendo o resultado um modelo mais completo e abrangente, apresentado e explicado no fim do capítulo.

3.1. Introdução

Foi utilizado, no seguimento do trabalho desenvolvido, o método *Plan, Do, Check, Act* (PDCA). É um processo cíclico, iterativo de melhoria contínua de forma a melhorar a postura de segurança das organizações. Ajuda a encontrar problemas, implementar soluções, monitorizando a eficácia das mesmas e fazendo os ajustes necessários para o melhoramento contínuo [35].

No primeiro passo do PDCA, *Plan*, que corresponde às funções Governo e Identificar, definem-se os objetivos estratégicos da organização em matéria de cibersegurança, avaliam-se os riscos, identificam-se os ativos críticos e planeiam-se as medidas de segurança com base nas melhores práticas dos quadros normativos anteriormente mencionados. Esta fase implica uma análise aprofundada dos processos existentes ou da implementação de novos, com o intuito de identificar oportunidades de melhoria. A definição clara dos resultados esperados facilita a elaboração de planos de ação eficazes e realistas. A fase de *Plan* assume-se como alicerce de uma gestão alinhada e iterativa, permitindo uma resposta eficaz, sustentada e alinhada aos objetivos organizacionais [35].

De seguida, *Do*, reflete-se nas fases Proteger, Detetar e Responder. Nesta etapa, são operacionalizadas as políticas, os procedimentos e os controlos definidos na fase anterior, sendo fundamental garantir a sua execução coerente e consistente. A implementação inicia-se, frequentemente, com mudanças de menor escala, permitindo testar a eficácia das ações e recolher dados para posterior avaliação.

A eficácia desta fase depende da capacidade da organização em aplicar os procedimentos definidos. Destaca-se também a importância da liderança e do envolvimento da gestão na concretização dos objetivos definidos previamente [35].

No que diz respeito à fase *Check*, esta assume um papel fundamental na verificação da eficácia das ações implementadas. A organização deve auditar, monitorizar e avaliar as medidas executadas na fase *Do*, verificando se os objetivos foram cumpridos e se os riscos estão efetivamente mitigados. A análise de dados recolhidos durante a execução deve transformar-se em informação auxiliar para a tomada de decisão [35].

A utilização de gráficos pode facilitar a identificação de tendências, especialmente quando o ciclo é repetido ao longo do tempo [35].

Por fim, o último passo, *Act*, representa o momento em que, com base nas conclusões da fase anterior, são implementadas ações corretivas e de melhoria, seja ajustando os controlos ou atualizando os planos e políticas ou até a redefinição de processos. Esta fase pode também ser entendida como uma fase de ajustamento, particularmente relevante após várias iterações do ciclo. A monitorização contínua das alterações permite evitar que os processos se tornem novamente ineficazes ao longo do tempo, reforçando a lógica de melhoria contínua [35].

O sucesso desta fase depende da qualidade das fases anteriores: um bom plano, uma execução eficaz e uma análise rigorosa dos dados aumentam significativamente a probabilidade de implementar mudanças eficazes [35].

Na figura 3 apresenta-se um diagrama exemplificativo do modelo PDCA.

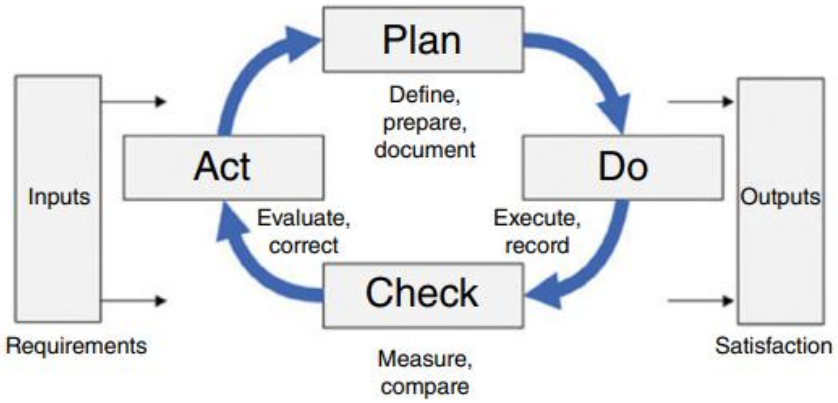


Figura 3. Modelo PDCA

3.2. Ciclo de Cibersegurança

A cibersegurança tem vindo a assumir uma importância cada vez mais reconhecida no seio dos países e organizações, das mais variadas áreas [36]. Qualquer profissional da área está consciente de que os esforços não se limitam a intervenções pontuais, mas sim a um trabalho de monitorização e proteção contínua dos ativos da organização [36].

A cibersegurança deve ser encarada como um ciclo de melhoria contínua. Começa com a identificação de riscos e vulnerabilidades nos ativos e sistemas das organizações, passando pelas fases de proteção, deteção, responder e recuperar. Quando um evento de segurança ocorre, a resposta tem de ser rápida e eficaz de forma a conter e reparar os danos o mais rapidamente possível, garantindo a continuidade de negócio [37].

É necessário aprender com os erros do passado, registar as lições aprendidas e utilizá-las de forma a prevenir e melhorar as defesas da organização. É um ciclo constante de avaliação, melhoramento e adaptação [38].

A cibersegurança deve ser pensada como um percurso e não como um destino, em que as empresas devem estar comprometidas e investir os recursos e estratégias necessárias de forma a garantir a sua própria segurança.

Na figura 4 apresenta-se um modelo representativo do ciclo da cibersegurança.

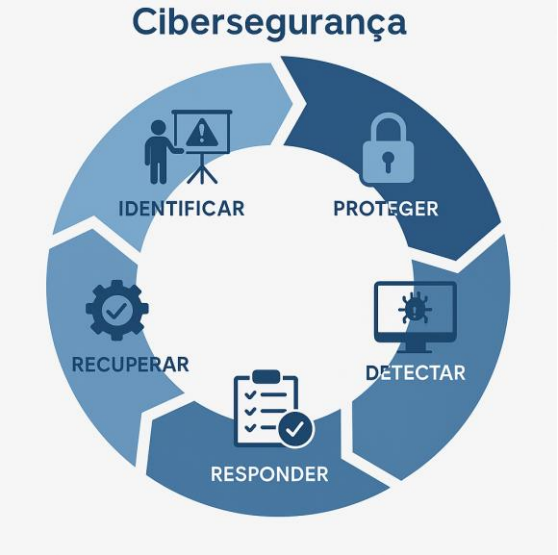


Figura 4. Ciclo Cibersegurança

3.3. Análise e comparação do modelo de referência NIST - CSF com os modelos de referência CIS, PCI-DSS e SWIFT CSCF

De seguida, apresentam-se análises sobre cada modelo de referência utilizado e as respetivas comparações com o quadro normativo da NIST - CSF.

3.3.1. NIST - CSF

É um modelo de referência desenhado para ajudar qualquer tipo de organização a reduzir os seus ciber-riscos. Não existe uma forma correta de implementação, cada organização tem riscos únicos e a mesma pode variar. É esperado que os resultados obtidos sejam entendidos por todos os colaboradores da organização, e não só pelos colaboradores da área de tecnologias da informação [37].

O modelo da NIST - CSF tem três componentes principais: núcleo CSF, perfis organizacionais e níveis. Começando pelo primeiro, é o núcleo do modelo. Os seus componentes são uma hierarquia de funções, categorias e subcategorias que detalham cada resultado [37].

Existem 5 núcleos: Governo, Identificar, Proteger, Detetar, Responder, Recuperar, como explicado anteriormente [37]. Os perfis organizacionais são um mecanismo de descrição dos níveis atuais e desejados da postura de segurança na organização [37].

Por fim, os níveis aplicam-se aos perfis acima referidos para caracterizar o rigor das práticas de gestão [37].

3.3.2. CIS

Liderados pelo CIS, estes controlos desenvolveram-se numa comunidade internacional de indivíduos e instituições voluntárias que partilham conhecimento sobre os ataques, identificam as causas principais e atuam sobre as mesmas, criam e partilham ferramentas de resolução de problemas [39]. Os controlos surgem de uma base combinada de conhecimento partilhado de especialistas de vários segmentos da indústria [39].

No desenvolvimento da nova versão, foram definidos princípios de desenho, que têm como

função relembrar o que realmente é importante. Estes princípios são:

- *Offense Informs Defense*: os controlos são selecionados e priorizados com base no comportamento do atacante;
- *Focus*: ajudar as equipas de proteção a identificar o que é mais crítico e o que devem fazer para conter o ataque;
- *Feasible*: as recomendações têm de ser práticas e implementáveis;
- *Measurable*: os controlos têm de ser mensuráveis;
- *Align*: os controlos têm de ser alinháveis com os vários quadros normativos e estruturas que estejam em vigor [39].

3.3.3. PCI-DSS

A PCI-DSS é um modelo de segurança vocacionado para as organizações que tratam informação de cartões de crédito/débito. Apresenta um conjunto de requisitos de modo que as organizações processem e armazenem os dados, aplicando as melhores práticas da indústria [40].

É gerida pelas principais organizações de cartões do mundo. Este quadro normativo foi desenhado para proteger os dados sensíveis dos cartões bancários, através de uma rede segura, da contínua gestão de vulnerabilidades, implementação de fortes medidas de controlo de acessos, da monitorização e testes regulares de rede [40].

São 3 as etapas fundamentais da PCI-DSS, avaliar, reparar e reporte. A primeira tem como objetivo identificar as localizações dos dados do titular do cartão, inventariar os ativos e processos empresariais para o processamento de cartões e analisá-los para detetar vulnerabilidades que possam expor os dados referidos [41].

A segunda etapa tem como foco a correção das vulnerabilidades anteriormente identificadas, remover dados que estejam armazenados e que já não exista necessidade para o seu armazenamento, e por fim implementar processos de negócio seguros [41].

Por fim, a última etapa, reporte, tem como objetivo documentar os pormenores da avaliação e da correção, e apresentar relatórios de conformidade às partes interessadas [41].

Este modelo aplica-se a todas as entidades que armazenam, processam ou transmitem dados do titular do cartão e/ou dados de autenticação sensíveis [40].

3.3.4. SWIFT CSCF

A SWIFT CSCF é composta por requisitos de segurança obrigatórios e aconselháveis para os utilizadores do modelo, com o objetivo de tornar o sistema financeiro mais seguro. Os primeiros requisitos devem ser implementados por todos os utilizadores nas respetivas infraestruturas. Estes requisitos são prioritários de forma a atingir um objetivo realista de curto prazo. Os aconselháveis são práticas recomendadas a todos os utilizadores [42].

Todos os controlos são articulados em torno de 3 objetivos: Proteger o ambiente, conhecer e limitar o acesso e detetar e responder [42].

O quadro normativo SWIFT CSCF é baseado na NIST - CSF, *International Organization for Standardization* (ISO) 27000 e PCI-DSS [42]. Os controlos foram desenvolvidos com base numa análise contínua da SWIFT CSCF sobre as informações relativas às ciberameaças e em conjunção com as opiniões de especialistas e utilizadores [42].

3.3.5. Comparação NIST - CSF / CIS

A NIST - CSF e a CIS apresentam várias semelhanças e diferenças entre si. Começando pelas

primeiras, em ambas, quer os requisitos, ou diretrizes, não são de implementação obrigatória, pelo que nenhuma empresa é obrigada a seguir rigorosamente estes modelos de referência. As duas têm como objetivo criar normas de segurança que qualquer organização possa utilizar e adaptar sem limitações.

Ambos os modelos de referência oferecem níveis de implementação. A NIST - CSF apresenta quatro opções possíveis para categorizar as organizações. No nível 1 estão inseridas as organizações com fracas práticas e medidas de segurança implementadas e no espectro oposto, no nível 4, estão as organizações que refletem o auge das normas de segurança.

No caso da CIS o sistema é ligeiramente diferente. Dependendo do número de controlos que a organização cumpre, de um total de 18, entra numa determinada categoria. Por exemplo, se cumprir 6 controlos significa que segue as normas básicas de segurança.

Uma vantagem da CIS é o facto de ser compatível com outras normas. Para o caso de se estar a trabalhar para cumprir as normas NIST - CSF, é possível adaptar a organização para cumprir os controlos CIS e vice-versa.

Na tabela 8 apresenta-se uma síntese comparativa entre os dois modelos.

Tabela 8. Síntese comparativa entre os modelos NIST-CSF e CIS

Aspeto	**NIST - CSF**	**CIS**
Objetivo	Ajuda qualquer tipo de organização a reduzir os ciber-riscos	Normas de segurança adaptáveis e práticas
Carácter	Fornece orientações. Opcional.	Opcional
Âmbito de aplicação	Pode ser usada por qualquer tipo de organização, independentemente do setor	Pode ser usada por qualquer tipo de organização, independentemente do setor
Flexibilidade	Estrutura flexível e adaptável às necessidades da organização	Flexível, permitindo a integração com outros quadros normativos

3.3.6. Comparação NIST - CSF / PCI-DSS

Enquanto o modelo NIST - CSF identifica resultados e atividades gerais de segurança, o quadro normativo da PCI-DSS fornece orientações específicas de segurança para ambientes de pagamentos, não sendo um o substituto do outro [43].

Existem várias diferenças entre os dois modelos, como o facto de no caso da PCI-DSS os requisitos serem obrigatórios e que as organizações devem ter em conformidade, e no caso da NIST - CSF os requisitos são opcionais. A PCI-DSS é direcionada para a implementação de controlos específicos na segurança da informação dos cartões de crédito, enquanto a NIST - CSF se foca no desenvolvimento de uma estratégia ampla de segurança, pelo que a PCI-DSS tem como foco as organizações que processam pagamentos com cartões de crédito, enquanto a NIST - CSF foi projetada para ser usada por qualquer tipo de organização.

São vários os pontos em que ambos os modelos de referência convergem, no que diz respeito à proteção de informação e das redes, à monitorização regular da postura de segurança, na revisão das estratégias de gestão, na documentação dos procedimentos e políticas de segurança, na implementação de planos de resposta a incidentes e no foco nas formações de sensibilização

para a segurança regular [44].

Na tabela 9 apresenta-se uma síntese comparativa entre os dois modelos.

Tabela 9. Síntese comparativa entre os modelos NIST-CSF e PCI-DSS

Aspeto	**NIST - CSF**	**PCI-DSS**
Objetivo	Ajudar qualquer tipo de organização a reduzir os ciber-riscos	Fornecer orientações específicas de segurança para ambientes de pagamento
Carácter	Fornece orientações. Opcional.	Obrigatório para empresas que lidam com dados de cartões de crédito
Âmbito de aplicação	Pode ser usada por qualquer tipo de organização, independentemente do setor	Direcionada para organizações que processam pagamentos com cartões de crédito
Flexibilidade	Estrutura flexível e adaptável às necessidades da organização	Estrutura rígida com requisitos específicos

3.3.7. Comparação NIST - CSF / SWIFT CSCF

Por um lado a NIST - CSF foi projetada para ser utilizada por um amplo espectro de indústrias, enquanto que o modelo de referência da SWIFT CSCF foi desenvolvido especificamente para o setor bancário, com o foco na segurança das operações financeiras e comunicações interbancárias [42]. Ao contrário da NIST - CSF, a SWIFT CSCF é de utilização exclusiva para organizações que utilizam a rede *swift*.

Outra diferença relativamente ao modelo da NIST - CSF depara-se no facto de que a SWIFT CSCF tem controlos de implementação obrigatória, e o cumprimento dos mesmos é também obrigatório para todas as instituições que fazem parte da rede SWIFT CSCF, enquanto a NIST - CSF apresenta um conjunto abrangente de controlos, sem exigência sobre uma implementação específica [42].

Na tabela 10 apresenta-se uma síntese comparativa entre os dois modelos.

Tabela 10. Síntese comparativa entre os modelos NIST-CSF e SWIFT CSCF

Aspeto	**NIST - CSF**	**SWIFT CSCF**
Objetivo	Ajudar qualquer tipo de organização a reduzir os ciber-riscos	Assegurar a segurança do ambiente financeiro
Carácter	Fornece orientações. Opcional.	Obrigatório para todas as instituições da rede SWIFT CSCF
Âmbito de aplicação	Pode ser usada por qualquer tipo de organização, independentemente do setor	Aplicável exclusivamente ao setor financeiro
Flexibilidade	Estrutura flexível e adaptável às necessidades da organização	Pouco flexível com controlos de natureza obrigatória

3.4. Exploração da NIST - CSF: Análise dos núcleos e integração com os requisitos da CIS, PCI-DSS e SWIFT CSCF

De seguida, apresenta-se a estrutura de cada núcleo da NIST - CSF, e apresentam-se os controlos escolhidos para complementar cada núcleo, integrando o modelo.

3.4.1. Núcleo: Governo

O objetivo desta fase é providenciar resultados que servem para informar o que uma organização pode fazer para alcançar e dar prioridade aos resultados dos outros núcleos.

Nesta fase, espera-se compreender e avaliar as necessidades e riscos específicos da organização e que risco a mesma está disposta a aceitar. É importante envolver os colaboradores e procurar ter o maior número de sugestões possíveis, analisando o que correu bem e menos bem, discutindo-o.

Com esta base, deve ser desenvolvida uma estratégia de risco à medida das necessidades da organização, tendo em conta as lições aprendidas [45].

Devem ser desenvolvidas políticas de gestão do risco, aprovadas e implementadas por toda a organização, tendo em conta as obrigações legais. Devem também ser desenvolvidas e comunicadas regularmente práticas de cibersegurança [45].

Têm de ser atribuídas responsabilidades aos colaboradores sobre a matéria de cibersegurança, como por exemplo quem fica encarregue de supervisionar os fornecedores, clientes e parceiros [45].

Todas estas etapas têm de ser regularmente monitorizadas e revistas [45].

Para cada função, e com o objetivo de complementar cada controlo da mesma, foram selecionados certos requisitos de cada modelo de referência, CIS, PCI-DSS e SWIFT CSCF.

Os controlos complementados estão apresentados na Tabela 11:

Tabela 11. Mapeamento dos controlos do Núcleo Governo

NIST - CSF Subcategoria	**Requisitos CIS**	**Requisitos PCI-DSS**	**Requisitos SWIFT CSCF**
GV.OC-02	-	-	SWIFT CSCF 2.8
GV.RR-02	CIS v8.0 14.1, 17.4	PCI-DSS v4: 12.10.2	-
GV.RM-01 GV.RM-06 GV.RR-03	-	PCI-DSS v3.2.1: 12.2	-
GV.RM-03 GV.PO-01	-	PCI-DSS v3.2.1: 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 11.6	-
GV.SC-07	-	PCI-DSS v4: 12.8.1, 12.8.2, 12.8.4	-

De forma a perceber os vários passos desta fase, é possível fazer um conjunto de perguntas:

- Com que regularidade está a ser feita a revisão da estratégia de cibersegurança? [46]
- Será necessário melhorar as competências dos colaboradores, contratar talento ou um parceiro externo para ajudar a organização a definir e gerir um plano de cibersegurança? [46]

- Estão implementadas políticas de aceitação? Os colaboradores estão informados sobre as mesmas? [46]

GV.OC-02: *Internal and external stakeholders are understood, and their needs and expectations regarding cybersecurity risk management are understood and considered*

Nos casos de terceirização de atividades críticas a terceiros e prestadores de serviços, é essencial assegurar que estes possuem um elevado nível de preocupação com a segurança, garantindo a sua consistência e em conformidade com os requisitos da organização. Aquando da subcontratação, os utilizadores permanecem os principais responsáveis pela conformidade com os controlos do modelo da SWIFT CSCF e devem sempre procurar a conformidade com os prestadores de serviços (Swift 2.8 Outsourced Critical Activity Protection) [42].

Quando são usados serviços partilhados por terceiros que não estão relacionados com os utilizadores SWIFT CSCF, estes devem estar registados no programa *Shared Infrastructure Programme* (SIP) ou *Alliance Lite2*. Os utilizadores continuam a ser responsáveis pela própria infraestrutura, organização e por garantir a segurança dos fluxos de dados para os fornecedores, através de mecanismos como autenticação multifator (Swift 2.8 Outsourced Critical Activity Protection) [42].

São também contratualizados *Service Level Agreements (SLA)* e *Non-disclosure agreements (NDA)* com qualquer prestador de serviços. É efetuada uma avaliação de risco ao prestador de serviços aquando da sua contratação (Swift 2.8 Outsourced Critical Activity Protection) [42].

É importante estabelecer e manter um plano de resposta a incidentes que defina as funções e responsabilidades, um plano de comunicação e requisitos de conformidade, coordenados e alinhados com os parceiros externos (CIS Controls v8.0: 17.4) [39]. Neste plano devem estar definidos os meios de comunicação (chamadas telefónicas, correio eletrónico ou cartas) (CIS Controls v8.0: 17.6) [39].

Por fim, entrevistar uma amostra dos responsáveis para verificar se entendem as políticas de segurança (PCI-DSS v3.2.1: 12.4) [40].

GV.RR-02: *Roles, responsibilities, and authorities related to cybersecurity risk management are established, communicated, understood, and enforced*

Designar uma pessoa-chave e pelo menos uma pessoa de apoio ou reserva, que tem como função gerir o processo de resposta a incidentes. A equipa de gestão é responsável pela coordenação e documentação dos esforços de resposta e recuperação de incidentes.
Se for escolhido um colaborador externo, designar pelo menos uma pessoa interna para supervisionar o trabalho efetuado. As responsabilidades devem ser revistas anualmente, ou quando ocorrerem alterações significativas (CIS Controls v8.0: 17.4) [39]. O plano de resposta a incidentes deve ser revisto e atualizado a cada 12 meses (PCI-DSS v4: 12.10.2) [40].

É necessário estabelecer um plano de sensibilização de segurança com o objetivo de educar os colaboradores neste tema. Realizar formações aquando da contratação e aos restantes colaboradores, no mínimo, anualmente, revendo a mesma também anualmente, ou quando ocorrerem alterações significativas (CIS Controls v8.0: 14.1) [39].

GV.RM-03: *Cybersecurity risk management activities and outcomes are included in enterprise risk management processes*

GV.PO-01: *Policy for managing cybersecurity risks is established based on organizational context, cybersecurity strategy, and priorities and is communicated and enforced*

Garantir que as políticas de segurança e procedimentos operacionais para gestão de *firewalls*, gerir as predefinições dos vendedores, proteção de dados do titular do cartão, encriptar as transmissões de informação dos titulares do cartão, proteção de sistemas contra *malware*, desenvolver e manter sistemas e aplicações seguras, restringir o acesso digital e físico aos dados do titular do cartão, identificação, autenticação, monitorização e testagem estão documentados (PCI-DSS v3.2.1: 1.5, 2.5, 3.7, 4.3, 5.4, 6.7, 7.3, 8.8, 9.10, 11.6) [40].

