INSTITUTO
UNIVERSITÁRIO
DE LISBOA

Avaliação de Riscos de Cibersegurança no Setor Financeiro - Uma Abordagem Baseada em IA para Gestão de Fornecedores e Controlo de Acessos

João Miguel Isidro Antas

Mestrado em Informática e Gestão

Orientadores:

Doutor João Pedro Calado Barradas Branco Pavia, Professor Auxiliar
Iscte – Instituto Universitário de Lisboa

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

Outubro, 2025

TECNOLOGIAS
E ARQUITETURA

Departamento de Ciências e Tecnologias da Informação

Avaliação de Riscos de Cibersegurança no Setor Financeiro - Uma Abordagem Baseada em IA para Gestão de Fornecedores e Controlo de Acessos

João Miguel Isidro Antas

Mestrado em Informática e Gestão

Orientadores:

Doutor João Pedro Calado Barradas Branco Pavia, Professor Auxiliar
Iscte – Instituto Universitário de Lisboa

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

Outubro, 2025

Direitos de cópia ou Copyright

© Copyright: João Miguel Isidro Antas

O ISCTE – Instituto Universitário de Lisboa tem o direito, perpétuo e sem limites geográficos, de arquivar e publicitar este trabalho através de exemplares impressos reproduzidos em papel ou de forma digital, ou por qualquer outro meio conhecido ou que venha a ser inventado, de o divulgar através de repositórios científicos e de admitir a sua cópia e distribuição com objetivos educacionais ou de investigação, não comerciais, desde que seja dado crédito ao autor e editor.

Aos meus pais e tia

Agradecimentos

Gostaria de agradecer de coração a todos que ajudaram direta ou indiretamente na elaboração desta dissertação.

Primeiramente, um agradecimento especial aos meus orientadores, Professor Doutor João Pedro Calado Barradas Branco Pavia e Professor Doutor Carlos José Corredoura Serrão, pela dedicação. Agradeço pelo suporte atento, pelas recomendações valiosas e pela presença contínua ao longo deste trajeto. O vosso saber, elevada exigência académica e estímulo foram cruciais para a realização deste trabalho.

Agradeço aos meus pais pelo incondicional apoio ao longo da minha vida académica, profissional e pessoal, amor e exemplo de dedicação que sempre me transmitiram. Sem a vossa confiança, ajuda constante e encorajamento, nada deste objetivo teria sido possível.

Quero dedicar um agradecimento especial à minha tia em virtude da sua generosidade que tornou a minha trajetória muito mais fácil. A sua constante presença, apoio inestimável em todas as fases da minha vida escolar e a força com que sempre me motivou a acreditar nas minhas capacidades foram de todo essenciais no escalar de objetivos e ultrapassar de obstáculos.

Aos meus amigos, pelo companheirismo, pelas palavras de ânimo e por todos os momentos de descontração que me ajudaram a equilibrar nos períodos mais exigentes. Agradeço ainda aos meus colegas de mestrado, com quem partilhei desafios, aprendizagens e conquistas, e que se tornaram também verdadeiros amigos, por todas as partilhas, trocas de ideias e pelo apoio mútuo que se foi criando ao longo deste caminho.

A todos os professores do Mestrado em Informática e Gestão do ISCTE que contribuíram para o meu crescimento académico e profissional, bem como a todas as pessoas e entidades que, direta ou indiretamente ajudaram na concretização deste projeto, o meu muito obrigado!

Resumo

A crescente digitalização dos serviços financeiros tem exposto as instituições bancárias a riscos cibernéticos cada vez mais sofisticados, impactando diretamente a sua operação, reputação e conformidade regulatória. Paralelamente, a dependência de fornecedores externos e o aumento da complexidade na gestão de acessos exigem abordagens inovadoras para garantir a segurança e a resiliência das infraestruturas críticas nas organizações.