GV.RM-01: *Risk management objectives are established and agreed to by organizational stakeholders*

GV.RM-06: *A standardized method for calculating, documenting, categorizing, and prioritizing cybersecurity risks is established and communicated*

GV.RR-03: *Adequate resources are allocated commensurate with the cybersecurity risk strategy, roles, responsibilities, and policies*

Implementar processos de avaliação de risco que identifiquem ativos críticos, riscos e vulnerabilidades, culminando na elaboração de um documento formal. Este documento deve ser revisto pelo menos anualmente ou sempre que ocorram mudanças significativas (PCI-DSS v3.2.1: 12.2) [40].

GV.SC-07: *The risks posed by a supplier, their products and services, and other third parties are understood, recorded, prioritized, assessed, responded to, and monitored over the course of the relationship*

É mantida uma lista com todos os prestadores de serviços com os quais existe partilha de dados. Nos acordos com os prestadores de serviços deve estar definido que estes são responsáveis pela segurança dos dados que possuem, processam ou transmitem. O estado de conformidade de cada provedor de serviços deve ser revisto, pelo menos, a cada 12 meses (PCI-DSS v4: 12.8.1, 12.8.2, 12.8.4) [40].

3.4.2. Núcleo: Identificar

É nesta fase que é feita a avaliação e averiguação, com base nos inventários de ativos, como sistemas, *hardware* ou *software*, nos fornecedores e riscos que a organização detém, de maneira a perceber quais são indispensáveis para o bom funcionamento da mesma. Desta forma, é possível fazer um planeamento de maneira a priorizar os recursos de acordo com a estratégia e objetivos [45].

É fundamental documentar que tipo de informação a empresa guarda e de que forma é utilizada, especialmente quando envolve entidades externas [45].

Está também incluído nesta fase a identificação de oportunidades de melhoria em todos os espectros da organização. No caso de ocorrência de um evento de segurança, é fundamental perceber e aprender com o mesmo, de forma a garantir a continuidade de negócio, registando o evento e que medidas foram tomadas na sua resolução [45].

Por fim, é crucial existirem canais simples e diretos de comunicação com os colaboradores da

organização, de forma a transmitir as melhores práticas, planos, políticas, riscos, ameaças e as formas de atuação [45].

De forma a perceber os vários passos desta fase, é possível fazer um conjunto de perguntas:

- Quais os ativos críticos? [46]
- Que riscos estão associados a cada ativo? [46]
- Quais os softwares/tecnologias que os colaboradores utilizam? Estes estão aprovados? [46]

De seguida, na tabela 12, apresenta-se o mapeamento dos requisitos do núcleo Identificar da NIST - CSF que foram complementados com os requisitos dos restantes quadros normativos.

Tabela 12. Mapeamento dos controlos do Núcleo Identificar

NIST - CSF Sub-categoria	**Requisitos CIS**	**Requisitos PCI-DSS**	**Requisitos SWIFT CSCF**
ID.AM-02	CIS v8.0: 1.1, 2.2	PCI-DSS 2.4b, 9.9.1.b	-
ID.AM-04	CIS v8.0: 12.4, 15.1	-	-
ID.AM-05	CIS v8.0: 3.7	-	-
ID.AM-08	CIS v8.0: 1.1, 3.1, 13.5	PCI-DSS v4: 3.2.1, 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 9.4.6, 12.3.8, 12.3.9	-
ID.RA-01	CIS v8.0: 18.2, 18.3	-	SWIFT CSCF 2.7, 7.3A
ID.RA-06	-	PCI-DSS v4: 6.3.1	-
ID.RA-08	-	PCI-DSS v4: 6.3.1	-
ID.RA-09	-	PCI-DSS v4: 9.5.1.2	-
ID.RA-04, ID-RA-05	-	PCI-DSS v3.2.1: 6.1	-
ID.IM-04	-	PCI-DSS v3.2.1: 12.10.6	-

ID.AM-02: *Inventories of software, services, and systems managed by the organization are maintained*

Neste controlo são criados e mantidos inventários para os *softwares* e serviços da organização.

Assegurar que todo o *software* utilizado na organização está documentado e registado como autorizado no inventário de ativos. Os ativos que não estejam sob o controlo da organização, mas que conectam regularmente à infraestrutura de rede também fazem parte deste inventário (CIS Controls v8.0: 1.1) [39].

Se o *software* não for suportado, mas for necessário para as atividades da empresa, é preciso definir uma exceção detalhada. Para quaisquer outros *softwares* não suportados, estes devem ser designados como não autorizados. Rever o inventário pelo menos mensalmente (CIS Controls v8.0: 2.2) [39].

Devem-se entrevistar as pessoas responsáveis pelos inventários de forma a garantir a constante atualização dos mesmos (PCI-DSS 2.4b) [40]. É importante também retirar uma amostra do inventário e observar caso a caso se realmente se encontram atualizados (PCI-DSS 9.9.1.b) [40].

ID.AM-04: *Inventories of services provided by suppliers are maintained*

Os inventários providenciados pelos fornecedores são guardados. Neste inventário devem estar listados todos os fornecedores de serviços conhecidos, incluindo classificação, designação da organização e respetivos contactos. Definir e manter um diagrama de arquitetura ou outros esquemas de sistema na documentação. Efetuar uma revisão deste esquema pelo menos anualmente, ou sempre que ocorram mudanças significativas (CIS Controls v8.0: 12.4, 15.1) [39].

ID.AM-05: *Assets are prioritized based on classification, criticality, resources, and impact on the mission*

Neste controlo é feita a priorização dos ativos. Estabelecer e manter um esquema global de classificação na organização. As organizações podem definir os processos de etiquetagem e classificar a informação de acordo com estes processos. É fundamental a revisão deste esquema pelo menos anualmente, ou sempre que ocorram mudanças significativas (CIS Controls v8.0: 3.7) [39].

ID.AM-08: *Systems, hardware, software, services, and data are managed throughout their life cycles*

Periodicamente analisar os sistemas, *hardware* e *software* de modo a averiguar uma possível redundância.

O acesso aos ativos da organização, aquando de ligações remotas aos recursos da empresa, tem de ser gerido.

Deve estar definido, para os casos de necessidade, autenticação remota para os prestadores de serviços e parceiros, sendo esta imediatamente desativada após a utilização. Estas sessões devem ter um período máximo até a sessão ser terminada (PCI-DSS v4: 12.3.8, 12.3.9) [40].

Estabelecer e manter um inventário detalhado e atualizado de todos os ativos da organização que possam potencialmente armazenar ou processar dados. Assegurar que o inventário guarda os endereços de rede, endereços do *hardware*, nome da máquina e responsável pela mesma, o respetivo departamento da máquina e se foi aprovada para se conectar à rede. Este inventário inclui qualquer dispositivo, físico ou virtual, que se conecte à infraestrutura de rede. Rever anualmente ou sempre que ocorram mudanças significativas (CIS Controls v8.0: 1.1) [39].

Definir um processo de gestão de dados, em que é estabelecido o responsável, de que forma os dados são tratados e eliminados, e os períodos máximos de retenção dos mesmos. Rever anualmente ou sempre que ocorram mudanças significativas (CIS Controls v8.0: 3.1) [39].

Determinar a quantidade de acesso aos recursos da organização com base no *software* anti *malware* instalado, conformidade das configurações e garantia de atualização das aplicações e sistema operativo (CIS Controls v8.0: 13.5) [39].

Todos os dispositivos que armazenam dados dos titulares dos cartões e as respetivas cópias de segurança estão fisicamente seguros, e são revistos a cada 12 meses. É feita uma classificação dos dados de acordo com a respetiva sensibilidade (PCI-DSS v4: 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2) [40].

O armazenamento dos dados das contas é minimizado durante a implementação, em conformidade com as políticas de retenção e eliminação de dados. Deve estar incluída todas as localizações do armazenamento e a cobertura de todos os dados de autenticação sensíveis. Quer o espaço como o tempo de armazenamento devem ser limitados. Os requisitos para a retenção

de dados têm de ser especificados, como a justificação e período, assim como processos para uma remoção segura e um período de revisão e verificação dos dados, pelo menos a cada 3 meses (PCI-DSS v4: 3.2.1) [40].

Os materiais que tenham informação dos titulares do cartão devem ser cortados, incinerados ou qualquer outra forma que impeça que sejam reconstruídos (PCI-DSS v4: 9.4.6) [40].

ID.RA-01: *Vulnerabilities in assets are identified, validated, and recorded*

Executar análises de vulnerabilidades pelo menos anualmente, ou sempre que ocorram mudanças significativas, utilizando ferramentas de análise dos fornecedores, tendo sempre em atenção o possível impacto de execução das análises, tentando que tenha o mínimo impacto possível e documentando os resultados obtidos (Swift 2.7 Vulnerability Scanning) (CIS Controls v8.0: 18.2) [42] [39].

Formalizar testes de intrusão com o objetivo de validar a segurança operacional e identificar falhas de defesa, no mínimo a cada 2 anos, ou sempre que ocorrerem mudanças significativas no ambiente. Deve ser previamente planeado para evitar falhas de disponibilidade ou integridade, e executado por colaboradores experientes e independentes da equipa. Deve ser executado em ambiente de produção e o resultado ser documentado (Swift 7.3A Penetration Testing) [42].

As medidas de segurança devem ser validadas após cada teste de penetração e, caso necessário, as regras devem ser alteradas para detetar as técnicas usadas durante os testes [39] (CIS Controls v8.0: 18.3).

ID.RA-06: *Risk responses are chosen, prioritized, planned, tracked, and communicated*

As vulnerabilidades são identificadas e geridas através de fontes de informação sobre vulnerabilidades de segurança reconhecidas pelo setor, incluindo alertas de equipas internacionais e nacionais de resposta a emergências CERT (PCI-DSS v4: 6.3.1) [40]. É atribuída uma classificação às vulnerabilidades baseada nas melhores práticas e no potencial impacto.

ID.RA-08: *Processes for receiving, analyzing, and responding to vulnerability disclosures are established*

As novas vulnerabilidades são identificadas utilizando fontes reconhecidas pela indústria, incluindo alertas das equipas CERT (PCI-DSS v4: 6.3.1) [40].

ID.RA-09: *The authenticity and integrity of hardware and software are assessed prior to acquisition and use*

Inspecionar periodicamente dispositivos para detetar possíveis adulterações ou substituições de dados não autorizadas (PCI-DSS v4: 9.5.1.2) [40].

ID.RA-01, **ID.RA-03**: *Threats, both internal and external, are identified and documented*, **ID.RA-04:** *Potential business impacts and likelihoods are identified*, **ID.RA-05:** *Threats, vulnerabilities, likelihoods, and impacts are used to determine risk*, **ID.RA-06**

Avaliar o risco da organização baseado num cenário plausível de um ataque cibernético, de forma a testar e melhorar a preparação na resposta a incidentes e melhorar a maturidade do programa de segurança da organização. Inclui *cyber wargames* e ataques de teste nos sistemas, exercícios técnicos e de gestão.

Com base nos resultados, é possível identificar áreas de risco e medidas futuras.

A avaliação de conformidade tem como principais objetivos identificar possíveis métodos que os atacantes consigam explorar, analisar a eficácia dos métodos de prevenção e deteção existentes, a probabilidade e impacto de um ataque e identificar a necessidade de controlos de deteção e prevenção.

Deve ser implementado um processo de identificação de vulnerabilidades de segurança utilizando fontes externas reputadas, atribuindo uma classificação de risco ("Elevado, Médio, Baixo", por exemplo) (PCI-DSS v3.2.1: 6.1) [40].

ID.IM-04: *Incident response plans and other cybersecurity plans that affect operations are established, communicated, maintained, and improved*

Verificar que estão implementados processos de modificação e atualização do plano de resposta a incidentes, com base nas lições aprendidas (PCI-DSS v3.2.1: 12.10.6) [40].

3.4.3. Núcleo: Proteger

Nesta etapa, após a identificação e priorização dos ativos e os respetivos riscos, implementam-se medidas de suporte à segurança de cada ativo, com o objetivo de diminuir a probabilidade de ocorrência de eventos de segurança e mitigar os impactos adjacentes [45].

Estão incluídas nesta fase a gestão de identidades, autenticação e controlo de acessos, sensibilização e formação, segurança dos dados e das plataformas (*hardware*, *software* e serviços das plataformas físicas e virtuais), e resiliência das infraestruturas tecnológicas [45].

A cada colaborador é atribuída uma conta única, garantindo que estes têm apenas acesso aos recursos estritamente necessários para o desempenho das suas funções [45].

Os colaboradores necessitam de formação de modo a ficarem consciencializados dos procedimentos e políticas internas para realizarem as tarefas corretamente, e reconhecer atividades suspeitas, bem como reagir às mesmas [45].

Nesta fase é também fundamental proteger e monitorizar os dispositivos, através de serviços *endpoint*. Generalizar configurações de segurança para os dispositivos necessários e descontinuar os que não sejam essenciais para as necessidades das organizações. Devem ser mantidos registos de atividades, através da instalação de um sistema dedicado para tal [45].

É imprescindível a proteção dos dados sensíveis, como na transmissão e transferência destes, através de canais encriptados e aplicar verificações de integridade, para detetar e evitar alterações aos mesmos [45].

É também importante realçar a necessidade de gestão do *software*, atualizando sempre que possível os sistemas operativos e aplicações, e efetuar regularmente cópias de segurança dos dados, garantindo o seu correto armazenamento (uma cópia armazenada *ofline*). Estas cópias devem ser testadas regularmente [45].

De forma a perceber os vários passos desta fase, é possível fazer um conjunto de perguntas:

• Estão a ser dados apenas os acessos e privilégios necessários para o desempenho de cada função [46]?

• Estes acessos são eliminados quando deixa de haver necessidade [46]?

• Os colaboradores têm conhecimento e competências necessárias para desempenharem as funções, garantindo a segurança [46]?

De seguida, apresenta-se, na tabela 13, o mapeamento dos requisitos do núcleo Proteger da NIST - CSF que foram complementados com os requisitos dos restantes modelos de referência:

Tabela 13. Mapeamento dos controlos do Núcleo Proteger

NIST - CSF Sub-categoria	**Requisitos CIS**	**Requisitos PCI-DSS**	**Requisitos SWIFT CSCF**
PR.AA-01	-	PCI-DSS v4: 2.2, 8.2.2	SWIFT CSCF 4.1, 5.4
PR.AA-03	CIS v8.0: 12.3, 12.6	PCI-DSS v4: 3.4.2, 8.3.1, 8.3.2, 8.3.4, 8.3.7, 8.4.3	-
PR.AA-05	CIS v8.0: 3.7, 5.6, 6.8	PCI-DSS v4: 2.2, 6.5.4, 7.2.6, 8.2.2	SWIFT CSCF 1.1, 2.9, 2.11A, 5.1
PR.AA-06	-	PCI-DSS v4: 9.3.2, 9.3.4	SWIFT CSCF 3.1
PR.AT-01	CIS v8.0: 15.4, 17.4	PCI-DSS v4.0: 12.1.3, 12.6.1, 12.6.2, 12.8.2, 12.10.4	-
PR.AT-02	CIS v8.0: 14.9	-	-
PR.IR-01	-	PCI-DSS v4: 1.2.3, 1.2.4, 1.4.1, 1.4.2, 1.4.4, 6.5.3, 6.5.4, 6.5.6	SWIFT CSCF 1.1, 1.4
PR.DS	CIS v8.0: 3.4	-	-
PR.DS-01	-	PCI-DSS v4: 3.4.2, 3.5.1, 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 12.10.1	-
PR.DS-02	CIS v8.0: 9.5	PCI-DSS v4:4.2.1, 4.2.1.1	SWIFT CSCF 2.4, 2.5A, 2.6
PR.DS-10	CIS v8.0: 3.6	-	-
PR.DS-11	-	PCI-DSS v4: 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 12.10.1	-
PR.PS-01	CIS v8.0: 4.3, 4.10, 12.1	-	SWIFT CSCF 2.3
PR.PS-03	CIS v8.0: 7.3	-	-
PR.PS-04	CIS v8.0: 8.1, 8.3, 8.9	PCI-DSS v4: 10.2.1.1, 10.2.1.4	SWIFT CSCF 6.4

PR.PS-06	CIS v8.0: 4.4, 4.5, 4.12, 16.13	PCI-DSS v4: 6.5.1	-

PR.AA-01: *Identities and credentials for authorized users, services, and hardware are managed by the organization*

As palavras-passe são guardadas numa localização segura, com acesso restrito, sendo que as escritas em meios físicos são guardadas em cofres e dentro de envelopes selados, enquanto as digitais são guardadas através de encriptação. Se um acesso de emergência for concedido a um operador que normalmente não teria acesso, a palavra-passe fornecida é alterada imediatamente após a intervenção (Swift 5.4 Password Repository Protection) [42].

Implementar políticas de palavras-chave com os seguintes parâmetros: Data de expiração, tamanho, composição, complexidade, negar a possibilidade de reutilização, bloqueio após número definido de tentativas, combinar com um segundo fator de autenticação (Swift 4.1 Password Policy) [42].

Ter em especial atenção as restrições do ambiente utilizado aquando da definição destas regras, a política de palavras-passe é aplicada através de meios técnicos como *Active Directory*. Esta deve ser revista anualmente e garantir que as credenciais utilizadas nas zonas seguras são armazenadas nas mesmas (Swift 4.1 Password Policy) [42].

Deve ser testado o acesso às contas predefinidas por parte dos vendedores, de forma a se assegurar que foram realmente alteradas. Casos em que as contas padrões não sejam utilizadas, as mesmas devem ser removidas ou desabilitadas (PCI-DSS v4: 2.2) [40].

Para o caso de contas de grupo, compartilhadas ou genéricas, devem-se evitar ao máximo a sua utilização, a justificativa para o negócio é documentada e aprovada pela administração e a identidade do usuário é confirmada antes que o acesso à conta seja concedido, sendo cada ação realizada atribuível a um usuário individual (PCI-DSS v4: 8.2.2) [40].

PR.AA-03: *Users, services, and hardware are authenticated*

O acesso aos componentes do sistema é autenticado por pelo menos dois dos seguintes fatores de autenticação: Algo que conhece (palavra-passe), algo que possui, como um *token*, e algo que é (elemento biométrico) (PCI-DSS v4: 8.3.1) [40]. Deve ser usada criptografia para proteger todos os fatores de autenticação ilegíveis durante a transmissão e armazenamento no sistema (PCI-DSS v4: 8.3.2) [40].

É importante que esteja implementado um limite de tentativas de autenticação, por exemplo, dez vezes, e um bloqueio temporal, por exemplo, trinta minutos (PCI-DSS v4: 8.3.4) [40]. Outra medida fundamental consiste em assegurar que as palavras-passe não possam ser reutilizadas (PCI-DSS v4: 8.3.7) [40].

As palavras-passe dos ativos da organização devem ser sempre únicas, com um mínimo de 8 caracteres para contas com autenticação multifator e 14 caracteres para contas sem autenticação multifator (CIS Controls V8.0: 5.2) [39].

A segurança da infraestrutura de rede da organização deve ser assegurada, utilizando protocolos de rede como *Hyper Text Transfer Protocol Secure* (HTTPS) e *Secure Shell* (SSH), e através de ***version-controlled-infrastructure-as-code*** , que é um sistema de auxílio de modo a conseguir monitorizar as alterações efetuadas no código (CIS Controls v8.0: 12.3) [39].

Devem também ser usados protocolos de comunicação seguros como *802.1X* ou *Wi-Fi Protected Access 2* (WPA2) (CIS Controls v8.0: 12.6) [39].

Todos os acessos remotos têm obrigatoriamente de ter autenticação multifator.

O *Primary Account Number* (PAN), através de controlos técnicos, não pode ser modificado, copiado nem realocado (PCI-DSS v4: 3.4.2, 8.4.3) [40].

PR.AA-05: *Access permissions, entitlements, and authorizations are defined in a policy, managed, enforced, and reviewed, and incorporate the principles of least privilege and separation of duties*

A gestão das contas de utilizadores deve ser centralizada, através de um diretório ou serviço próprios (CIS Controls v8.0: 5.6) [39].

Implementar deteção transacional, prevenção e validação de controlos de forma a garantir que não ocorrem transações fora do período expectável, por exemplo, limitar tráfego fora de horas laborais, considerar a restrição de transações *swift* fora de horas, sendo preciso submissão e aprovação nos períodos fora de horário laboral, utilizar sessões *Financial Information Network* (FIN) ativas com o mecanismo automático de encerramento das sessões após o término do período laboral, e restringir transações *swift* com base nos limites definidos por utilizador (Swift 2.9 Transaction Business Controls) [42].

Colocar em prática controlos *Relationship Management Application* (RMA) para restringir transações a entidades efetivas. É feita uma análise de relações comerciais efetivas, o RMA é um mecanismo para evitar tráfego indesejado num serviço, controlando quem pode enviar tráfego e o tipo de mensagens que são aceites (Swift 2.11A RMA Business Controls) [42].

Realizar validações sistemáticas, por exemplo ao final de cada dia, de um conjunto de parâmetros como verificar quaisquer mensagens de confirmação, registos contabilísticos com mensagens de extrato, mensagens que são enviadas da organização para a rede *swift* e vice-versa, e verificar pagamentos efetuados (Swift 2.9 Transaction Business Controls) [42].

Deve ser testado o acesso às contas predefinidas pelos vendedores, de forma a se assegurar que foram realmente alteradas e detetar casos que possam ter escapado, e casos em que as contas padrões não sejam utilizadas, as mesmas devem ser removidas ou desativadas (PCI-DSS v4: 2.2) [40].

Todas as permissões de acessos têm de estar definidas na política da organização. É necessário rever as permissões regularmente, para tratar casos de saídas de colaboradores, por exemplo, forçando o princípio do mínimo acesso (CIS Controls v8.0: 3.7, 6.8) [39].

É essencial aplicar os princípios de necessidade de saber, privilégio mínimo e segregação de funções. No que diz respeito ao primeiro princípio, apenas os operadores com razões válidas têm acesso à informação, ficheiros e recursos necessários para desempenhar as suas funções. Para o segundo, os colaboradores têm apenas os privilégios estritamente necessários para o desempenho das suas tarefas. No último princípio, existe uma separação de funções, onde as mais sensíveis não podem ser desempenhadas pelos mesmos colaboradores (Swift 5.1 Logical Access Control) [42].

O acesso a contas de nível administrativo deve ser o mais restrito possível, pelo que a utilização das mesmas deve ser controlada, monitorizada e apenas permitida na necessidade de operações relevantes, como instalações e configurações de software (Swift Environment Protection 1.1) [42].

O acesso do utilizador a bases de dados com informação dos titulares do cartão é restrito, com base nas funções e privilégios de cada utilizador (PCI-DSS v4: 7.2.6) [40]. Para o caso de contas de grupo, compartilhadas ou genéricas, devem-se evitar ao máximo a sua utilização e recomenda-se a definição de tempo limite. A justificativa para o negócio é documentada e aprovada pela administração, a identidade do usuário é confirmada antes que o acesso à conta seja concedido, sendo cada ação realizada atribuível a um usuário individual (PCI-DSS v4: 8.2.2) [40].

As funções são separadas entre os ambientes de produção e pré-produção, de modo que apenas as mudanças revistas sejam implementadas (PCI-DSS v4: 6.5.4) [40].

PR.AA-06: *Physical access to assets is managed, monitored, and enforced commensurate with risk*

Garantir a segurança de equipamento removível, sendo estes sempre supervisionados e seguramente armazenados num espaço trancado. Garantir que apenas pessoal autorizado acede aos computadores operacionais.

No que diz respeito ao trabalho remoto, é expectável que os seguintes parâmetros sejam seguidos: segurança física do ambiente de trabalho, computadores pessoais não possam aceder às infraestruturas da organização, garantir as condições de segurança em transportes públicos e privados, que familiares e amigos não consigam aceder aos equipamentos, e por fim a proteção dos equipamentos móveis de palavras-passe de utilização única.

Os servidores estão instalados em espaços bloqueados com controlo de acesso. Utilizar serviços de vídeo-vigilância nesses mesmos espaços, com sensores de movimento.

Assegurar a correta eliminação de dados dos equipamentos quando forem destruídos ou reutilizados.

No que respeita aos acessos por parte de visitantes, estes têm de ser autorizados previamente, sempre acompanhados e claramente identificados, por exemplo, utilizando um crachá (PCI-DSS v4: 9.3.2) [40]. Deve ser mantido um registo de visitantes, com o nome e a organização representada, a data e hora da visita e o nome de quem concedeu o acesso. Esta lista deve ser mantida por pelo menos 3 meses (PCI-DSS v4: 9.3.4) [40].

Por fim, os acessos físicos são registados e revistos, estando disponíveis para serem auditados e usados em investigações, sendo mantidos por um período mínimo de 12 meses. Os acessos físicos são revistos anualmente (Swift 3.1 Physical Security) [42].

PR.AT-01: *Personnel are provided with awareness and training so that they possess the knowledge and skills to perform general tasks with cybersecurity risks in mind*

Deve estar implementado um plano de treino e consciencialização para a segurança, que deve ser revisto e atualizado a cada 12 meses (PCI-DSS v4.0: 12.6.1, 12.6.2) [40].

Definir e manter um plano de resposta a incidentes onde estejam explícitas as funções e responsabilidades dos colaboradores da organização, os requisitos de conformidade e um plano de comunicação. Rever anualmente ou sempre que ocorram mudanças significativas (CIS Controls v8.0: 17.4) [39].

Garantir que é definido no contrato, com os fornecedores de serviços, a inclusão de requisitos de segurança, como, por exemplo, a notificação em caso de incidentes de segurança, requisitos de encriptação de dados e a eliminação correta dos mesmos. É também fundamental garantir que estes requisitos estão alinhados com a política de gestão do prestador de serviços. Efetuar uma revisão anual (CIS Controls v8.0: 15.4) [39].

Os prestadores de serviços, os quadros superiores da organização e os colaboradores da área de segurança física entendem e aceitam as suas funções e responsabilidades (PCI-DSS: v4: 12.1.3, 12.8.2) [40].

Os colaboradores responsáveis pela resposta a incidentes de segurança recebem formação adequada e periódica sobre as suas responsabilidades (PCI-DSS v4: 12.10.4) [40].

PR.AT-02: *Individuals in specialized roles are provided with awareness and training so that they possess the knowledge and skills to perform relevant tasks with cybersecurity risks in mind*

Levar a cabo treinamento específico com base na função do utilizador, implementando cursos de gestão segura de sistemas de administração, como o *Open Web Application Security Project* (OWASP) Top 10, por exemplo (CIS Controls v8.0: 14.9) [39].

PR.IR-01: *Networks and environments are protected from unauthorized logical access and usage*

As palavras-passe e outros métodos de autenticação que são utilizados dentro da zona segura (segmentação) não são guardados nem usados fora da zona segura. Esta é adequadamente delimitada ao ambiente de cada utilizador. Os componentes dentro da zona segura são todos protegidos ao mesmo nível de segurança.

Todos os sistemas, softwares e serviços dentro da zona segura são avaliados quanto à necessidade e removidos da zona se não suportarem as operações.

As *firewalls* da camada de transporte criam separações lógicas nas zonas seguras. As listas de controlo de acessos adicionam uma camada extra de proteção. Conexões de entrada e saída para a zona segura são minimizadas e geridas por regras de *firewall*. Não podem existir regras de permissão absoluta, os fluxos de rede são explicitamente autorizados e a conectividade entre os limites da zona segura é geralmente restrita às comunicações bidirecionais. As regras de *firewall* são revistas anualmente.

Os acessos às zonas seguras são efetuados de diversas formas: Através de um computador localizado dentro da zona segura, através de uma máquina de salto, pelos próprios computadores, apenas conseguindo aceder a certas interfaces, ou através de conexões remotas (Swift Environment Protection 1.1) [42].

Todos os computadores dedicados, assim como os sistemas dentro da zona segura, têm o acesso à internet controlado, não sendo permitido o acesso para fins gerais, nem para o servidor de salto.

O acesso é permitido pelos computadores gerais para os casos de acesso a uma aplicação do prestador de serviços ou agentes (Swift Environment Protection 1.4) [42].

Os ambientes de pré-produção e produção são controlados através de controlo de acessos. Também as funções e responsabilidades estão separadas entre os ambientes, de forma que

apenas as mudanças revistas e aprovadas sejam implementadas. As contas e dados de teste devem ser removidos antes de o sistema entrar em produção (PCI-DSS v4: 6.5.3, 6.5.4, 6.5.6) [40].

Deve estar desenhado e implementado um diagrama da arquitetura de rede, de forma a evitar que as ligações e dispositivos sejam "esquecidos", e inadvertidamente, inseguros e vulneráveis. No mesmo âmbito, deve estar desenhado um diagrama de fluxo de dados, de forma que a organização perceba como os dados fluem através das redes e entre os sistemas, evitando que dados das contas sejam negligenciados e deixados sem as devidas medidas de segurança (PCI-DSS v4: 1.2.3, 1.2.4) [40].

As conexões entre redes confiáveis e não confiáveis são controladas, o tráfego de entrada vindo de redes não confiáveis é restrito, e os componentes do sistema que tenham dados dos titulares dos cartões não estão em contacto direto com redes não confiáveis (PCI-DSS v4: 1.4.1, 1.4.2, 1.4.4) [40].

PR.DS: *Data are managed consistent with the organization's risk strategy to protect the confidentiality, integrity, and availability of information*

Deve estar definido um período mínimo e máximo no que diz respeito à retenção de dados (CIS Controls v8.0: 3.4) [39].

PR.DS-01: *The confidentiality, integrity, and availability of data-at-rest are protected*

O PAN está seguro em qualquer lugar que esteja armazenado, sendo tornado ilegível através de *hashes* unidirecionais baseados em criptografia, truncamento e *index tokens* (PCI-DSS v4: 3.5.1) [40]. Todos os dispositivos que armazenam dados dos titulares dos cartões e cópias de segurança estão fisicamente seguros, e são revistos a cada 12 meses. É feita uma classificação dos dados de acordo com a respetiva sensibilidade.

Deve estar também definido no plano de resposta a incidentes os processos a realizar para o caso das cópias de segurança (PCI-DSS v4: 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 12.10.1) [40]. Se for utilizado acesso remoto, devem estar implementadas tecnologias que impeçam a cópia e realocação do PAN, exceto exceções devidamente autorizadas (PCI-DSS v4: 3.4.2) [40].

PR.DS-02: *The confidentiality, integrity, and availability of data-in-transit are protected*

Existem bastantes métodos de proteção de dados essenciais para assegurar a continuidade de negócio da organização, tais como proteção ponto a ponto, um mecanismo que assegura a autenticação, integridade e confidencialidade dos dados a nível aplicacional, *transitive protection*, que é um protocolo seguro de troca entre os componentes do sistema e os servidores, aplicando controlos da SWIFT CSCF nos servidores, e proteger conexões diretas entre os servidores e os *back office hops*.

Implementação faseada é recomendada, o foco da primeira fase é relativamente à proteção dos fluxos ponto a ponto e aos servidores que armazenam os dados. Na segunda fase, os fluxos antigos serão protegidos de forma semelhante (Swift 2.4 A Back Office Data Flow Security) [42].

É fundamental que a informação que sai da zona segura seja protegida quando guardada fora da mesma, e a sua encriptação quando está em transmissão.

Algumas formas de proteção incluem: Encriptação de cópias de segurança e dados em repouso, autorização devidamente apropriada e controlos de acesso.

No que diz respeito aos serviços *cloud*, é necessário garantir a encriptação dos dados. Usar protocolos de encriptação que usem algoritmos aceites e atualizados, como o *Advanced Encryption Standard* (AES) ou *Elliptic Curve Diffie-Hellman Ephemeral* (ECDHE), em conformidade com as melhores práticas e com a legislação. No caso de ter havido uma falha de segurança, deve estar definido um processo de aplicação de nova criptografia e destruição de cópias de dados comprometidas (Swift 2.5 A External Transmission Data Protection) [42].

É necessário garantir a confidencialidade e integridade das sessões operativas que se conectam remotamente às instalações físicas. Deste modo, todas as sessões devem ser protegidas por protocolos de criptografia, como SSH e HTTPS com *one-way tls*, que usam algoritmos atualmente aceites e atualizados, como o AES ou ECDHE, que estejam em conformidade com as melhores práticas, implementar períodos de auto-bloqueio, e a comunicação entre o servidor de salto e o dispositivo deve ser protegida usando os protocolos anteriormente mencionados (Swift 2.6 Operator Session Confidentiality and Integrity) [42].

É recomendada a implementação de uma política *Domain-based Message Authentication, Reporting and Conformance* (DMARC), para reduzir as probabilidades de obtenção e alteração de *e-mails*, começando por implementar normas como *Sender Policy Framework* (SPF) e *DomainKeys Identified Mail* (DKIM) (CIS Controls v8.0: 9.5) [39].

No caso de dados como o PAN, em transmissão, é necessário implementar criptografia. Apenas chaves e certificados confiáveis são aceites. Os protocolos em utilização só suportam versões seguras. Deve ser mantido um inventário de todas as chaves e certificados usados durante a transmissão (PCI-DSS v4:4.2.1, 4.2.1.1) [40].

PR.DS-10: *The confidentiality, integrity, and availability of data-in-use are protected*

A informação deve estar encriptada nos dispositivos dos utilizadores, através de softwares como *Windows BitLocker, Apple FileVault* ou *Linux dm-crypt* (CIS Controls v8.0: 3.6) [39].

PR.DS-11: *Backups of data are created, protected, maintained, and tested*

Todos os dispositivos que armazenam dados dos titulares dos cartões e cópias de segurança estão fisicamente seguros, e são revistos a cada 12 meses. É feita uma classificação dos dados de acordo com a respetiva sensibilidade. Deve estar também definido no plano de resposta a incidentes os processos a realizar para o caso das cópias de segurança (PCI-DSS v4: 9.4.1, 9.4.1.1, 9.4.1.2, 9.4.2, 12.10.1) [40].

PR.PS-01: *Configuration management practices are established and applied*

Implementar o bloqueio automático da sessão em todos os ativos da organização após um período de inatividade. Para dispositivos de uso geral, o período não deve exceder 15 minutos, enquanto para dispositivos móveis de utilizador final, o período não deve exceder 2 minutos.

Deve estar implementado um número máximo de tentativas de autenticação falhadas. Para os computadores portáteis, não devem ser permitidas mais de vinte tentativas, para telemóveis e *tablets* não devem ser permitidas mais de dez (CIS Controls v8.0: 4.3, 4.10) [39].

No processo de endurecimento devem estar incluídos os seguintes parâmetros: Mudar as palavras-chave pré-definidas, desabilitar ou remover contas, *software*, serviços e portas desnecessárias, restringir acesso nas portas físicas, desabilitando-as o máximo possível, e definir tempos de auto-bloqueio. É necessário para manter os sistemas seguros revisões regulares, 2 vezes ao ano, dos sistemas para identificar ações corretivas (Swift CSCF 2.3) [42].

Por fim, garantir que a infraestrutura de rede está e é mantida atualizada. Rever as versões disponíveis pelo menos mensalmente (CIS Controls v8.0: 12.1) [39].

PR.PS-03: *Hardware is maintained, replaced, and removed commensurate with risk*

Devem ser feitas atualizações regulares do sistema operativo nos ativos da organização através da gestão automatizada de correções e atualizações, pelo menos mensalmente (CIS Controls v8.0: 7.3) [39].

PR.PS-04: *Log records are generated and made available for continuous monitoring*

Deve estar implementado um processo de gestão de registos, onde estejam definidos os requisitos para os mesmos. Abordar pelo menos a recolha, revisão e retenção dos registos. Esta documentação deve ser realizada no mínimo anualmente ou sempre que ocorrerem mudanças significativas na organização (CIS Controls v8.0: 8.1) [39]. Assegurar que existe espaço suficiente para cumprir o processo de gestão dos registos (CIS Controls v8.0: 8.3) [39]. Estes devem estar o mais centralizados possível.

Após serem gerados os registos, estes têm de ser analisados. Devem estar implementados processos de identificação de atividades suspeitas de autenticação nos sistemas operativos dentro das zonas seguras, e registar igualmente estas atividades (PCI-DSS v4: 10.2.1.4) [40]. Devem estar implementados processos de monitorização para revisão do servidor, aplicações, bases de dados e rede, todos acompanhados de alertas. Atividade suspeita é reportada (Swift 6.4 Logging and Monitoring) [42].

Os registos de comunicações e mensagens são retidos por um período mínimo de 12 meses, e estão devidamente protegidos. Registos dos computadores operacionais, *firewalls* e bases de dados são mantidos por pelo menos 31 dias. Registos de auditoria identificados noutros componentes são mantidos por pelo menos 12 meses (Swift 6.4 Logging and Monitoring) [42].

Os registos de auditoria dos ativos da organização devem ser retidos por um período mínimo de 90 dias (CIS Controls v8.0: 8.9) [39].

É fundamental assegurar que todos os acessos aos dados dos titulares dos cartões são registados (PCI-DSS v4: 10.2.1.1) [40].

PR.PS-06: *Secure software development practices are integrated, and their performance is monitored throughout the software development life cycle*

Todas as mudanças nos sistemas são documentadas, aprovadas e testadas para verificar que cumprem as medidas de segurança necessárias e que não comprometem o sistema (PCI-DSS v4: 6.5.1) [40].

Devem ser implementadas e geridas *firewalls* nos sistemas, servidores e dispositivos dos utilizadores (CIS Controls v8.0: 4.4, 4.5) [39].

Nos dispositivos móveis devem estar implementados ambientes de trabalho separados, de forma a existir uma divisão entre aplicações e dados pessoais de dados corporativos (CIS Controls v8.0: 4.12) [39].

No caso das aplicações críticas, têm de ser levados a cabo testes de penetração de forma a detetar vulnerabilidades que possam pôr em causa a continuidade de negócio, entre outros (CIS Controls v8.0: 16.13) [39].

3.4.4. Núcleo: Detetar

Depois de identificados e priorizados quer os ativos quer os riscos, esta fase atua como apoio à capacidade de proteção sobre os ativos da organização, de forma a reduzir a probabilidade de eventos adversos de segurança. É necessário desenvolver e testar procedimentos de segurança para detetar estes eventos. Os registos podem conter informação valiosa para tal [45].

Após a deteção de um incidente de segurança, a organização deve atuar o mais rapidamente possível de forma a compreender os possíveis impactos do mesmo. Deve ser transmitido aos colaboradores autorizados para tal todas as informações relevantes de forma a serem tomadas as medidas de resposta adequadas [45].

É de extrema importância fazer avaliações periódicas dos *softwares* e *hardwares* internos e externos, como do ambiente de trabalho, de forma a detetar possíveis variações comportamentais dos mesmos. Priorizar a instalação de antivírus e anti-*malware* em todos os dispositivos da organização [45].

Nesta fase incluem-se a gestão da identidade, a autenticação e o controlo de acesso, sensibilização e formação, a segurança dos dados e plataformas (ou seja, a segurança do *hardware*, do *software* e dos serviços das plataformas físicas e virtuais), e a resiliência da infraestrutura tecnológica [45].

De forma a perceber os vários passos desta fase, é possível fazer um conjunto de perguntas:

- Os dispositivos utilizados pelos colaboradores têm antivírus instalado? [46]
- Os colaboradores estão preparados para detetar e comunicar possíveis ataques? [46]
- A organização monitoriza os registos e alertas para detetar potenciais incidentes? [46]

De seguida, apresenta-se, na tabela 14, o mapeamento dos requisitos do núcleo Detetar da NIST - CSF que foram complementados com os requisitos dos restantes modelos de referência:

Tabela 14. Mapeamento dos controlos do Núcleo Detetar

NIST - CSF Sub-categoria	**Requisitos CIS**	**Requisitos PCI-DSS**	**Requisitos SWIFT CSCF**
DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09	-	PCI-DSS v4: 10.4.1, 11.2.1, 11.2.2	-
DE.CM-01	-	PCI-DSS v4: 5.2.1, 5.3.1, 5.3.5	SWIFT CSCF 6.1, 6.2, 6.3, 6.5A
DE.AE	-	PCI-DSS v4: 11.3.1.3	-
DE.AE-02	CIS v8.0: 3.14	PCI-DSS v4: 10.4.1	-
DE.AE-03	CIS v8.0: 8.2, 8.5, 8.6, 8.7, 8.8, 8.12	-	-
DE.AE-06	CIS v8.0: 13.1, 17.5	PCI-DSS v4: 12.10.4	-

DE.CM-01: *Networks and network services are monitored to find potentially adverse events*

DE.CM-03: *Personnel activity and technology usage are monitored to find potentially adverse events*

DE.CM-06: *External service provider activities and services are monitored to find potentially adverse events*

DE.CM-09: *Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events*

Todos os seguintes registos são revistos pelo menos diariamente: eventos de segurança, eventos de todos os componentes críticos do sistema e de todos os servidores e componentes que têm funções de segurança (PCI-DSS v4: 10.4.1) [40].

Os pontos autorizados e não autorizados de acesso sem fios são testados, identificados e detetados pelo menos a cada 3 meses (PCI-DSS v4: 11.2.1) [40]. É mantido um inventário de todos os pontos de acesso autorizados (PCI-DSS v4: 11.2.2) [40].

DE.CM-01: *Networks and network services are monitored to find potentially adverse events*

DE.CM-09: *Computing hardware and software, runtime environments, and their data are monitored to find potentially adverse events*

Análise no acesso, também conhecida como análise em tempo real, é feita em todos os sistemas. Análises a pedido são feitas pelo menos todas as semanas. Devem ser analisados todos os ficheiros do sistema, com certas exceções devido ao risco envolvido nos mesmos (Swift 6.1 Malware Protection) [42].

O software deve ser configurado em modo prevenção, e os ficheiros suspeitos devem ser mantidos em quarentena, para detetar eventuais falsos positivos. Soluções *Endpoint Protection Platform* (EPP) combinadas com *Endpoint Detection and Response* (EDR) correspondem também a uma implementação válida (Swift 6.1 Malware Protection) [42].

São feitas verificações de integridade do *software* utilizado regularmente, sendo recomendado pelo menos uma vez por dia (Swift 6.2 Software Integrity) [42]. De igual modo, também são

feitas análises de integridade das bases de dados, de forma a detetar mudanças inesperadas nos dados (Swift 6.3 Database Integrity) [42].

Deve ser implementado um sistema de deteção de intrusões, para detetar acessos não autorizados e atividades anómalas. É possível utilizar *Network Intrusion Detection System* (NIDS), *Host Intrusion Detection Systems* (HIDS), EDR, *Extended Detection and Response* (XDR) ou uma combinação destas soluções, são opções válidas para o efeito. Quando uma intrusão é detetada, o alarme entra em ação e aciona-se um mecanismo de defesa, automático ou não (Swift 6.5A Intrusion Detection) [42].

É recomendada a implementação de soluções de anti-*malware* em todos os componentes do sistema, mantendo-a sempre atualizada, e não pode ser possível desabilitar ou alterar os mecanismos da solução (PCI-DSS v4: 5.2.1, 5.3.1, 5.3.5) [40].

DE.AE: *Anomalies, indicators of compromise, and other potentially adverse events are analyzed to characterize the events and detect cybersecurity incidents*

Verificações de vulnerabilidades internas devem ser feitas sempre que vulnerabilidades críticas e de alto risco sejam resolvidas (PCI-DSS v4: 11.3.1.3) [40].

DE.AE-02: *Potentially adverse events are analyzed to better understand associated activities*

Todos os acessos efetuados a informação sensível devem ser registados, e definidos processos para a sua gestão, e eventual eliminação (CIS Controls v8.0: 3.14) [39].

Os seguintes registos devem ser revistos pelo menos diariamente: eventos de segurança, registos de componentes críticos e registos de servidores e componentes do sistema que desempenham funções de segurança (PCI-DSS v4: 10.4.1) [40].

DE.AE-03: *Information is correlated from multiple sources*

Transferir registos gerados por outras fontes para servidores dedicados. Utilizar sistemas de correlação para coletar informação capturada por várias fontes e utilizar *cyber threat intelligence*, que se refere à recolha, processamento e análise de dados com o objetivo de transformar os mesmos em informações práticas e úteis, para ajudar a correlacionar estes registos. Devem ser também recolhidos os registos provenientes do prestador de serviços, como eventos de autenticação e autorização ou criação e eliminação de dados (CIS Controls v8.0: 8.12) [39].

Assegurar a recolha de registos de auditoria detalhados sobre dados sensíveis, incluindo data, nome de utilizador, registo de hora, endereço de destino e quaisquer outros campos fundamentais numa análise forense. Recolher registos de SSH, *Uniform Resource Locator* (URL) e linha de comandos (CIS Controls v8.0: 8.2, 8.5, 8.6, 8.7, 8.8, 8.12) [39].

DE.AE-06: *Information on adverse events is provided to authorized staff and tools*

Designar funções específicas para a resposta a incidentes, incluindo colaboradores da equipa judicial, TI, segurança, instalações, recursos humanos, relações públicas, etc. Rever as funções anualmente ou quando ocorrerem mudanças significativas (CIS Controls v8.0: 17.5) [39].

Os alertas de eventos de segurança nos ativos da organização devem estar centralizados para correlação e análise de registos (CIS Controls v8.0: 13.1) [39].

Os colaboradores responsáveis por atuar sobre as ameaças estão treinados e são periodicamente testados na atuação das suas responsabilidades (PCI-DSS v4: 12.10.4) [40].

3.4.5. Núcleo: Responder

Nesta fase é feito o apoio à capacidade de contenção dos incidentes de segurança. Os resultados desta função abrangem a gestão, análise, atenuação e comunicação.

É fundamental pôr em ação o plano de resposta a incidentes quando os mesmos são declarados. Para o executar corretamente, é necessário certificar-se de que todos conhecem as suas responsabilidades [45].

Categorizar e priorizar incidentes, escalando-os conforme a gravidade. Comunicar esta prioridade à equipa e assegurar que todos compreendem a quem devem ser comunicadas as informações relativas a um incidente prioritário [45].

A recolha de dados sobre incidentes, preservando a sua integridade, é também de extrema relevância, visto que ajudará na resposta da organização a um incidente. Garantir a segurança e integridade dos dados após o incidente, para manter a reputação e confiança da organização, e atualizar planos de resposta futuros para que sejam ainda mais eficazes [45].

Notificar as partes interessadas de quaisquer incidentes, e partilhar as informações sobre os mesmos, seguindo as políticas da organização, de forma segura e consistente com os planos de resposta e acordos de partilha de informações [45].

Uma vertente de extrema importância também é a contenção e erradicação de incidentes. A execução de um plano de resposta desenvolvido e testado ajudará a organização a conter os efeitos de um incidente e a erradicá-lo. Uma coordenação e comunicação significativas com as partes interessadas levam a uma resposta mais eficaz, resultando na atenuação do incidente [45]. De forma a perceber os vários passos desta fase, é possível fazer um conjunto de perguntas:

• Está desenvolvido um plano de resposta a incidentes? Se sim, já foi praticado para confirmar a sua exequibilidade? [46]

• É de conhecimento quem são as principais partes interessadas internas e externas e os decisores que ajudarão a organização em caso de ocorrer um incidente? [46]

De seguida, apresenta-se, na tabela 15 o mapeamento dos requisitos do núcleo Responder da NIST - CSF que foram complementados com os requisitos dos restantes modelos de referência:

Tabela 15. Mapeamento dos controlos do Núcleo Responder

NIST - CSF Sub-categoria	**Requisitos CIS**	**Requisitos PCI-DSS**	**Requisitos SWIFT CSCF**
RS.MA-01	CIS v8.0: 1.2, 17.5	PCI-DSS v4: 12.10.1	-
RS.MA-02	-	PCI-DSS v4: 10.4.1, 10.4.3	-
RS.MA-03	CIS v8.0: 17.4	PCI-DSS v4: 10.4.1	-
RS.MA-04	CIS v8.0: 17.5	-	-
RS.CO-02	CIS v8.0: 17.5	PCI-DSS v4: 10.7.2	-
RS.CO-03	CIS v8.0: 17.5	-	-

RS.MA-01: *The incident response plan is executed in coordination with relevant third parties once an incident is declared*

Designar funções chave e responsabilidades para o reporte de incidentes, como da equipa jurídica, TI, recursos humanos, etc. Rever as funções anualmente ou sempre que ocorrerem mudanças significativas [39] (CIS Controls v8.0: 17.5).

Deve ser assegurada uma revisão regular dos ativos não autorizados, semanalmente. Pode ser feita a remoção, mudança de acessos ou colocá-los em quarentena (CIS Controls v8.0: 1.2) [39].

O plano de resposta a incidentes existe e deve estar pronto a ser implementado assim que existir uma suspeita ou confirmação de um incidente de segurança (PCI-DSS v4: 12.10.1) [40].

RS.MA-02: *Incident reports are triaged and validated*

Exceções e anomalias identificadas são tratadas. Os responsáveis pelo tratamento devem ser entrevistados de modo a perceber se foram e ficaram tratadas (PCI-DSS v4: 10.4.3) [40].

Os seguintes registos devem ser revistos pelo menos diariamente: eventos de segurança, registos de componentes críticos e registos de servidores e componentes do sistema que desempenham funções de segurança (PCI-DSS v4: 10.4.1) [40].

RS.MA-03: *Incidents are categorized and prioritized*

Análise e categorização dos incidentes, atribuindo-lhes prioridade com base no seu âmbito e impacto. Os seguintes registos devem ser revistos pelo menos diariamente: eventos de segurança, registos de componentes críticos e registos de servidores e componentes do sistema que desempenham funções de segurança (PCI-DSS v4: 10.4.1) [40].

Definir e manter limiares de incidentes de segurança, incluindo a diferenciação entre um incidente e um evento, por exemplo, incidentes de privacidade, fuga de dados, vulnerabilidades de segurança. Rever anualmente ou sempre que ocorram mudanças significativas (CIS Controls v8.0: 17.4) [39].

RS.MA-04: *Incidents are escalated or elevated as needed*

Designar funções chave e responsabilidades para o reporte de incidentes, como da equipa jurídica, TI, recursos humanos, etc. Rever as funções anualmente ou sempre que ocorrerem mudanças significativas (CIS Controls v8.0: 17.5) [39].

RS.CO-02: *Internal and external stakeholders are notified of incidents*

Designar funções chave e responsabilidades para o reporte de incidentes, como da equipa jurídica, TI, recursos humanos, etc. Rever as funções anualmente ou sempre que ocorrerem mudanças significativas (CIS Controls v8.0: 17.5) [39].

Eventuais falhas dos sistemas críticos de controlo de segurança são detetadas e alertadas às partes interessadas e tratadas prontamente (PCI-DSS v4: 10.7.2) [40].

RS.CO-03: *Information is shared with designated internal and external stakeholders*

Designar funções chave e responsabilidades para o reporte de incidentes, como da equipa jurídica, TI, recursos humanos, etc. Rever as funções anualmente ou sempre que ocorrerem mudanças significativas (CIS Controls v8.0: 17.5) [39].

3.4.6. Núcleo: Recuperar

Esta etapa apoia o restabelecimento atempado das operações normais, visando minimizar ao máximo os efeitos dos incidentes de cibersegurança, permitindo uma comunicação eficaz durante os esforços de recuperação.

É fundamental compreender os papéis e as responsabilidades, ou seja, quem tem responsabilidade de recuperação. Saber quem tem acesso e autoridade para tomar decisões.

Nesta fase é executado o plano de recuperação. Assegurar a disponibilidade operacional dos sistemas e serviços afetados. [45]

É crucial verificar duas vezes o trabalho. É importante garantir a integridade das cópias de segurança e de outros ativos de recuperação antes de os utilizar [45].

Comunicar com as partes interessadas, tendo em conta o quê, como e quando as informações serão partilhadas com estas, de modo que todas recebam as informações de que necessitam. Comunicar também aos colaboradores as lições aprendidas e as revisões de processos, procedimentos e tecnologias. É importante aproveitar para formar, ou reciclar, os colaboradores sobre as melhores práticas de cibersegurança [45].

De forma a perceber os vários passos desta fase, é possível fazer um conjunto de perguntas:

• Quais são as lições aprendidas? De que forma é possível reduzir as hipóteses de ocorrência de um incidente de cibersegurança? [46]

• Quais são as obrigações legais, regulamentares e contratuais para comunicar às partes interessadas sobre um incidente de cibersegurança? [46]

• De que forma é possível garantir que as medidas de recuperação utilizadas não introduzem novas vulnerabilidades? [46]

De seguida, apresenta-se, na tabela 16 o mapeamento dos requisitos do núcleo Recuperar da NIST - CSF que foram complementados com os requisitos dos restantes modelos de referência:

Tabela 16. Mapeamento dos controlos do Núcleo Recuperar

NIST - CSF Subcategoria	Requisitos CIS	Requisitos PCI-DSS	Requisitos SWIFT CSCF
RC.RP	-	PCI-DSS v4: 12.10.6	-

RC.RP: *Incident Recovery Plan Execution*

O plano de resposta a incidentes deve ser regularmente modificado e atualizado com base nas lições aprendidas, após a ocorrência de um incidente, incorporando também o que de novo surge

na indústria. Os colaboradores responsáveis devem ser entrevistados de forma a garantir que o plano de resposta a incidentes tem sido modificado e atualizado de acordo com o expectável.

De realçar a importância de identificar o que funcionou bem e avaliar de que forma essas práticas podem ser incorporadas noutras áreas do plano que apresentaram fragilidades.

Por fim, é fundamental olhar para as outras organizações, mais propriamente no que diz respeito aos ataques sofridos, e utilizar as informações recolhidas para ajustar os processos internos (PCI-DSS v4.0: 12.10.6) [40].

3.5. Fundamentação e Estrutura do Modelo Proposto

Tendo por base o ciclo descrito no ponto anterior, o presente trabalho propõe um modelo que procura responder de forma prática e estruturada a cada uma das fases do mesmo.

Está dividido em seis grandes funções, alinhado com a NIST - CSF, onde cada uma foi complementada com requisitos provenientes dos quadros normativos PCI-DSS, CIS e SWIFT CSCF. Cada uma das funções representa uma etapa essencial na gestão da cibersegurança organizacional, formando um ciclo que deve ser constantemente revisto, ajustado e reforçado.

Neste modelo, foram criadas seis tabelas, uma para cada núcleo, com as atividades, entradas e resultados associados a cada um. As entradas representam os recursos e requisitos necessários para que cada função seja corretamente executada de acordo com os objetivos da organização. Incluem qualquer tipo de documentos e/ou recursos que auxilie na tomada de decisão, como por exemplo, o inventário de ativos ou políticas e regulamentos internos existentes.

As atividades dizem respeito às ações efetuadas sobre as entradas de modo a obter resultados concretos. Essas ações podem incluir, por exemplo, a implementação de políticas, a realização de auditorias ou a monitorização dos sistemas informáticos.

Por fim, os resultados são obtidos a partir da fase anterior, as atividades. Representam o produto final, como políticas revistas e relatórios de segurança. Servem também como forma de concluir se os objetivos propostos foram, ou não, alcançados.

De seguida, na figura 5 apresenta-se o modelo desenvolvido, sendo que em anexo o modelo se encontra dividido em duas partes de modo a facilitar a sua visualização.

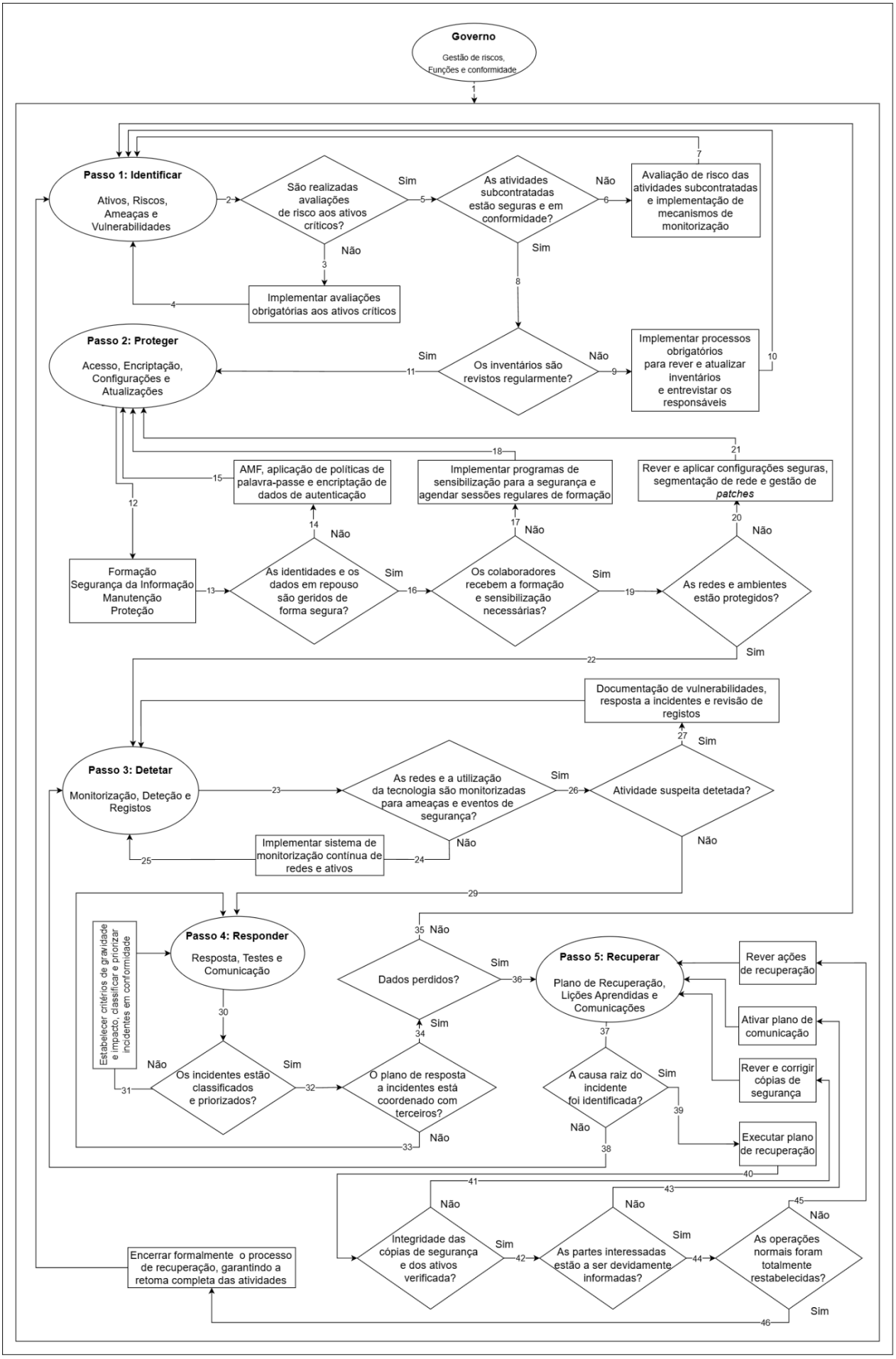


Figura 5. Modelo desenvolvido

3.6. Apresentação do Modelo Proposto

Neste ponto, apresenta-se o modelo proposto, assim como o funcionamento do mesmo. Para uma melhor interpretação do modelo, é importante perceber, em primeiro lugar, a notação usada. Assim, os círculos representam o início ou fim de processos, os losangos representam decisões e os retângulos representam ações ou tarefas. A unir cada um destes elementos, existem setas que se encontram devidamente numeradas e que representam fluxos entre os diferentes elementos do modelo. Na apresentação e explicação que se segue, o número dos fluxos apresentados encontra-se igualmente indicado.

O modelo inicia-se através da função Governo (1), fase esta que funciona como suporte para as restantes. É estabelecida uma base de cibersegurança por prioridades, funções e políticas organizacionais que estão alinhadas com a gestão de riscos e com os objetivos operacionais.

Começa no **Contexto Organizacional** (GV.CO), através da documentação clara da missão, objetivos e dependências, ao mesmo tempo que incorpora os requisitos legais e das partes interessadas nas estratégias. Deste modo, obtém-se a missão alinhada com os objetivos e riscos, bem como um inventário de dependências e capacidades críticas.

É fundamental estabelecer e manter um plano de resposta a incidentes que defina claramente as funções e responsabilidades, integre um plano de comunicação eficaz e cumpra requisitos de conformidade (CIS Controls v8.0: 17.4) [39].

Segue-se a estratégia de **Gestão de Riscos** (GV.RM), onde é documentada a tolerância ao risco, priorizando os mesmos. É assegurado que as políticas, funções e estratégias estão claramente definidas e são atualizadas. No final, obtém-se a integração da gestão do risco nos objetivos organizacionais e métricas/critérios para priorização e comunicação de riscos.

Nesta etapa são também abordados os riscos da **Cadeia de Fornecimento** (GV.SC), gerindo as relações com terceiros, estabelecendo requisitos de segurança e através da monitorização destes. Os fornecedores são então incorporados na resposta a incidentes, daqui resultando listas de priorização, *Service Level Agreement* (SLA) e mecanismos de controlo de conformidade.

A atribuição de **Funções, Responsabilidades e Autoridade** (GV.RR) é fundamental para a correta distribuição de papéis na organização, de onde se obtém a definição e comunicação dos papéis dos colaboradores, a atribuição adequada de recursos e a integração da cibersegurança nos processos de recursos humanos.

O passo seguinte, **Política** (GV.PO), envolve a elaboração e revisão de políticas no contexto organizacional, de onde resultam as políticas revistas e atualizadas e as expectativas das partes interessadas documentadas. Neste contexto, é necessário entrevistar uma amostra dos responsáveis de forma a validar que os mesmos entendem as políticas de segurança (PCI-DSS v3.2.1: 12.4) [40].

A última etapa, **Supervisão** (GV.OV) garante que os resultados da gestão de risco são medidos e ajustados. As auditorias permitem a revisão das políticas e estratégias, resultando na melhoria das mesmas, na definição de *Key Performance Indicators* (KPIs) e *Key Risk Indicators* (KRIs) aprimorados e na melhoria geral da posição de cibersegurança da organização.

De seguida, apresenta-se a Tabela 17, criada para o núcleo Governo, anteriormente referida, com as atividades, entradas e resultados associados a cada núcleo.

Tabela 17. Atividades, Entradas e Resultados - Governo

Governo	Entradas	Atividades	Resultados
GV.OC	• Missão e Objetivos • Expetativas dos Stakeholders • Dependências internas e externas • Requisitos legais, regulatórios e contratuais	• Identificar e documentar as expectativas das partes interessadas • Mapear as dependências críticas e avaliar o seu impacto nos objetivos	• Missão alinhada com os riscos • Expectativas das partes interessadas incorporadas na gestão do risco • Inventário de dependências e capacidades críticas • Objetivos de resiliência definidos
GV.RM	• Riscos atuais e possíveis • Tolerância ao risco por parte dos stakeholders • Estratégias existentes de cibersegurança	• Estabelecer e documentar a apetência e a tolerância ao risco • Agregar e priorizar os riscos • Rever e atualizar as estratégias de risco	• Tolerância ao risco documentada e comunicada • Estratégia de gestão do risco alinhada com os objetivos organizacionais • Métricas e critérios para priorização e comunicação de riscos
GV.SC	• Relação entre os fornecedores e as terceiras partes • Avaliação de risco da cadeia de abastecimento • Contratos	• Identificar e priorizar os fornecedores críticos • Definir e implementar requisitos de segurança nos contratos • Monitorizar a conformidade dos fornecedores • Integrar os fornecedores na resposta a incidentes	• Lista de fornecedores prioritários com base na criticidade • Requisitos de segurança incluídos nos contratos e *SLAs* • Mecanismos de controlo da conformidade dos fornecedores • Protocolos de resposta a incidentes para os fornecedores • Planos de gestão de riscos da cadeia de abastecimento, incluindo estratégias de saída
GV.RR	• Políticas organizacionais • Estrutura de	• Definir funções e responsabilidades	• Funções e responsabilidades definidas e comunicadas

	cibersegurança • Processos operacionais e de recursos humanos	• Desenvolver objetivos de desempenho • Desenvolver mecanismos de responsabilização • Assegurar a atribuição adequada de recursos • Integrar a cibersegurança nas políticas de RH • Verificação dos antecedentes	• Objetivos de desempenho para as funções de cibersegurança • Recursos atribuídos com base nas prioridades de gestão do risco • Integração da cibersegurança nos processos de RH
GV.PO	• Estratégia de Cibersegurança • Cenário de ameaças • Requisitos regulamentares e organizacionais	• Elaborar políticas abrangentes de cibersegurança • Rever e atualizar as políticas com base em ameaças e alterações legais • Comunicar e aplicar as políticas na organização	• Políticas de cibersegurança revistas e atualizadas • Expectativas da direção documentadas • Políticas reconhecidas e cumpridas pelos colaboradores
GV.OV	• Resultados da gestão do risco • Dados de desempenho da estratégia de cibersegurança • Constatações de incidentes e auditorias	• Medir o desempenho das estratégias de gestão do risco • Analisar os resultados das auditorias e incidentes no domínio da cibersegurança • Ajustar as políticas e estratégias • Revisão dos *KPIs* e *KRIs*	• Estratégias e políticas de gestão de riscos ajustadas • Tomadas de decisão informadas e alinhadas com os objetivos de gestão do risco • Melhoria contínua da postura de cibersegurança

Por fim, e após garantidas as fases anteriormente explicadas, avança-se para a segunda etapa do modelo, Identificar.

A fase Identificar tem como foco compreender a organização e priorizar os esforços na criticidade e no risco. Utiliza inventários completos de ativos, a identificação de vulnerabilidades, a avaliação de ameaças e a modelação de potenciais impactos para apoiar a tomada de decisão. Termina com avaliações e testes regulares com o objetivo de refinar as estratégias e melhorar a resiliência.

Inicia-se, como é possível observar pela figura 6, com a avaliação de risco dos ativos críticos (2). O primeiro passo para garantir a correta avaliação é através da **Gestão de Ativos** (ID.AM), que necessita de um inventário de ativos, sistemas e serviços, bem como critérios de classificação e priorização dos mesmos. Por fim, são necessários dados organizacionais relevantes.

De seguida, sucedem-se as atividades a realizar decorrentes dos documentos anteriores, como a manutenção e atualização dos inventários, o acompanhamento da atualização e configuração dos ativos, a monitorização de alterações no sistema e a documentação do fluxo de dados. Resultam destas atividades os inventários de ativos atualizados, uma listagem dos riscos críticos, as linhas de base do fluxo de dados e a garantia de segurança e higienização dos dados.

Se não forem realizadas avaliações de risco aos mesmos (3), é necessário implementar processos obrigatórios para o efeito antes de prosseguir (4).

Após este passo estar assegurado (5), é necessário perceber se as atividades terceirizadas

estão seguras e em conformidade com as normas de segurança e regulamentos da organização. Em caso negativo (6), uma avaliação de risco das atividades que envolvam terceiras partes é essencial, implementando também mecanismos de monitorização (7). Esta avaliação insere-se no domínio da **Avaliação de Riscos** (ID.RA), que requer como entradas os dados das vulnerabilidades existentes, avaliações dos impactos e probabilidades, bem como opções viáveis de resposta aos riscos identificados. São usadas ferramentas específicas de deteção de vulnerabilidades, análise dos dados disponíveis sobre as ameaças, modelação dos potenciais impactos, registados e priorizados os riscos e desenvolvidos planos de resposta.

Por fim, obtém-se a documentação das vulnerabilidades, os registos de risco atualizados, a priorização clara e informada das respostas aos riscos e monitorização contínua e comunicação dos ajustes realizados.

O domínio de **Melhoria Contínua** (ID.IM) utiliza como entradas os resultados obtidos de avaliações anteriores, os planos de resposta aos incidentes e métricas detalhadas de desempenho. As atividades deste domínio incluem autoavaliações frequentes e auditorias realizadas por terceiros, testes de intrusão, revisão das políticas internas com base nas lições aprendidas e a atualização periódica dos planos de resposta. Os resultados destas atividades são áreas claramente identificadas para melhorias futuras, planos de cibersegurança atualizados, bem como informações consolidadas sobre lições aprendidas e métricas detalhadas de desempenho organizacional.

Depois de garantida a segurança das atividades subcontratadas (8) é fundamental analisar se os inventários são regularmente atualizados e revistos, e as pessoas responsáveis pelos mesmos entrevistadas. Se não forem regularmente revistos (9) é aconselhável implementar procedimentos de revisão claros para o efeito (10).

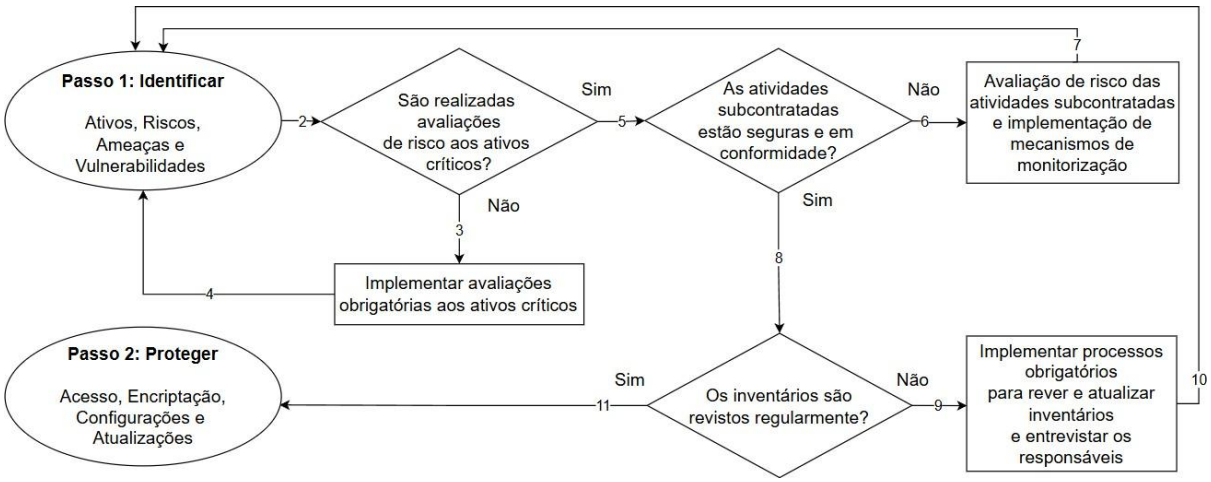


Figura 6. Secção do modelo: Identificar

De seguida, apresenta-se a Tabela 18, criada para o núcleo Identificar, anteriormente referida, com as atividades, entradas e resultados associados a cada núcleo.

Tabela 18. Atividades, Entradas e Resultados – Identificar

Identificar	Entradas	Atividades	Resultados
ID.AM	• Inventário de *hardware*, *software*, sistemas e serviços. • Critérios de classificação e priorização. • Dados organizacionais e meta dados.	• Manter inventários de *hardware*, *software*, sistemas e serviços • Monitorizar as alterações na rede • Classificar e priorizar os ativos • Documentar o fluxo de dados e os meios de comunicação da rede • Acompanhar e atualizar os ativos e as configurações ao longo do seu ciclo de vida	• Inventários de ativos atualizados • Lista de ativos críticos • Dados e *hardware* seguros e higienizados
ID.RA	• Dados de vulnerabilidade • Informações sobre ciberameaças • Avaliações de impacto e de probabilidade • Opções de resposta aos riscos	• Utilizar ferramentas para identificar vulnerabilidades • Análise de informações sobre ciberameaças • Modelar ameaças e avaliar impactos • Registar e priorizar riscos • Desenvolver planos de resposta a riscos	• Vulnerabilidades e mitigações documentadas • Registo de riscos atualizado • Priorização informada das respostas aos riscos • Ajustes de risco monitorados e comunicados
ID.IM	• Resultados de avaliações, testes e exercícios • Planos de resposta a incidentes • Métricas de desempenho	• Autoavaliações e auditorias a terceiros • Exercícios e testes de penetração • Rever as políticas com base nas lições aprendidas • Atualizar regularmente os planos de resposta a incidente	• Áreas a melhorar identificadas • Planos de cibersegurança atualizados e melhorados • Informações sobre as lições aprendidas e métricas de desempenho

Em caso positivo (11) chega-se então à segunda etapa, Proteger.

A fase Proteger garante que os serviços críticos são mantidos e que a probabilidade de eventos de segurança é minimizada. Esta fase inicia-se com a **Gestão das Identidades e Acessos** (PR.AA), fase essa que inclui atividades-chave como autenticação segura dos utilizadores, gestão de identidades e princípios de privilégio mínimo, de onde resultam a segura autenticação dos utilizadores e permissões alinhadas com as políticas organizacionais (12), como é possível observar pela figura 7.

O acesso aos componentes do sistema deve ser protegido com autenticação multifator, e os dados de autenticação encriptados. Executar bloqueio após um número definido de tentativas e proibir a reutilização de palavras-passe (PCI-DSS v4: 8.3.2 e 8.3.7) [40].

Se estas atividades não estiverem bem consolidadas na organização (14), é necessário rever as políticas de autenticação multifator, aplicar as políticas de palavras-passe e encriptação aos dados de autenticação (15).

Ao mesmo tempo, a **Sensibilização e Treino** (PR.AT) requer planos de formação e cenários de ameaças (16). As atividades desta fase incluem a formação contínua dos colaboradores e a avaliação periódica do seu nível de compreensão das políticas, resultando em colaboradores informados e capacitados para responder às ameaças de segurança. Caso os colaboradores não sejam treinados e formados adequadamente (17) é necessária a implementação de programas de consciencialização e formação regulares (18).

Os dados são protegidos durante todo o seu ciclo de vida, garantido pela fase de **Segurança dos Dados** (PR.DS), que utiliza políticas de classificação dos dados, ferramentas de criptografia e sistemas de cópias de segurança, reduzindo a exfiltração ou perda de dados.

De seguida, vem a fase de **Segurança das Plataformas** (PR.PS), que tem como apoio guias de configurações seguras, inventários atualizados de *hardware* e *software* e planos de gestão de vulnerabilidades. As atividades realizadas incluem a aplicação de configurações seguras, monitorização contínua e bloqueios não autorizados. Resultam das atividades anteriores sistemas reforçados, armazenamento de registos detalhados, e bloqueios não autorizados são feitos com sucesso.

Finalmente, a **Resiliência da Infraestrutura Tecnológica** (PR.IR) (19). Esta depende de estratégias de risco para sistemas e infraestruturas, métricas detalhadas de utilização de recursos e avaliações frequentes das ameaças ambientais. Estão incluídas nesta fase a segmentação lógica das redes, a proteção de ativos essenciais, a monitorização das ameaças ambientais e o planeamento da redundância necessária. Assim, garantem-se redes segregadas e seguras, ativos protegidos e resilientes, assim como recursos adequados às necessidades operacionais.

Se estas infraestruturas não se encontrarem protegidas (20), é necessário rever e implementar todas as configurações necessárias de segurança, processos de gestão de correções e atualizações, entre outros (21).

Outras medidas como a segmentação da rede e a resiliência da infraestrutura garantem a continuidade do negócio.

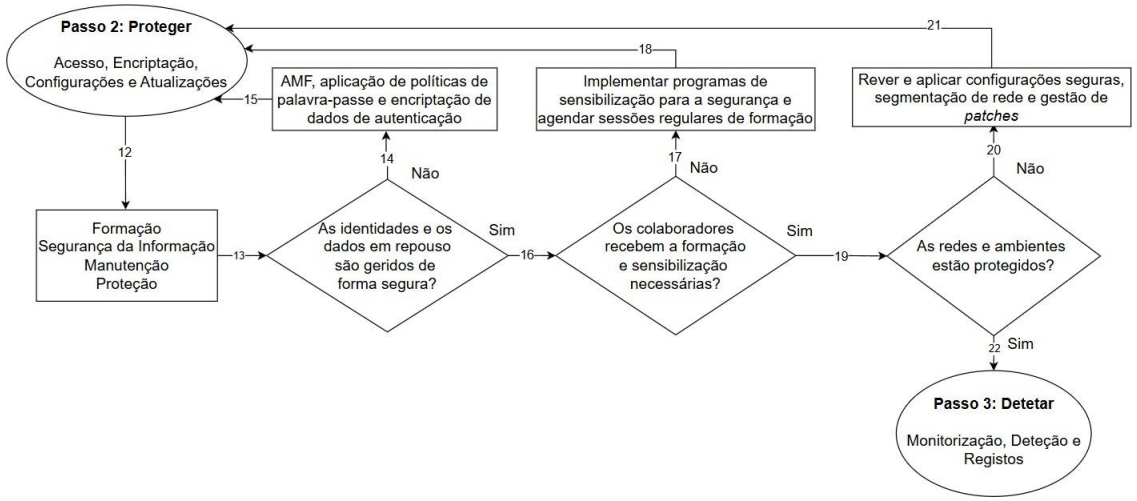


Figura 7. Secção do modelo: Proteger

De seguida, apresenta-se a Tabela 19, criada para o núcleo Proteger, anteriormente referida, com as atividades, entradas e resultados associados a cada núcleo.

Tabela 19. Atividades, Entradas e Resultados - Proteger

Proteger	Entradas	Atividades	Resultados
PR.AA	• Dados de identidade do utilizador, do serviço e do *hardware* • Políticas de autorização e autenticação	• Gerir identidades e credenciais • Comprovar identidades • Autenticar utilizadores, serviços e *hardware* • Proteger e verificar afirmações de identidade • Definir e aplicar permissões de acesso com base no privilégio mínimo	• Utilizadores, serviços e *hardware* autenticados • Afirmações de identidade verificadas e protegidas • Permissões de acesso alinhadas com as políticas organizacionais
PR.AT	• Planos de formação • Cenários de ameaças específicos da organização • Requisitos de funções do utilizador	• Fornecer formação para cada função • Avaliar periodicamente a compreensão dos utilizadores • Atualizar os materiais de formação com base nas ameaças emergentes	• Pessoal informado e formado • Redução da suscetibilidade às ameaças • Melhoria da adesão às políticas de cibersegurança
PR.DS	• Políticas de classificação de dados • Ferramentas criptográficas • Sistemas de *backup* e restauração • Planos de gestão do ciclo de vida dos dados	• Proteger os dados em repouso, trânsito e utilização • Criar e testar cópias de segurança • Aplicar políticas de acesso e retenção de dados • Limpar e destruir de forma segura os dados obsoletos	• Dados protegidos durante o seu ciclo de vida • Cópias de segurança de dados testadas e funcionais • Risco reduzido de perda ou exfiltração de dados
PR.PS	• *Baselines* de configuração • Inventários de *hardware* e *software* • Planos de gestão de vulnerabilidades	• Aplicar configurações seguras • Manter, substituir ou retirar software e hardware • Monitorizar e gerar registos • Impedir a execução não autorizada de software • Implementar práticas de desenvolvimento seguras	• Plataformas seguras e reforçadas • Registos de *logs* • Bloqueio de execução não autorizada de software
PR.IR	• Estratégias de risco para sistemas e infraestruturas	• Segmentar as redes de forma lógica	• Redes segregadas e seguras

	• Métricas de utilização de recursos • Avaliações de ameaças ambientais	• Proteger os ativos contra ameaças ambientais • Assegurar a resiliência através de redundância e equilíbrio de carga • Monitorizar e prever as necessidades de recursos	• Ativos protegidos e resilientes • Recursos adequados para as necessidades operacionais

Se estiver garantido que a informação está protegida e que as identidades e credenciais são geridas de forma segura, segue-se a quarta fase, Detetar (22).

A fase Detetar tem como principal objetivo a rápida identificação de eventos de segurança. Foca-se na monitorização contínua dos sistemas da organização, atividades dos colaboradores e fornecedores de serviços externos. Estes eventos são posteriormente analisados, de forma a determinar a sua causa e o âmbito. Ao correlacionar a informação, é possível ter um entendimento do cenário de ameaças, mantendo a resiliência do sistema (23).

Existem duas fases principais, **Monitorização Contínua** (DE.CM) e **Análise de Eventos Adversos** (DE.AE). Na monitorização contínua, as principais entradas incluem dados da rede e do ambiente físico, registos de atividade e acesso, e informações sobre ameaças cibernéticas. As atividades realizadas envolvem a monitorização dos controlos de acesso físico e das condições ambientais, o acompanhamento da atividade dos colaboradores, bem como a monitorização das atividades dos fornecedores, do *hardware/software* e das redes e serviços da organização para detetar potenciais eventos adversos. Como resultado, obtêm-se alertas de anomalias, indicadores de comprometimento e relatórios sobre eventos adversos.

Como se observa na figura 8, se não for realizada uma monitorização contínua da rede e atividade (24), é necessário implementar um sistema especializado para o efeito (25), através de políticas com diretrizes claras que definam o âmbito da monitorização, utilizar soluções como *Security Information and Event Management* (SIEM), *Intrusion Detection System* (IDS) e *Intrusion Prevention System* (IPS), entre outros, configurar alertas e notificações para os eventos suspeitos, treinar as equipas técnicas e auditar e testar frequentemente o sistema de monitorização.

Já na análise de eventos adversos, as entradas consistem em registos e alertas de sistemas de monitorização, informações sobre ciberameaças e inventários de ativos. As atividades centram-se na análise de anomalias, correlação de informações, estimativa do impacto e âmbito dos eventos detetados, fornecimento de dados relevantes aos colaboradores autorizados, e na integração de informações sobre ameaças.

Como resultados, obtém-se dados de eventos analisados e correlacionados, estimativas de impacto e âmbito, alertas e relatórios para equipas de resposta a incidentes, e sistemas de deteção enriquecidos com contexto adicional sobre ameaças. Caso seja detetada atividade suspeita (27) é necessário ativar o plano de resposta a incidentes, conter a ameaça através de mecanismos de isolamento do sistema, bloqueando tráfego malicioso e analisando registos e alertas, e por fim, classificar e documentar o acidente (28).

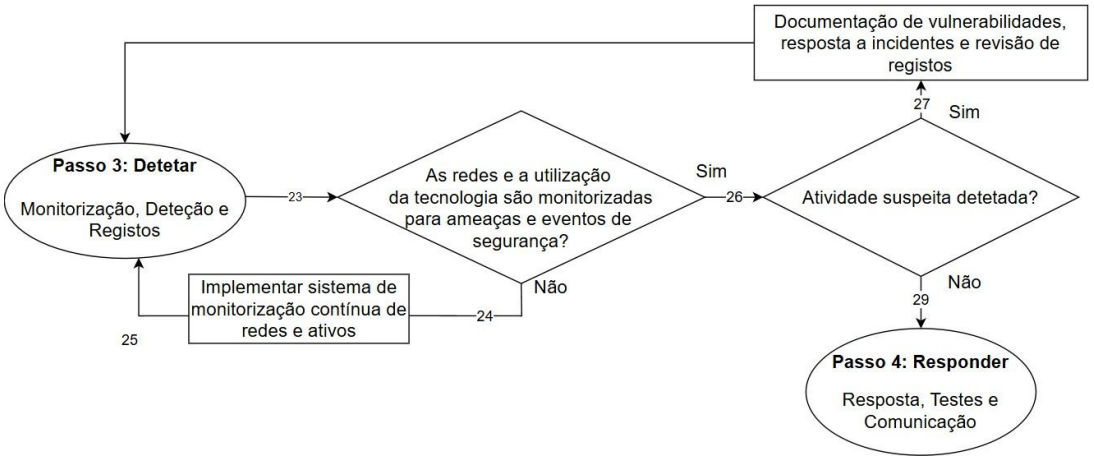


Figura 8. Secção do modelo: Detetar

De seguida, apresenta-se a Tabela 20, criada para o núcleo Detetar, anteriormente referida, com as atividades, entradas e resultados associados a cada núcleo.

Tabela 20. Atividades, Entradas e Resultados – Detetar

Detetar	Entradas	Atividades	Resultados
DE.CM	• Dados da rede e do ambiente físico • *Logs* de atividade e acesso • Informações sobre ciberameaças	• Monitorizar os controlos de acesso físico e as condições ambientais • Acompanhar a atividade dos colaboradores • Monitorizar as atividades dos fornecedores, o *hardware*/*software* e as redes e serviços para detetar eventos adversos	• Alertas de anomalias • Indicadores de comprometimento • Relatórios sobre eventos adversos
DE.AE	• *Logs* e alertas de sistemas de monitorização • Informações sobre ciberameaças • Inventários de ativos	• Análise de anomalias • Correlacionar informações • Estimar o impacto e o âmbito dos eventos adversos • Fornecer informações e ferramentas aos colaboradores autorizados • Integrar informações sobre ameaças na análise	• Dados de eventos analisados e correlacionados • Estimativas de impacto e âmbito • Alertas e relatórios para equipas de resposta a incidentes • Sistemas de deteção enriquecidos com informações contextuais sobre ameaças

Se no fim desta fase não forem detetadas ameaças, ou após as ameaças detetadas e atividades suspeitas terem sido documentadas, segue-se a quinta fase, Responder (29).

Esta fase centra-se na mitigação do impacto dos incidentes de segurança, permitindo uma recuperação eficaz. A primeira fase deste núcleo, **Gestão de Incidentes** (RS.MA) destaca-se pela

execução de planos de resposta, com base em relatórios, dados de eventos de segurança e planos previamente definidos.

Na figura 9 é possível observar esta fase no modelo. As principais atividades desta fase incluem a triagem e validação dos relatórios, categorização e priorização dos incidentes (30), e critérios de início de recuperação. No caso de os incidentes não estarem categorizados nem priorizados, é necessário voltar a rever este tema (31). Como resultados, provêm a documentação estruturada de respostas a incidentes e a priorização dos mesmos (32).

A subcategoria **(Análise de Incidentes)** (RS.AN) foca-se na análise detalhada dos incidentes, utilizando dados específicos, ferramentas de análise e indicadores de comprometimento. O objetivo é compreender a sequência dos eventos e identificar as principais causas, garantindo a integridade dos registos utilizados na investigação. São recolhidos e validados dados essenciais para estimar a magnitude dos incidentes. Os resultados incluem registos de investigação, avaliações de impacto validadas e relatórios pormenorizados de causalidade.

A subcategoria **(Mitigação de Incidentes)** (RS.MI) envolve a contenção dos incidentes, incluindo o isolamento de sistemas e a passagem de ativos comprometidos para ambientes próprios de mitigação. As decisões são tomadas pelos resultados obtidos da deteção e análise, por ferramentas de contenção e dados de vulnerabilidades. Como resultados, obtém-se a contenção efetiva dos incidentes, a correção dos sistemas afetados e a redução do seu âmbito e impacto.

Por fim, a comunicação é tratada na subcategoria **(Comunicação e Relatório de Resposta a Incidentes)** (RS.CO), que envolve canais definidos para notificação às partes interessadas, entidades reguladoras e fornecedores. Com base nos requisitos legais e regulamentares, são partilhadas informações relevantes, a gestão é atualizada e são estabelecidos registos de comunicação com entidades externas. Estes esforços asseguram que todos os intervenientes são devidamente informados e que a resposta é coordenada de forma eficaz (34). No caso de o processo de comunicação não estar eficazmente definido (33) é necessário rever este passo na íntegra.

No caso de ter ocorrido perda de dados (36) avança-se para a última fase, Recuperar. Caso não tenha ocorrido perda de dados (35), volta-se para o início do diagrama.

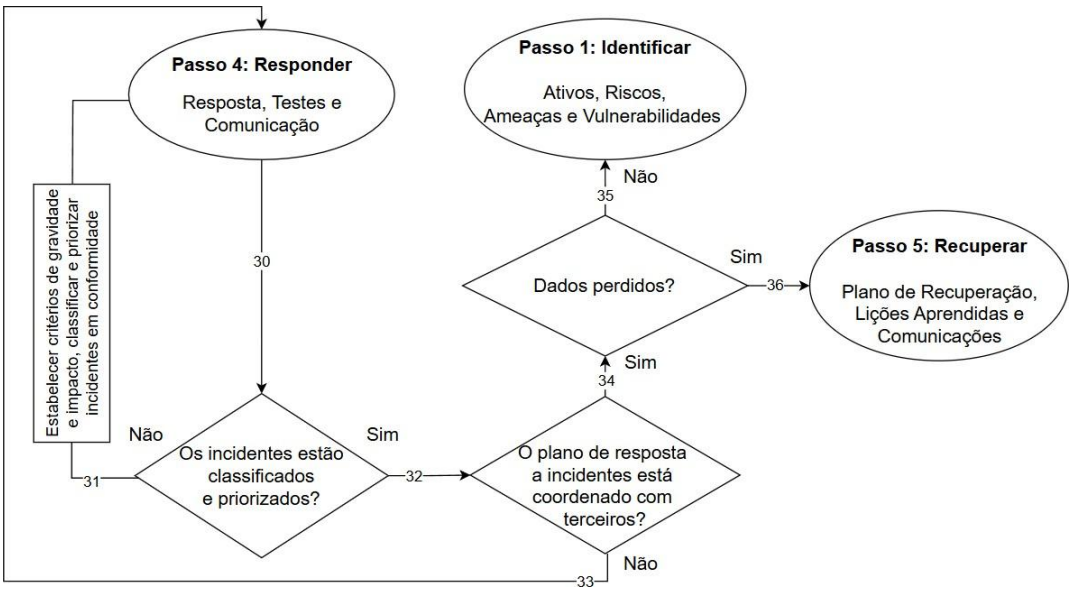


Figura 9. Secção do modelo: Responder

De seguida, apresenta-se a tabela 21, criada para o núcleo Responder, anteriormente referida, com as atividades, entradas e resultados associados a cada núcleo.

Tabela 21. Atividades, Entradas e Resultados - Responder

Responder	Entradas	Atividades	Resultados
RS.MA	• Relatórios de incidentes • Planos de resposta a incidentes • Dados de eventos de cibersegurança	• Executar o plano de resposta a incidentes • Triagem e validação de relatórios de incidentes • Categorizar, priorizar e escalar os incidentes • Aplicar critérios de início de recuperação	• Gestão e documentação de respostas a incidentes • Priorização dos incidentes • Processos de escalonamento confirmados • Decisões de início de recuperação
RS.AN	• Dados de incidentes • Ferramentas de análise • Indicadores de comprometimento	• Analisar as sequências de incidentes e as principais causas • Preservar a integridade dos *logs* de investigação • Recolher e validar dados de incidentes • Estimar a magnitude e a persistência do incidente	• Registos de investigação preservados • Avaliações de impacto validadas • Relatórios pormenorizados de causalidade
RS.CO	• Dados de incidentes • Canais de comunicação com as partes interessadas • Requisitos legais e regulamentares	• Notificar as partes interessadas • Comunicar informações de acordo com os planos de resposta • Atualizar a direção • Coordenar a comunicação com os fornecedores	• Notificações das partes interessadas e das entidades reguladoras • Partilha e atualização de informações sobre incidentes • Estabelecimento de registos de comunicação com entidades externas
RS.MI	• Resultados de deteção e análise • Ferramentas de contenção • Dados de vulnerabilidade	• Conter incidentes, colaborando, se necessário, com terceiros • Transferir ativos comprometidos para ambientes de correção	• Incidentes contidos • Isolamento e correção dos sistemas • Redução do âmbito e do impacto dos incidentes

Por fim, e após validadas todas estas etapas, segue-se a última fase, Recuperar.

Nesta última etapa, o foco está no restauro dos sistemas e serviços após um incidente de cibersegurança, assegurando a continuidade de negócio. As ações de recuperação são executadas com base nos planos anteriormente definidos, sendo as cópias de segurança e os ativos avaliados quanto à sua integridade antes de serem utilizados.

Esta fase divide-se em duas subcategorias principais: **Execução do Plano de Recuperação de Incidentes** (RC.RP) e **Comunicação da Recuperação de Incidentes** (RC.CO).

A primeira contempla a identificação da causa raiz do incidente (37), como é possível observar na figura 10, que caso não tenha sido identificada, deve-se voltar à fase Detetar (38), execução dos planos de recuperação (39), a definição do âmbito e da prioridade das ações a serem implementadas, a verificação da integridade das cópias de segurança e dos ativos restaurados (40),

que, se não tiverem sido verificados, é necessário rever e corrigir os mesmos (41), bem como a monitorização contínua dos sistemas restaurados, garantindo o seu correto funcionamento (42). Já a subcategoria (RC.CO) foca-se na comunicação durante o processo de recuperação. Uma comunicação transparente mantém as partes interessadas informadas (44), reforçando a confiança na organização. Esta comunicação baseia-se em dados sobre o progresso da restauração, canais de comunicação apropriados e requisitos legais ou regulamentares aplicáveis. Assim, é possível comunicar atualizações de forma segura e notificar as partes afetadas através de mensagens previamente aprovadas. Caso não exista uma comunicação eficaz e transparente, é necessário implementar o plano de comunicação (43).

Finalmente, deve ser avaliado se as operações normais foram plenamente restauradas. Se a resposta for afirmativa (46), a organização pode encerrar formalmente o processo de recuperação, garantindo a retoma completa das suas atividades. Caso contrário (45), devem ser revistos os planos e medidas aplicadas, assegurando que eventuais falhas sejam corrigidas antes da finalização desta etapa.

Como resultado, esta fase visa garantir a disponibilidade operacional da organização e assegurar que as partes interessadas, tanto internas como externas, sejam atualizadas de forma segura e eficaz ao longo de todo o processo de recuperação.

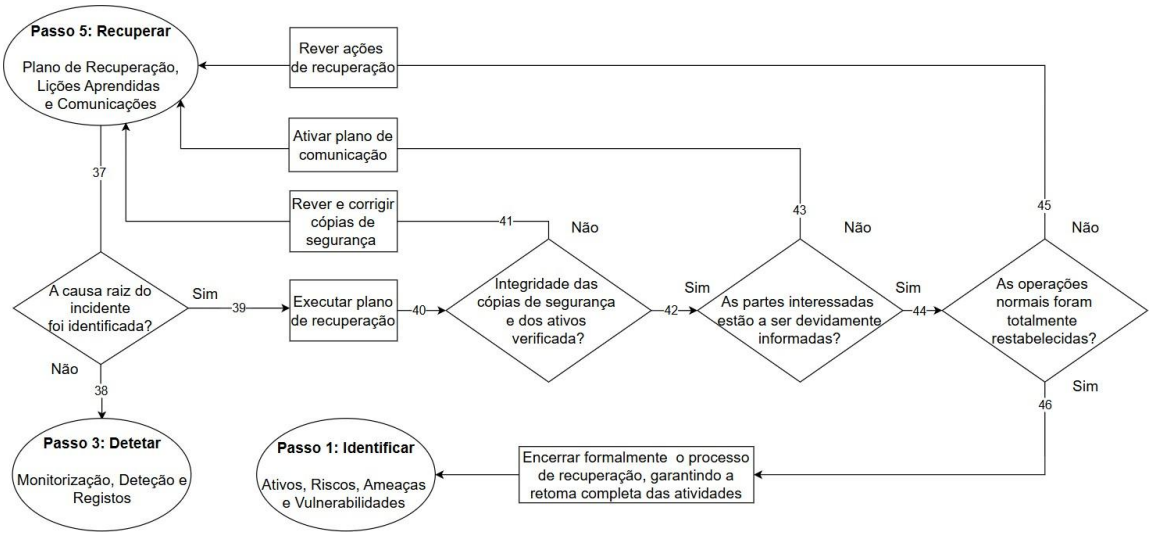


Figura 10. Secção do modelo: Recuperar

De seguida, apresenta-se a tabela 22, criada para o núcleo Recuperar, anteriormente referida, com as atividades, entradas e resultados associados a cada núcleo.

Tabela 22. Atividades, Entradas e Resultados – Recuperar

Recuperar	Entradas	Atividades	Resultados
RC.RP	• Resultados da resposta a incidentes • Planos de recuperação	• Executar planos de recuperação • Definir o âmbito e a prioridade das ações de recuperação • Verificar a integridade dos *backups* e dos ativos de restauro • Monitorizar os sistemas restaurados	• Garantir a disponibilidade operacional
RC.CO	• Dados sobre o progresso da restauração • Canais de comunicação • Requisitos legais e regulamentares	• Comunicar atualizações de recuperação com as partes interessadas • Notificar as partes afetadas através de mensagens aprovadas	• Atualização das partes interessadas internas e externas, de forma segura

3.6.1. Conclusões

Neste capítulo foram realizadas as agregações dos controlos dos modelos escolhidos e incorporados nos vários núcleos da NIST - CSF. De seguida, foi apresentado e explicado o modelo desenvolvido, tendo por base o trabalho de agregação feito anteriormente.

CAPÍTULO 4

Validação do Modelo

O objetivo deste capítulo é apresentar o processo de validação do modelo desenvolvido. Este processo teve como base a realização de entrevistas a especialistas da área de cibersegurança.

A validação é uma etapa fundamental para aferir a aplicabilidade, relevância e robustez do modelo proposto, de forma a garantir que corresponde às necessidades das organizações nesta área.

Deste modo, foram conduzidas uma série de entrevistas com preparação prévia, compostas por uma série de perguntas que abordaram os principais pilares do modelo.

No que diz respeito à seleção dos entrevistados, foram inquiridas 49 pessoas via *LinkedIn*, das quais apenas 6 responderam positivamente e participaram nas entrevistas. Foram selecionados com base na sua experiência profissional dentro da área de cibersegurança, assegurando a credibilidade das suas contribuições.

Neste capítulo será apresentado o guião geral das entrevistas, bem como sínteses das respostas obtidas às mesmas. Por fim, irão ser apresentadas as alterações realizadas ao modelo, com base nas sugestões dos intervenientes.

4.1. Perfil dos entrevistados

De seguida, apresenta-se, na tabela 23, a caracterização dos perfis profissionais dos entrevistados.

Tabela 23. Perfil dos Especialistas Entrevistados

Nome	Posição	Anos Experiência
Especialista 1	*Information Security and Technology Risk*	3 anos
Especialista 2	CISO	16 anos
Especialista 3	*Head of Information Security and TI Risk*	8 anos
Especialista 4	*Cyber Security Engineer*	3 anos
Especialista 5	*Cyber Security Engineer*	7 anos
Especialista 6	*Senior Advisor Cyber Security and Fraud*	20 anos

4.2. Estrutura das entrevistas

Preparou-se uma apresentação estruturada que serviu de base para a condução das entrevistas com os especialistas. Estas tiveram como objetivo principal contextualizar os participantes relativamente ao trabalho desenvolvido.

A apresentação seguiu a seguinte estrutura:

- **Introdução e contextualização do projeto**

Iniciou-se com uma breve apresentação introdutória, onde foram apresentados os objetivos e as motivações do trabalho desenvolvido.

- **Apresentação e explicação do modelo**

Nesta fase, foi detalhado o modelo desenvolvido, com uma explicação dos seus componentes e modo de funcionamento.

- **Questões dirigidas aos entrevistados**

Procedeu-se à colocação de um conjunto de perguntas previamente elaboradas, com o intuito de recolher a opinião dos especialistas sobre a aplicabilidade, utilidade e exequibilidade do modelo. Serviram como guia para a entrevista, havendo sempre existido espaço para questões e temas adicionais.

As questões colocadas aos especialistas foram as seguintes:

• Na sua opinião, o modelo proposto cobre adequadamente os principais riscos enfrentados por instituições financeiras atualmente?

• Considera que a combinação dos modelos (NIST - CSF, PCI-DSS, SWIFT CSCF e CIS) é útil ou acrescenta complexidade desnecessária?

• Acredita que este modelo, tal como está estruturado, é realisticamente implementável numa organização bancária?

• Vê alguma função ou domínio da segurança que esteja sub-representado ou em excesso no modelo?

• O modelo pode ser entendido e utilizado por equipas não técnicas, como conformidade ou gestão de risco?

• Que desafios práticos prevê na implementação deste modelo?

• Há algum aspeto do modelo que deveria ser simplificado para facilitar a adoção?

• Há algum controlo, área ou prática que considera importante retirar/acrescentar ao modelo?

4.3. Contributos das Entrevistas

Antes de se prosseguir para o conteúdo proveniente das entrevistas realizadas aos especialistas, houve espaço para comentários prévios após a apresentação do modelo.

Para o especialista 6 existe uma preocupação com a mistura entre modelos de referência e regulamentação, como a PCI-DSS. Na opinião do especialista, são dois conceitos complementares, mas distintos, e seria importante distinguir os dois. No entanto, acrescenta que combinar as duas pode ser bastante pertinente, porque demonstra que a organização consegue cumprir ambas.

Outro ponto referido pelo mesmo é a questão de que organizações da área financeira estão inseridas no lote de organizações com as melhores infraestruturas de cibersegurança do mundo, e com todas as exigências que têm, especialmente regulamentares, qualquer adaptação de um quadro normativo deve ser extremamente abrangente, visto que não faria sentido para a banca implementar um modelo que deixasse de fora certos componentes.

Adiciona também o forte condicionamento que a banca em geral sofre no que diz respeito às regulamentações e exigências, ao ponto de parecer não fazer outra coisa que não auditorias. Na

empresa do setor bancário onde o especialista esteve, esta era alvo de sete ou oito auditorias anuais de cibersegurança. Quando uma empresa é posta sob grande pressão, acaba por apenas garantir que os quadros normativos são cumpridos, o que não deixa espaço suficiente para desenvolver outros temas inovadores ou relevantes.

4.3.1. Cobertura do modelo aos riscos das instituições bancárias

A pergunta realizada no decorrer da entrevista que diz respeito a este tema foi a seguinte: Na sua opinião, o modelo proposto cobre adequadamente os principais riscos enfrentados por instituições financeiras atualmente?

Na generalidade das entrevistas, as opiniões foram positivas, como referiu o especialista 1, tendo o modelo sido capaz de realizar uma análise de impacto de negócio e estratégias para recuperar tudo o que são sistemas de TI. O especialista 3 avalia o modelo como sendo inovador, apontando que o diagrama funciona como um guia, algo que, segundo refere, ainda não tinha observado. Normalmente, o mais comum é existir um conjunto de questões e controlos, mas não há propriamente uma árvore de decisão, como é o caso do modelo proposto.

No entanto, surgiram sugestões de melhoria na estrutura do modelo, nomeadamente nas categorias da NIST - CSF, como referiu o especialista 3, faria ligeiras alterações na estrutura do mesmo, dividindo as categorias da NIST - CSF apenas por categorias em detrimento dos passos, de acordo com a seguinte lógica: uma árvore para o núcleo Governo, outra para o Identificar, etc. Apesar de no modelo desenvolvido estarem ordenados de forma lógica, isso não significa que um seja menos importante que o outro.

O especialista 5 refere também a necessidade de incorporação do *Digital Operational Resilience Act* (DORA) no modelo desenvolvido.

Por outro lado, pode estar-se a perder conteúdo importante, como refere o especialista 6, que concorda que o risco está a ser coberto, se possa estar a deixar de incorporar a regulamentação na sua totalidade, olhando apenas para o risco pontual deste modelo.

O especialista 2 sugere um diagrama mais conciso, visto que o atual é consideravelmente extenso, contendo demasiadas questões e momentos de decisão. Sem um arranjo, pode acabar por transmitir alguma confusão.

4.3.2. Adequação dos modelos de referência

A pergunta realizada no decorrer da entrevista que diz respeito a este tema foi a seguinte: Considera que a combinação dos modelos de referência (NIST - CSF, PCI-DSS, SWIFT CSCF e CIS) é útil ou acrescenta complexidade desnecessária?

De forma abrangente, as opiniões foram positivas sobre a escolha dos modelos de referência, como aponta o especialista 1, que considera a PCI-DSS adequada devido à excelente contextualização no que respeita à aplicabilidade de cada controlo, e no caso da SWIFT CSCF como sendo ótima no tema das infraestruturas.

Já para o especialista 5, faz todo o sentido a NIST - CSF ser o alicerce do modelo, e os restantes quadros normativos foram também escolhas sensatas na opinião do mesmo.

Relativamente aos restantes modelos de referência, não se adiciona nada de desnecessário, quanto mais informação for possível centralizar, melhor. As escolhas feitas foram acertadas, por exemplo, para testes de intrusão, a NIST - CSF como base é uma excelente opção.

Para o especialista 2 é clara a utilidade do modelo, no sentido em que se está a unificar, visto que há um problema crónico nas instituições do setor em questão, o facto de terem de alinhar muita legislação e regulamentação.

O especialista 4 aborda o tema no seu próprio contexto, comentando a existência de uma equipa focada na área de normativos e conformidade, referindo que muitos dos normativos internos têm como base a documentação da NIST - CSF e da CIS. Como banco, a PCI-DSS e a SWIFT CSCF são também fundamentais para a atividade do próprio, sendo regularmente auditados no tema.

No entanto, um reparo que alguns dos especialistas fizeram foi o facto de que o modelo ganharia com a incorporação de mais quadros normativos, como a ISO 27001 ou o DORA, que é um novo regulamento aplicável ao setor bancário, a ISO 27001 por uma questão de boas práticas de gestão, *Network and Information Security Directive* (NIS2) ou ISO 22301 para abranger também diferentes temas.

O especialista 3 comentou sobre a importância do que o modelo pretende resolver, referindo que atualmente o setor bancário está a começar a desenvolver uma estrutura semelhante ao modelo conseguido no âmbito desta investigação, criando modelos de referência para o próprio banco que incorporam todos os requisitos legais e regulamentares. Por exemplo, cumprir com os objetivos da *Target*, cumprir com os objetivos da PCI-DSS e cumprir com os objetivos da SWIFT CSCF. Um modelo central com o complemento das demais é de extrema importância.

Por outro lado, para o especialista 6, a junção dos quadros normativos acrescenta complexidade desnecessária, devido à larga exigência existente. Logo, cruzá-las de forma uniformizada tornaria mais difícil garantir a sua implementação.

4.3.3. Exequibilidade do Modelo no Contexto Organizacional

As perguntas realizadas no decorrer da entrevista que dizem respeito a este tema foram as seguintes:

Acredita que este modelo, tal como está estruturado, é realisticamente implementável numa organização bancária?

Que desafios práticos prevê na implementação deste modelo?

De modo geral, a maioria dos entrevistados concordou que a implementação do modelo seria possível, apesar de existir sempre complexidade devido à dimensão das organizações financeiras, e ao se transpor o modelo para a realidade do banco será certamente complicado, considerando a dimensão do mesmo e os processos e políticas já bastante cimentadas no núcleo destas organizações, o que dificultaria a entrada de um novo modelo, como aborda o especialista 4. Os processos revelam-se difíceis de transpor da teoria para a prática. Do que o especialista observa, a conceção geral parece adequada, não só para um banco, mas também para qualquer tipo de organização num setor de atividade diferente, mostrando-se realista e exequível.

Para os especialistas 5 e 6, o modelo é realisticamente aplicável no contexto bancário, visto que se estão a agregar controlos já obrigatórios para este setor e que o modelo seria automatizado nas operações da organização.

O especialista 3 concorda com a afirmação de aplicabilidade do modelo no contexto bancário, como o mesmo explica, os bancos fazem uma avaliação controlo a controlo com base nos modelos de referência, definindo objetivos e avaliando o estado de maturidade dos mesmos. Através das avaliações, que têm por base os modelos de referência, as organizações definem os objetivos

estratégicos para os próximos anos, melhorando a maturidade nestes controlos.

Na mesma perspetiva, também o especialista 2 considera viável a implementação do modelo, uma vez que estas entidades estão habituadas a operar com este tipo de regulamentos. A referência da NIST - CSF é bastante usada, e a nível nacional complementada com o CNCS. Este enquadramento é conhecido pelas instituições, contribuindo para a estruturação e ligação entre os diversos regulamentos.

No que diz respeito aos desafios da implementação do modelo, realça-se o apoio da alta gestão, como afirma o especialista 3. A segurança deve estar presente em todas as áreas da organização, e apenas é eficaz se estiver embutida nos processos de negócio do banco. É necessário que seja concebida desde a fase de desenho, e ser incorporada em todas as atividades desenvolvidas na organização, o que implica tipicamente transformação, e para que tal transformação ocorra é preciso haver apoio das partes interessadas principais da instituição.

Outro desafio relaciona-se com os recursos disponíveis, como o orçamento. Estes processos envolvem avolumados investimentos, quer na monitorização de segurança, num SIEM, numa equipa SOC 24/7 ou um *Privileged Access Management* (PAM). Para o especialista 6, o mesmo problema é levantado, sendo de extrema importância que o modelo esteja apoiado e aprovado por parte da administração. O próprio experienciou situações, no decorrer de um ataque, onde a equipa de segurança, ao tentar tomar medidas, foi bloqueada pela administração, que não tinha o conhecimento das ações necessárias a tomar para mitigar o ataque.

O próprio explica que, no decorrer de um ataque a uma infraestrutura de um país, em que era necessário isolar uma máquina. Contudo, o advogado da empresa não permitiu, alegando que era ilegal, e a única entidade que o poderia permitir era o próprio governo. Este impedimento resultou na prolongação do ataque por mais duas horas do que seria necessário.

Por outro lado, o especialista 6 levanta também outra limitação, a falta de treino dos modelos. Mesmo que estes estejam muito bem estruturados, e que os processos de segurança estejam bem desenhados, se não existir treino regular, de forma a criarem-se hábitos de como agir no decorrer de um incidente, tudo o que está desenvolvido previamente fica em causa. É necessário criar-se hábito, reação, fazer sem ter de "pensar". O mesmo sugere a integração destes procedimentos na fase Detetar.

Outra dificuldade apontada relaciona-se com a constante mudança do mundo da cibersegurança, como aponta o especialista 4, abordando o seu contexto profissional, visto que, especialmente neste setor, os processos são bastante complexos, e quando um novo normativo é emitido ou uma boa prática a implementar nos processos é identificada, a implementação torna-se desafiante devido ao conjunto das dependências existentes. Qualquer alteração pode ter um impacto significativo no funcionamento dos processos organizacionais.

Verificou-se também outra dificuldade referida pelo especialista 1, que se relaciona com os casos de empresas que sejam subsidiárias, esta terá que estar em conformidade tanto com o modelo desenvolvido como com toda a regulamentação e normativos do grupo a que pertence.

O especialista 1 levantou também outra dificuldade, que diz respeito à complexidade do processo de interligação, quer entre os quadros normativos e os seus, como entre as políticas e normativos da própria organização.

Outra preocupação abordada é o facto de que o modelo irá ser implementado por vários departamentos e equipas diferentes, como refere o especialista 2, quem está responsável por cada tema, normalmente, não é uma única equipa, nem um único departamento. Por exemplo, no que respeita a NIST - CSF seria muito possivelmente dentro do âmbito das áreas de cibersegurança,

enquanto os temas de conformidade com os modelos da PCI-DSS ou SWIFT CSCF seriam do âmbito dos departamentos de pagamentos e TI, respetivamente.

O mesmo adiciona o obstáculo de implementação do modelo em organizações com elevada maturidade, como é o caso do setor bancário, visto que estas têm a tendência de criar modelos próprios, adaptados às suas necessidades, em detrimento de um modelo já existente, o que as obrigaria a compreender e a adaptar o mesmo às suas necessidades.

Em organizações de menor escala, como instituições de crédito e não propriamente banca de retalho, o modelo serviria uma maior utilidade.

A dificuldade a seguir apresentada pelo especialista 1 não é exclusiva ao modelo, mas comum à generalidade dos modelos de referência. A necessidade de garantir conformidade com todos os normativos e regulamentos, mas também com decretos emitidos por entidades reguladoras, no caso das organizações bancárias, pelo Banco de Portugal, e, no caso das seguradoras, pela Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF).

Além disso, outra dificuldade apontada, neste caso pelo especialista 5, é a resistência à mudança, quer devido ao custo associado, tanto na questão do tempo de adaptação a novas ferramentas de trabalho, como de recursos financeiros.

Noutra linha de pensamento, para o especialista 6, a engenharia social é um desafio complicado, devido à enorme pressão que o setor bancário sofre sobre o tema. É preocupante que a área financeira, que está estrangulada com tanta regulamentação, não tenha recursos para outros desafios. Os quadros normativos e modelos estão ainda, na opinião do especialista, focados nas velhas frases e maneiras de agir.

Por fim, o especialista 6 apresenta uma perspetiva de carácter futurista, sublinhando a importância da evolução da inteligência artificial na área de cibersegurança. Uma das preocupações destacadas relaciona-se com a qualidade dos dados utilizados no treino dos modelos de inteligência artificial, visto que estes nem sempre se encontram devidamente corretos, nem sempre existe um cuidado em garantir que os dados que estão a alimentar o modelo estão devidamente tratados, o que compromete o correto funcionamento dos sistemas. Acresce também o risco de interferência externa, concorrência, que pode interferir com os modelos desenvolvidos. Na eventualidade de estes não se encontrarem devidamente protegidos, corre-se o risco de ter inteligência artificial que será mais prejudicial do que benéfica.

4.3.4. Equilíbrio e Abrangência do Modelo

As perguntas realizadas no decorrer da entrevista que dizem respeito a este tema foram as seguintes:

Vê alguma função ou domínio da segurança que esteja sub-representado ou em excesso no modelo?

Há algum controlo, área ou prática que considera importante retirar/acrescentar ao modelo?

No que diz respeito à estrutura do diagrama, as opiniões foram semelhantes entre si, referindo-se que o mesmo se apresenta equilibrado e que não seria vantajoso aumentar o grau de complexidade, como refere o especialista 1. Paralelamente, o especialista 5 sublinha a importância de garantir a adaptação do modelo às necessidades do cliente, referindo que a base já se encontra desenvolvida.

No entanto, o núcleo Governo poderia estar mais desenvolvido no diagrama, como sugere o especialista 3, apesar de entender o posicionamento no topo do modelo, agindo como alicerce do mesmo, mas seria benéfico existir uma maior presença do núcleo em questão no modelo.

Na mesma linha de pensamento, também o núcleo Identificar poderia ser melhorado, na opinião do especialista 1, acrescentando a identificação das funções de negócio críticas, que seriam de extrema importância de modo a definir uma hierarquia de criticidade com o objetivo de alocação de recursos de acordo com a prioridade dada. O DORA é muito holístico neste aspeto e demonstra a importância desta identificação, uma vez que terá impacto em diversas dimensões, como a gestão de incidentes, a gestão de fornecedores e a gestão do risco. Por exemplo, no caso dos testes de intrusão, estes são obrigatórios a todos os sistemas que suportam funções críticas. De igual modo, na gestão de incidentes é obrigatório reportar os mesmos às entidades de supervisão, todos os que estejam relacionados com sistemas que suportam funções críticas, o que demonstra a importância desta análise, concretizada, por exemplo, num *Business Impact Analysis* (BIA).

O especialista 4 sugere também complementar o processo de identificação de ativos, com a classificação dos mesmos.

A recomendação seguinte está relacionada com a monitorização, salientando a necessidade de existência de um programa de gestão de vulnerabilidades. Principalmente no contexto português, dado que grande parte do setor bancário ainda recorre à *mainframe*, que tem componentes de infraestrutura que não são frequentemente atualizadas, sendo por isso especialmente importante gerir estas vulnerabilidades antigas, como conclui o especialista 3.

Como dito anteriormente, para o especialista 5 apenas seria necessário acrescentar o DORA. O especialista 2 aborda a importância do processo de gestão de terceiras partes, um processo fundamental e que a sua integração no modelo seria bastante vantajosa. Muito importante em duas vertentes. A primeira relaciona-se com a ocorrência de incidentes em fornecedores, que podem impactar diretamente a instituição. Nestes casos, a deteção pode não ser imediata, dado que não existe, necessariamente, monitorização direta dos ativos do fornecedor.

A segunda vertente diz respeito à capacidade de resposta, e na dependência dos fornecedores, dado que grande parte das instituições bancárias recorre à terceirização de TI, o que leva a que certas atividades críticas da organização estejam dependentes do prestador de serviços. Atividades como administração de sistemas, SOC externalizado ou ambiente *cloud*, por exemplo.

O mesmo aponta o que poderia complementar o modelo atendendo a necessidades específicas do setor bancário relacionadas com regulamentações e normativos, como é o caso do DORA, aplicável a entidades críticas, *Markets in Crypto-Assets* (MiCA), para os criptoativos, e a diretiva NIS2 para todos os serviços essenciais e infraestruturas críticas. De acordo com a análise efetuada, estas dimensões ficam de fora do âmbito do modelo. Ao submeter o modelo à avaliação de uma instituição bancária, a questão de aplicabilidade no cumprimento das exigências anteriores iria ser levantada. Reconhece-se, contudo, que desenvolver um modelo que cumpra com o DORA, NIS2, e outros regulamentos resultaria inevitavelmente numa solução excessivamente complexa. Por fim, o especialista 6 acrescentaria a questão anteriormente debatida, treino, na fase de Detetar. Esta rotina deve ser executada pelo menos duas vezes por ano, apesar de o especialista aconselhar pelo menos quatro.

4.3.5. Clareza e Acessibilidade do modelo para pessoas não especializadas na área

A pergunta realizada no decorrer da entrevista que diz respeito a este tema foi a seguinte: O modelo pode ser entendido e utilizado por profissionais fora da área de cibersegurança?

Neste aspeto houve uma maior divergência nas opiniões dos especialistas, apesar de para a maioria o modelo estar compreensível, não significa que a sua implementação seja fácil para

profissionais fora da área de cibersegurança. Saber o que priorizar será complicado para estes colaboradores. Todas as organizações têm o seu próprio contexto, e apesar dos modelos de referência serem vitais para a organização, existe uma necessidade posterior de tomada de decisão, que cabe aos responsáveis de segurança.

O especialista 2 partilha uma opinião semelhante à do especialista 3, que compreender o diagrama não seria problemático. No entanto, dependeria sempre do histórico académico e profissional das pessoas em questão. Colaboradores habituados a temas de conformidade teriam mais facilidade. Por outro lado, se for uma equipa não familiarizada com os temas, seria complicado.

No mesmo âmbito também o especialista 1 refere a questão da implementação, que a seu ver o modelo não seria facilmente entendido e implementado por profissionais fora da área de cibersegurança, uma vez que vai existir muito contacto com fornecedores, e caso seja realizado na própria entidade, vai exigir a alocação de recursos específicos para cada uma das áreas e controlos.

O especialista 4 apresentou reticência na questão de implementação, receando que atividades como avaliações de risco pudessem ficar incompletas. No que diz respeito ao entendimento, dependeria da área dos colaboradores.

Já para o especialista 6, a implementação do modelo seria um processo bastante complicado, visto que os profissionais não familiarizados com a área apresentam bastante dificuldade na compreensão da lógica e a correta implementação dos controlos. Há um desconhecimento geral, fora da área de cibersegurança, sobre a correta implementação dos controlos. É um dos problemas mais comuns observados em auditorias, em que os controlos se encontram incorretamente implementados, devido à falha na interpretação dos mesmos.

4.3.6. Simplicidade de Adoção

A pergunta realizada no decorrer da entrevista que diz respeito a este tema foi a seguinte: Há algum aspeto do modelo que deveria ser simplificado para facilitar a adoção?

Neste tópico foi questionado se algum aspeto do modelo deveria ser simplificado, de forma a facilitar a sua implementação. As opiniões foram bastante semelhantes entre si, onde a maioria dos especialistas considera que o mesmo não seria necessário. No entanto, existem bastantes componentes que devem estar implícitas, como aponta o especialista 1, por exemplo, na questão dos planos de recuperação, é necessário o desenvolvimento de um estudo de ativos críticos ou a avaliação de riscos e falhas. Da mesma forma, é essencial identificar o grau de confidencialidade da informação, assegurando a integração no inventário de ativos.

Paralelamente, os especialistas 2, 3, 4 e 6 também partilham a opinião de que o modelo se encontra equilibrado e que não seria necessária nenhuma alteração neste sentido, apontando que o modelo se encontra funcional, não fugindo às regras de boas práticas.

Por fim, o especialista 5 apresenta duas perspetivas diferentes. Na perspetiva de negócio, para o especialista, o modelo encontra-se demasiado técnico, consistindo essencialmente num fluxograma, sem explicar claramente o problema que se pretende resolver e a justificação da sua necessidade. Na perspetiva técnica, encontra-se adequado e bem estruturado.

4.4. Resultados das Entrevistas

De seguida, apresenta-se uma síntese, dividida por tema abordado, dos resultados das entrevistas.

4.4.1. Cobertura do modelo aos riscos das instituições bancárias

O modelo foi de modo geral bem recebido, sendo considerado útil e inovador. Destaca-se a sua estrutura em árvore de decisão, o que o diferencia de abordagens comuns.

Por outro lado, foram apontadas oportunidades de melhoria, como reorganizar as categorias da NIST - CSF, propondo-se a separação por categorias em vez etapas. Foi também salientada a ausência do DORA, o que limita a abrangência do modelo. Adicionalmente, levantou-se a questão de que, ao focar apenas no risco, certas componentes regulamentares possam estar a ser deixadas de parte. Por fim, foi sugerida uma simplificação do diagrama, dado o seu tamanho e complexidade.

4.4.2. Adequação das modelos de referência

As opiniões recolhidas sobre os modelos de referência selecionados foram, de forma geral, bastante positivas. Destacou-se a PCI-DSS pela clareza e aplicabilidade dos seus controlos, e a SWIFT CSCF, pela adequação às exigências específicas de infraestruturas críticas. A escolha da NIST - CSF como base do modelo foi muito elogiada, sendo considerada uma estrutura sólida e abrangente, capaz de sustentar a integração dos restantes quadros normativos.

A utilidade do modelo foi também reconhecida, sobretudo pelo seu contributo para a centralização de requisitos regulatórios e legais, respondendo a uma necessidade das organizações financeiras. Foi valorizada a centralização da informação e a tentativa de consolidar múltiplas exigências normativas num único modelo.

No entanto, foram também apontadas oportunidades de melhoria. Foi novamente sugerida a inclusão de outros modelos de referência relevantes, como o DORA, a ISO 27001, a NIS2 e a ISO 22301, de modo a alargar o alcance do modelo a temas como a resiliência e as boas práticas de gestão. Por outro lado, corre-se o risco de criar complexidade excessiva. Essa complexidade pode dificultar a implementação prática do modelo, especialmente em contextos organizacionais sobrecarregados por exigências normativas.

4.4.3. Exequibilidade do Modelo no Contexto Organizacional

A maioria dos entrevistados considera que o modelo proposto é aplicável e passível de implementação na área em questão, mesmo reconhecendo a complexidade inerente a organizações de grande dimensão.

Ainda assim, foram identificados diversos desafios à sua implementação, como a necessidade de envolvimento e apoio da gestão de topo. Sem o compromisso da administração, a segurança tende a ser tratada como um aditivo aos processos, e não como parte fundamental do modo operacional da organização. Além disso, os custos associados à implementação, tanto ao nível de tecnologia como de recursos humanos, constituem um obstáculo relevante.

A falta de treino prático e de exercícios regulares de cibersegurança também foi apontada como uma limitação. A eficácia dos controlos depende não só do seu desenho, mas da capacidade de reação das equipas aquando dos incidentes.

Outros desafios incluem a necessidade de alinhar o modelo com eventuais subsidiárias, a dificuldade de integrar e consolidar diferentes quadros normativos nos procedimentos internos, e o facto de que múltiplos departamentos partilham a responsabilidade pela conformidade, o que exige coordenação entre os mesmos.

Foi também destacada uma limitação natural do modelo: a sua menor aceitação em organi-

zações com elevada maturidade, como grandes bancos, que tendem a criar estruturas próprias, ajustadas às suas necessidades. O modelo pode ser mais uma mais-valia para instituições de menor dimensão. Obstáculos comuns à adoção de novas ferramentas e modelos, como a resistência à mudança e a escassez de tempo para implementação nestas organizações.

Por fim, foi levantada uma perspetiva sobre o futuro da cibersegurança, destacando a importância crescente da inteligência artificial, mas alertando para os riscos associados a dados mal preparados e à potencial manipulação por parte de terceiros. A engenharia social continua a ser um desafio significativo, especialmente num setor tão pressionado por obrigações legais.

4.4.4. Equilíbrio e Abrangência do Modelo

As opiniões foram bastante positivas, sendo que a maioria dos participantes considerou que o modelo apresenta uma estrutura equilibrada, sendo considerado adequado na sua forma atual.

Aponta-se a necessidade de complementar os domínios de Governo e Identificar, incluindo a definição de funções de negócio críticas, políticas, procedimentos e papéis como o CISO.

Recomenda-se também a classificação dos ativos após a sua inventariação e a inclusão de um programa de gestão de vulnerabilidades, especialmente relevante em ambientes com infraestruturas antigas. A gestão de terceiras partes deve ser mais detalhada, dado o impacto potencial de incidentes em fornecedores e a dependência destes na resposta a incidentes.

4.4.5. Clareza e Acessibilidade do modelo para pessoas não especializadas na área

As opiniões sobre a aplicabilidade do modelo foram diversas. Embora a maioria considere o modelo compreensível, a sua implementação revela-se de certo modo complexa para quem não possui formação ou experiência em cibersegurança. O seu entendimento é, em geral, acessível, mas a correta priorização e aplicação dos controlos depende do contexto organizacional e do perfil dos intervenientes. A implementação requer conhecimento específico, sobretudo em áreas como gestão de risco, conformidade e interação com fornecedores. Sem essa base, o modelo poderá ser mal interpretado ou aplicado de forma inadequada.

4.4.6. Simplicidade de Adoção

A maioria dos participantes considera que o modelo não deve ser simplificado, uma vez que a sua complexidade é necessária para assegurar a qualidade da implementação. É defendido que muitos elementos essenciais devem estar implícitos e bem fundamentados desde a origem.

Foi também apontado que o modelo poderá parecer excessivamente técnico, carecendo de uma explicitação clara do problema que pretende resolver e do seu valor estratégico. Ainda assim, do ponto de vista técnico, está equilibrado e funcional.

4.4.7. Síntese Final das Entrevistas

As entrevistas realizadas com especialistas do setor de cibersegurança revelaram, de forma geral, uma receção positiva ao modelo proposto, considerando-o abrangente, funcional e inovador no seu formato, destacando-se a estrutura em árvore de decisão. O modelo é visto como uma ferramenta útil para organizar e alinhar práticas de segurança com diversos modelos de referência relevantes, especialmente no contexto bancário.

Contudo, surgiram algumas sugestões de melhoria, nomeadamente a necessidade de integrar

regulamentações recentes como o DORA, NIS2 ou ISO 27001, bem como reforçar domínios como o Governo, identificação de funções críticas, classificação de ativos, gestão de vulnerabilidades e terceiras partes. Adicionalmente, foi recomendada a inclusão de uma componente prática de treino regular para assegurar a eficácia operacional.

A aplicabilidade do modelo nas organizações bancárias foi, de modo geral, validada, embora os especialistas tenham salientado desafios relevantes: o apoio da gestão de topo, orçamentos limitados, complexidade organizacional, resistência à mudança e dificuldade na adaptação a entidades com elevada maturidade.

Quanto à clareza e acessibilidade do modelo, as opiniões foram mais díspares: embora compreensível para profissionais com alguma experiência, a sua implementação por pessoas fora da área de cibersegurança poderá ser difícil, especialmente sem conhecimento prévio. Ainda assim, a maioria considera o modelo equilibrado e não demasiado complexo.

De seguida apresenta-se a tabela 24, com um resumo de cada tema.

Tabela 24. Síntese Entrevistas

Tema	Síntese
Perceção geral do modelo	Bem recebido e considerado útil e inovador, destacando-se a estrutura em árvore de decisão. Reconhece-se a sua relevância para o contexto bancário e a capacidade de representar os riscos de forma clara e estruturada.
Sugestões de melhoria	Integração de regulamentações como DORA, NIS2 e ISO 27001, bem como o reforço de domínios como Governo, funções críticas, classificação de ativos, gestão de vulnerabilidades e terceiras partes. Também foi sugerida a inclusão de treino prático e regular para reforçar a eficácia operacional.
Aplicabilidade nas organizações	Aplicabilidade validada, mas foram identificados desafios relevantes, como a necessidade de apoio da gestão de topo, limitações orçamentais, complexidade organizacional, resistência à mudança e adaptação difícil em entidades de elevada maturidade.
Clareza e acessibilidade	Compreensível para profissionais experientes, podendo ser difícil de aplicar por pessoas sem formação em cibersegurança. Ainda assim, é considerado equilibrado e não excessivamente complexo.

4.5. Alterações Sugeridas

De seguida, apresentam-se as alterações realizadas ao modelo proposto, resultantes das entrevistas conduzidas com os profissionais da área. As entrevistas tiveram como principal objetivo recolher avaliações sobre a utilidade, clareza e aplicabilidade do modelo desenvolvido, bem como identificar oportunidades de melhoria.

Importa salientar que nem todas as sugestões recolhidas foram implementadas. A seleção das alterações a adotar foi feita com base em dois critérios principais: a relevância da sugestão face aos objetivos definidos para esta dissertação e a viabilidade da sua concretização no tempo

disponível. Foram, assim, priorizadas as contribuições que acrescentavam valor ao modelo, sem comprometer a sua estrutura, coerência e aplicabilidade prática.

Segue-se a primeira alteração sugerida e aplicada, que diz respeito ao núcleo Identificar, mais concretamente adicionando uma secção, "funções críticas de negócio identificadas?", que trata a identificação de linhas ou funções críticas na organização, que têm uma enorme relevância visto que é fundamental existir uma hierarquia de criticidade do que é necessário proteger. Ainda no que respeita ao núcleo Identificar, foi implementada outra sugestão, que diz respeito à necessidade de, para além de existirem processos de revisão dos inventários de ativos, existirem também processos definidos para a classificação dos mesmos, garantindo que os recursos recebem o nível de proteção que precisam.

Apresentam-se na figura 11 as alterações efetuadas, destacadas pelos retângulos vermelhos:

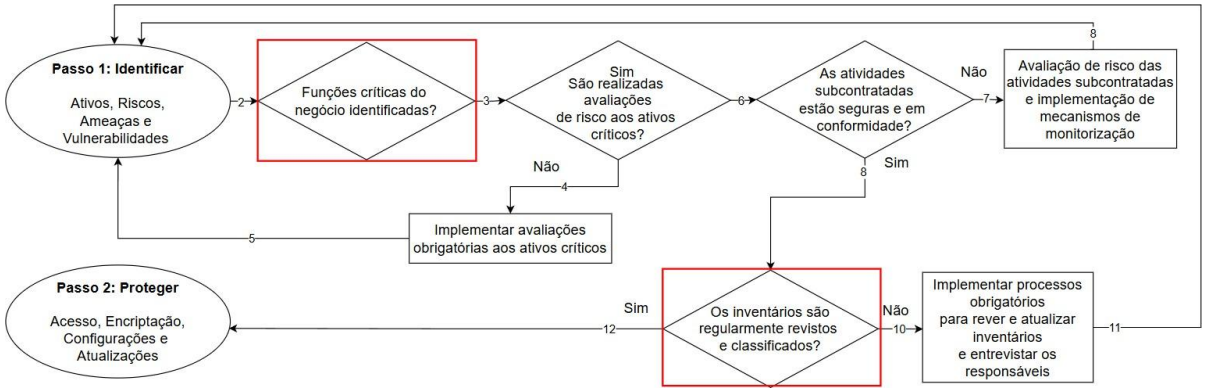


Figura 11. Alteração sugerida: Identificação de Funções Críticas do Negócio e Classificação de Inventários

A recomendação seguinte está relacionada com os processos de monitorização, através da criação de um programa específico para a gestão de vulnerabilidades. Esta etapa visa assegurar que as organizações têm a capacidade de identificar, avaliar e priorizar vulnerabilidades de forma contínua, minimizando o tempo de exposição.

A gestão de vulnerabilidades deve incluir a monitorização regular de fontes de *threat intelligence*, sistemas de análise de vulnerabilidades, um inventário completo e atualizado de ativos e um processo claro de correção e mitigação. Deve também existir uma priorização com base no risco, tendo em conta a criticidade do ativo, potencial impacto e facilidade de exploração.

Deve ter-se em atenção as infraestruturas e componentes antigos, frequentemente presentes em instituições financeiras. Estes sistemas, por vezes críticos para o negócio, tendem a estar fora de suporte, com atualizações limitadas ou inexistentes, tornando-se alvos muito apetecíveis para os atacantes.

A implementação de um processo eficaz de gestão de vulnerabilidades não só reduz significativamente a superfície de ataque como também contribui para uma resposta mais rápida.

Paralelamente ao núcleo envolvido na sugestão anterior, foi também recomendada a inclusão da vertente de treino no modelo, particularmente associada à fase de Detetar. Esta prática visa garantir que as equipas estão preparadas para reagir de forma eficaz a incidentes de segurança. Foi recomendado que estes exercícios de treino sejam realizados pelo menos duas vezes ao ano, sendo idealmente conduzidos trimestralmente.

De seguida, apresentam-se na figura 12 as alterações efetuadas, destacadas pelos retângulos

vermelhos:

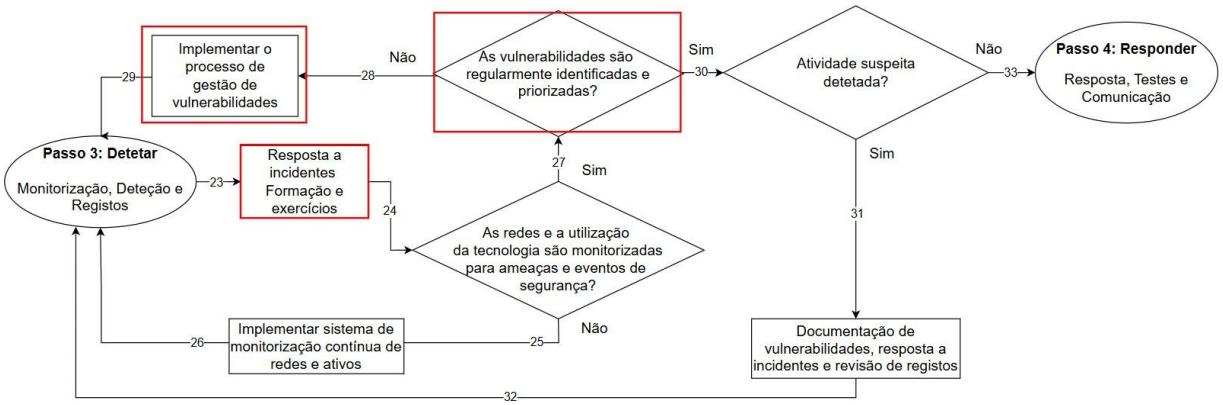


Figura 12. Alteração sugerida: Gestão de Vulnerabilidades e Sensibilização/Treino

A alteração que se apresenta de seguida está relacionada com a gestão de terceiras partes, uma componente crítica da cibersegurança no setor bancário, devendo estar devidamente representada no modelo proposto. A crescente dependência de fornecedores, seja através de terceirização de sistemas, serviços *cloud* ou operações de segurança, cria uma exposição significativa a riscos que nem sempre estão sob controlo direto da organização.

Este risco manifesta-se em duas vertentes principais. A primeira diz respeito à possibilidade de ocorrência de um incidente no fornecedor que, direta ou indiretamente, afete a instituição financeira. Nesses casos, a deteção pode ser difícil, visto que muitas vezes não existe monitorização direta sobre os ativos do fornecedor, e a organização depende da comunicação voluntária do incidente por parte do fornecedor.

A segunda vertente relaciona-se com a capacidade de resposta. Quando funções críticas estão delegadas a terceiros, a resposta a incidentes irá depender diretamente da disponibilidade, rapidez e eficácia dos mesmos. Esta dependência reforça a importância de cláusulas contratuais claras, planos de resposta colaborativos e canais de comunicação definidos.

De seguida, apresenta-se na figura 12 a alteração efetuada, destacada pelo retângulo vermelho:

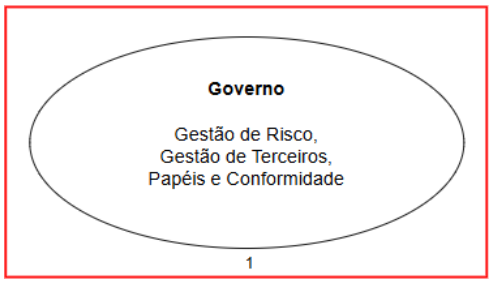


Figura 13. Alteração sugerida: Processo de Gestão de Terceiras Partes

CAPÍTULO 5

Conclusões

Neste capítulo são apresentadas as principais conclusões resultantes do trabalho desenvolvido ao longo desta investigação.

Adicionalmente, será feita uma reflexão crítica de modo a perceber se a questão de investigação inicialmente proposta foi respondida com sucesso, tendo em conta os objetivos definidos e os resultados alcançados.

Por fim, este capítulo incluirá sugestões de trabalho futuro, com o objetivo de servir como base para investigações posteriores.

5.1. Conclusões do Trabalho

Através da análise detalhada de alguns dos principais modelos de referência reconhecidos internacionalmente, foi possível identificar e consolidar um conjunto robusto de práticas de cibersegurança fundamentais. Estas práticas foram agregadas num modelo e adaptadas ao contexto específico das instituições do setor bancário.

O modelo proposto está representado de forma esquemática num diagrama, que apresenta de forma sequencial os passos a seguir para a sua implementação. Cada etapa do diagrama foi acompanhada de uma explicação detalhada, clarificando as ações a adotar, a lógica por detrás da sua ordem de execução, e o seu contributo específico para a mitigação dos riscos enfrentados pelas instituições financeiras.

A abordagem adotada permite às organizações aplicar o modelo de forma prática e escalável, enquanto assegura um alinhamento com os principais referenciais normativos e regulamentares do setor. A validação qualitativa realizada junto de profissionais da área reforçou a utilidade, pertinência e clareza do modelo. Foram ainda recolhidas sugestões de melhoria, algumas das quais foram incorporadas na versão final do modelo, reforçando a sua aplicabilidade. Não obstante, importa referir algumas limitações levantadas ao longo da investigação. Em primeiro lugar, a enorme abrangência dos quadros normativos, diretrizes e regulamentação existentes, sendo possível que determinados controlos e boas práticas não tenham sido incluídas no modelo. Em segundo lugar, a constante mudança presente no que diz respeito às regulamentações e tecnologia, o que implica que qualquer modelo possa perder a sua relevância num curto espaço de tempo. Por último, destaca-se a dificuldade em reunir um número mais alargado de especialistas disponíveis para realizar as entrevistas de validação do modelo, o que restringiu a diversidade de perspetivas recolhidas.

Assim, conclui-se que a dissertação respondeu adequadamente à questão de investigação, ao identificar, organizar e justificar práticas de segurança fundamentais com base em normas consolidadas e adaptá-las ao setor bancário sob a forma de um modelo claro e exequível.

5.2. Trabalho Futuro

Tendo em conta os resultados alcançados neste trabalho e as sugestões recolhidas durante as entrevistas, existem várias oportunidades para trabalhos futuros, aprofundando o que foi desenvolvido.

Uma primeira direção poderia centrar-se na validação prática do modelo desenvolvido, aplicando-o em instituições bancárias reais, de modo a avaliar a eficácia e aplicabilidade do mesmo, o que permitiria testar a usabilidade, identificar lapsos e recolher dados de desempenho que apoiem ou contradigam os pressupostos do modelo.

Outro caminho possível seria o desenvolvimento de uma ferramenta digital baseada no modelo desenvolvido, que poderia permitir às organizações autoavaliarem o seu nível de conformidade e maturidade. Para tal, competências de engenharia de *software*, segurança da informação e experiência do utilizador seriam fundamentais, podendo dar origem a um trabalho técnico.

Adicionalmente, seria também interessante explorar a expansão do modelo a outros setores, como a saúde, energia ou telecomunicações. Essa adaptação permitiria estudar a flexibilidade e escalabilidade do modelo, bem como identificar controlos adicionais ou específicos a integrar consoante o setor em questão.

Por fim, outra vertente possível de exploração futura será a integração do modelo com regulamentações emergentes, como o DORA.

Referências Bibliográficas

[1] A. Marotta e K. Pearlson, «A culture of cybersecurity at Banca Popolare di Sondrio,» 2019.

[2] L. C. Stoica, «Considerations On Artificial Intelligence And Cybernetic Risks, A New Paradigm Of The Banking Financial System,» *Journal of Smart Economic Growth*, vol. 7, n.º 2, pp. 93–101, 2022. ISSN: 2537-141X

[3] A. Raghavan e L. Parthiban, «The effect of cybercrime on a Bank's finances,» *International Journal of Current Research & Academic Review*, vol. 2, n.º 2, pp. 173–178, 2014. ISSN: 2347-3215

[4] C. P. Skinner, «Bank disclosures of cyber exposure,» *Iowa L. Rev.*, vol. 105, p. 239, 2019.

[5] S. Abulhaija, S. Hattab e A. Qusef, «Cyber Security Awareness, Knowledge and Behavior in the Banking Sector in Jordan,» em *2022 13th International Conference on Information and Communication Systems (ICICS)*, IEEE, 2022, pp. 48–53. doi: 10.1109/ICICS55353.2022.9811212

[6] Centro Nacional de Cibersegurança, *Relatório de Riscos e Conflitos no Ciberespaço 2023*, dez. de 2023. URL: https://www.cncs.gov.pt/docs/rel-riscosconflitos2023-obcibercncs.pdf.

[7] A. Fazio e F. Zuffranieri, «Interbank payment system architecture from a cyber security perspective,» *Bank of Italy Occasional Paper*, n.º 418, 2018. doi: 10.2139/ssrn.3123094

[8] O. A. AUSTIN-OLOWO, I. O. AILEMEN e L. BUSARI, «CYBERSECURITY ISSUES AFFECTING ONLINE BANKING AND TRANSACTIONS IN NIGERIA,» ISSN:3027-0510

[9] A. Annarelli, F. Nonino e G. Palombi, «Understanding the management of cyber resilient systems,» *Computers & industrial engineering*, vol. 149, p. 106 829, 2020. doi: 10.1016/j.cie.2020.106829

[10] T. Somogyi e R. Nagy, «Cyber threats and security challenges in the Hungarian financial sector,» *Contemporary Military Challenges/Sodobni Vojaški Izzivi*, vol. 24, n.º 3, pp. 15–29, 2022. doi: 10.33179/bsv.99.svi.11.cmc.24.3.1

[11] X. M. Liu, «A risk-based approach to cybersecurity: a case study of financial messaging networks data breaches,» *The Coastal Business Journal*, vol. 18, n.º 1, p. 2, 2021. ISSN: 2163-9280

[12] N. H. Al-Kumaim e S. K. Alshamsi, «Determinants of cyberattack prevention in UAE financial organizations: assessing the mediating role of cybersecurity leadership,» *Applied Sciences*, vol. 13, n.º 10, p. 5839, 2023. doi: 10.3390/app13105839

[13] K. Peffers, T. Tuunanen, M. A. Rothenberger e S. Chatterjee, «A design science research methodology for information systems research,» *Journal of management information systems*, vol. 24, n.º 3, pp. 45–77, 2007. doi: 10.2753/MIS0742-1222240302

[14] M. Peihani, «Regulation of cyber risk in the banking system: a Canadian case study,» *Journal of Financial Regulation*, vol. 8, n.º 2, pp. 139–161, 2022. doi: 10.1093/jfr/fjac006

[15] S. Tikhonov e M. Bondarenko, «The Practice of Malware Protection for Commercial Banking.,» *ISSA Journal*, vol. 14, n.º 4, 2016. ISSN: 1949-0550

[16] N. P. Matlala, «Behavioural Insights Into Cybersecurity Practices Among Digital Banking Consumers in South Africa,» *Indonesian Journal of Business Analytics*, vol. 3, n.º 4, pp. 1425–1442, 2023. doi: 10.55927/ijba.v3i4.5515

[17] F. X. ADRIAN e G. WANG, «Measure the Level Capability It Governance in Effectiveness Internal Control for Cybersecurity Using the Cobit 2019 in Organization: Banking Company,» *Journal of Theoretical and Applied Information Technology*, vol. 101, n.º 5, 2023. ISSN: 1992-8645

[18] V. Wang, H. Nnaji e J. Jung, «Internet banking in Nigeria: Cyber security breaches, practices and capability,» *International Journal of Law, Crime and Justice*, vol. 62, p. 100 415, 2020. doi: 10.1016/j.ijlcj.2020.100415

[19] A. Kosse e Z. Lu, «Transmission of cyber risk through the Canadian wholesale payment system,» *Journal of Financial Market Infrastructures*, vol. 10, n.º 4, 2022. doi: 10.21314/JFMI.2023.001

[20] M. J. Sembay, D. D. J. de Macedo, L. P. Júnior, R. M. M. Braga e A. Sarasa-Cabezuelo, «Provenance data management in health information systems: a systematic literature review,» *Journal of Personalized Medicine*, vol. 13, n.º 6, p. 991, 2023. doi: 10.3390/jpm13060991

[21] M. Pradana, A. Silvianita, P. N. Madiawati, D. Calandra, F. Lanzalonga, M. Oppioli et al., «A Guidance to Systematic Literature Review to Young Researchers by Telkom University and the University of Turin,» *To Maega: Jurnal Pengabdian Masyarakat*, vol. 6, n.º 2, pp. 409–417, 2023. doi: 10.35914/tomaega.v6i2.1915

[22] A. L. Johnson, «Cybersecurity for financial institutions: The integral role of information sharing in cyber attack mitigation,» *NC Banking Inst.*, vol. 20, p. 277, 2016.

[23] J. C. Najar Pacheco e H. C. I. Alemán Novoa, «Technology and bank fraud.,» *Visión electrónica*, vol. 11, n.º 2, 2017. doi: 10.14483/22484728.12922

[24] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan et al., «The PRISMA 2020 statement: an updated guideline for reporting systematic reviews,» *bmj*, vol. 372, 2021. doi: 10.1136/bmj.n71

[25] M. J. Page, J. E. McKenzie, P. M. Bossuyt, I. Boutron, T. C. Hoffmann, C. D. Mulrow, L. Shamseer, J. M. Tetzlaff, E. A. Akl, S. E. Brennan et al., «A declaração PRISMA 2020: diretriz atualizada para relatar revisões sistemáticas,» *Revista panamericana de salud publica*, vol. 46, e112, 2023. doi: 10.26633/RPSP.2022.112

[26] *Os Utilizadores de Homebanking e Riscos de Segurança mais Relevantes Associados*, Relatório académico, 2023.

[27] D. Kuttiyappan et al., «Improving the Cyber Security over Banking Sector by Detecting the Malicious Attacks Using the Wrapper Stepwise Resnet Classifier.,» *KSII Transactions on Internet & Information Systems*, vol. 17, n.º 6, 2023. doi: 10.3837/tiis.2023.06.007

[28] A. K. AlSalamah, «Security Risk Management in Online System,» em *2017 5th Intl Conf on Applied Computing and Information Technology/4th Intl Conf on Computational Science/Intelligence and Applied Informatics/2nd Intl Conf on Big Data, Cloud Computing, Data Science (ACIT-CSII-BCD)*, 2017, pp. 119–124. doi: 10.1109/ACIT-CSII-BCD.2017.59.

[29] S. Gadalay, «Cybersecurity Assessments,» *International Journal of Recent Technology and Engineering (IJRTE)*, vol. 9, n.º 4, pp. 330–333, nov. de 2020. doi: 10.35940/ijrte.

D5004.119420. URL: https://www.ijrte.org/wp-content/uploads/papers/v9i4/D5004119420.pdf.

[30] C. Koto, R. Smith e B. Schutte, «Cyber risk management frameworks for the South African banking industry,» International Conference on Public Administration e Development . . ., 2021.

[31] S. Nayak e J. Chandiramani, «A crisis that changed the banking scenario in India: exploring the role of ethics in business,» *Asian Journal of Business Ethics*, vol. 11, n.º Suppl 1, pp. 7–32, 2022. doi: 10.1007/s13520-022-00151-4

[32] M. L. Yaeger, M. G. R. Goldstein e K. G. Monty, «The Bangladesh bank hack and compliance programmes,» *E-Finance & Payments Law & Policy*, pp. 3–5, mai. de 2016, Special report on cyber crime and AML compliance.

[33] J. M. Alghazo, Z. Kazmi e G. Latif, «Cyber security analysis of internet banking in emerging countries: User and bank perspectives,» em *2017 4th IEEE international conference on engineering technologies and applied sciences (ICETAS)*, IEEE, 2017, pp. 1–6. doi: 10.1109/ICETAS.2017.8277910

[34] T. Godbole, S. Gochhait e D. Ghosh, «Developing a framework to measure cyber resilience behaviour of Indian bank employees,» em *ICT with Intelligent Applications: Proceedings of ICTIS 2021, Volume 1*, Springer, 2022, pp. 299–309. doi: 10.1007/978-981-16-4177-0_31

[35] «Appendix A - Plan-do-check-act (PDCA) cycle,» em *Introduction to Energy Essentials*, B. Zohuri e P. McDaniel, eds., Academic Press, 2021, pp. 549–558, ISBN: 978-0-323-90152-9. doi: 10.1016/B978-0-323-90152-9.00015-3.

[36] R. Von Solms e J. Van Niekerk, «From information security to cyber security,» *computers & security*, vol. 38, pp. 97–102, 2013. doi: 10.1016/j.cose.2013.04.004

[37] C. Pascoe, S. Quinn e K. Scarfone, «The NIST Cybersecurity Framework (CSF) 2.0,» 2024. doi: 10.6028/NIST.CSWP.29

[38] T. Miller, A. Staves, S. Maesschalck, M. Sturdee e B. Green, «Looking back to look forward: Lessons learnt from cyber-attacks on industrial control systems,» *International Journal of Critical Infrastructure Protection*, vol. 35, p. 100 464, 2021. doi: 10.1016/j.ijcip.2021.100464

[39] Center for Internet Security, «CIS Controls v8: Critical Security Controls,» rel. téc., 2023. URL: https://www.cisecurity.org/controls/v8.

[40] P. S. S. Council, «PCI Data Security Standard (PCI DSS) v4.0.1,» PCI Security Standards Council, rel. téc., 2024, Accessed: 2024-10-12.

[41] https://listings.pcisecuritystandards.org/documents/PCI_DSS-QRG-v3_2_1.pdf, [Accessed 01-05-2025].

[42] SWIFT, «Customer Security Controls Framework (CSCF) - v2024,» SWIFT, rel. téc., 2023, Accessed: 2024-10-12.

[43] PCI Security Standards Council, *Mapping PCI DSS to the NIST Cybersecurity Framework: At-a-Glance*, https://www.pcisecuritystandards.org/pdfs/Mapping-PCI-DSS-to-NIST-Framework-At-a-Glance.pdf, Accessed: 2025-08-23, 2020.

[44] 6clicks, *Comparison Overview*, https://www.6clicks.com/resources/overview?selected=comparison, Accessed: 2024-08-09, 2024.

[45] K. Rigopoulos, S. Quinn, C. Pascoe, J. Marron, A. Mahn e D. Topper, «NIST Cybersecurity Framework 2.0: Resource & Overview Guide,» 2024. doi: 10.6028/NIST.SP.1299

[46] S. B. Q.-S. Guide, «NIST Cybersecurity Framework 2.0,» 2024. doi: 10.6028/NIST.CSWP.29

APÊNDICE A

Modelo

De seguida, apresenta-se o modelo dividido em duas imagens, ampliadas e com melhor qualidade, de modo a tornar a sua visualização mais percetível.

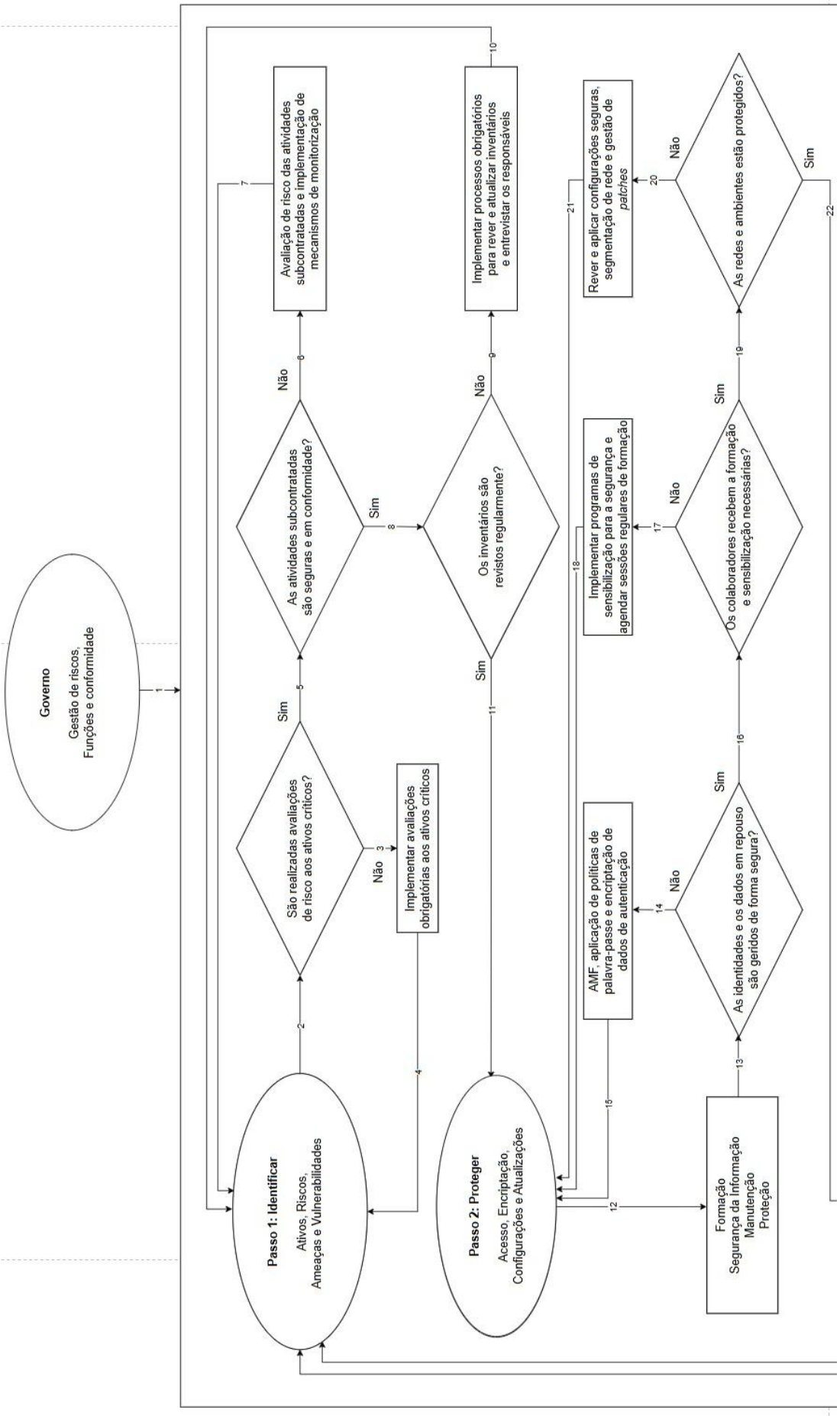


Figura 13. Modelo Parte 1

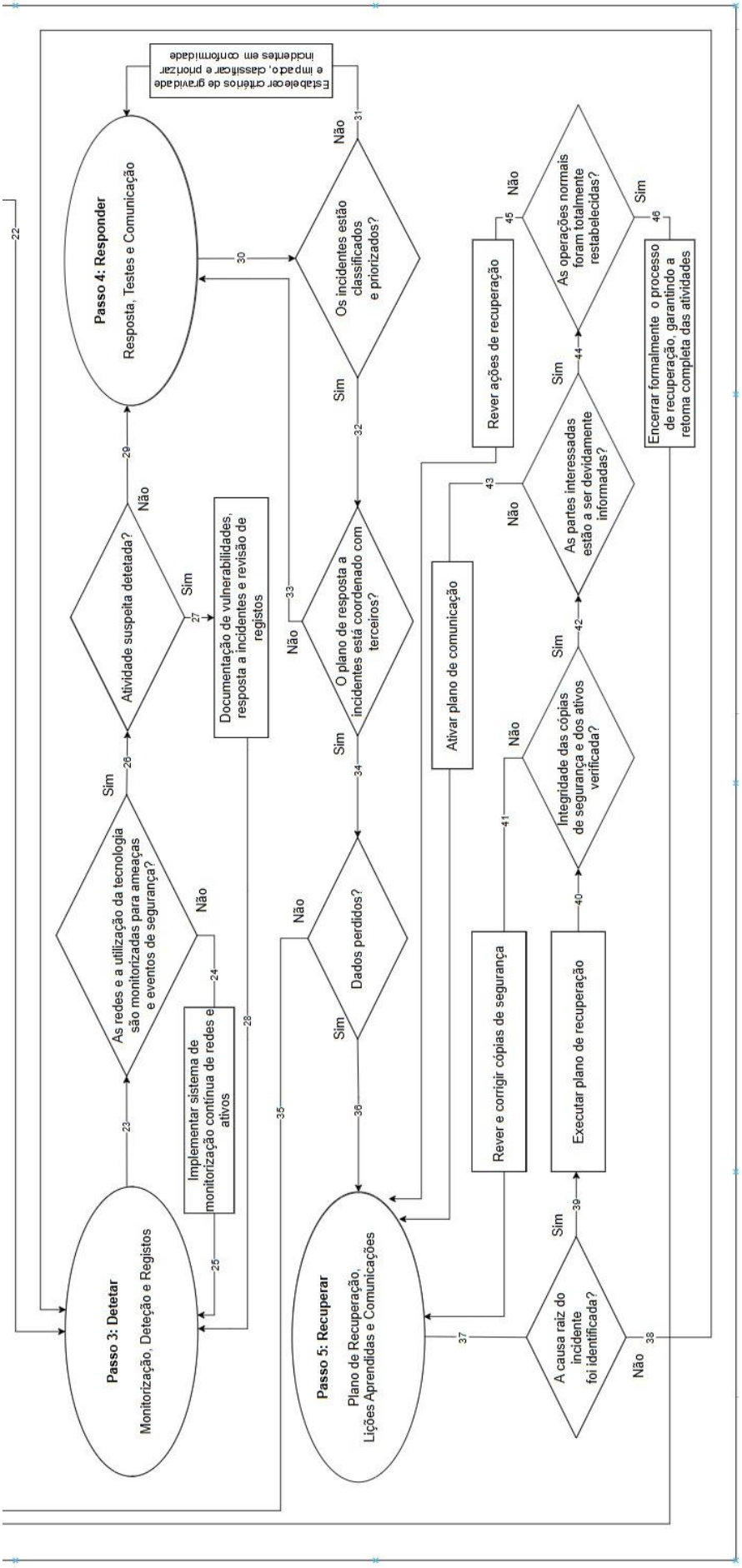


Figura 14. Modelo Parte 2