Esta investigação tem como objetivo propor uma solução baseada em Inteligência Artificial (IA) para a avaliação de conformidade de políticas de cibersegurança com a Diretiva NIS 2, tendo como principal foco domínios da gestão de fornecedores e controlo de acessos. Através do desenvolvimento de uma ferramenta web, suportada por Modelos de Linguagem de Grande Escala (Large Language Models ou LLMs), é possível automatizar a análise de documentos técnicos e detetar lacunas de segurança. Os testes realizados demonstram que a ferramenta permite aumentar a eficiência e a consistência das auditorias internas, mesmo sem a necessidade do utilizador possuir uma especialização avançada em cibersegurança. Este trabalho contribui para a mitigação de riscos no setor financeiro, promovendo uma abordagem proativa, automatizada e em conformidade com os regulamentos europeus atualmente emergentes.

Palavras-chave: Cibersegurança, Diretiva NIS 2, Inteligência Artificial, gestão de fornecedores, controlo de acessos, conformidade regulatória no setor financeiro

Abstract

The growing digitalisation of financial services has exposed banking institutions to increasingly sophisticated cyber risks, directly impacting their operations, reputation, and regulatory compliance. At the same time, dependence on external suppliers and increased complexity in access management require innovative approaches to guarantee the security and resilience of critical infrastructures in organisations.

This research proposes an artificial intelligence-based solution for assessing the compliance of cybersecurity policies with the NIS 2 Directive, with a focus on the areas of supplier management and access control. By developing a web prototype, supported by large-scale language models (LLMs), it is possible to automate the analysis of technical documents and detect security gaps. The tests carried out demonstrate that the tool enables the enhancement of efficiency and consistency in internal audits, even without advanced specialization in cybersecurity. This work contributes to risk mitigation in the financial sector by promoting a proactive and automated approach that complies with emerging European regulations.

Keywords: Cybersecurity, NIS 2 Directive, artificial intelligence, supplier management, access control, financial sector regulatory compliance

Índice

Agradecimentos i
Resumo iii
Abstract v
Índice de Figuras ix
Índice de Tabelas xi
Acrónimos xiii
1. Introdução 1
1.1. Contexto e Motivação 1
1.2. Questões de Investigação 4
1.3. Metodologia de Investigação 4
1.4. Estrutura do documento 7
2. Estado de Arte 9
2.1. Revisão Sistemática de Literatura 9
2.1.1. Critérios de inclusão e exclusão 11
2.2. Desafios da Cibersegurança no setor financeiro 12
2.2.1. Gestão de Riscos e Avaliação de Ameaças em Cibersegurança 13
2.3. Gestão de Risco Integrada: Processos, IA e Cultura Organizacional 16
2.4. Gestão de Risco e Fornecedores: Conformidade, Acessos e Supply Chain 19
2.4.1. Enquadramento Regulatório Aplicado à Cadeia de Fornecimento 20
2.4.2. Fluxos de Dados Transfronteiriços e Obrigações de Proteção 22
2.4.3. TPRM: Ciclo de Gestão de Riscos de Terceiros e Controlo de Acessos 22
2.4.3.1. Abordagens Emergentes: FSUA e Controlo de Acessos Discricionários 24
2.5. KPIs para Avaliação de Políticas de Cibersegurança 25
2.6. Exploração do Uso de Modelos de Governança de Cibersegurança 26
2.7. Aplicação de Inteligência Artificial e Análise Preditiva 26
2.7.1. Tendências Futuras em Cibersegurança e IA 27
2.8. Automação na Avaliação em Conformidade 28
3. Desenvolvimento do Protótipo NIS 2 Insight e Validação 31
3.1. Análise de Benchmarking 31

3.2. Análise detalhada das soluções 31
3.2.1. ALYA vs NIS 2 Insight 32
3.2.2. Comparação com outras soluções relevantes 32
3.2.3. Diferenciação e Especificidade da NIS 2 Insight 33
3.3. Estrutura da Plataforma Web 35
3.3.1. Introdução da Plataforma Web 35
3.3.2. Diagrama da Arquitetura 35
3.3.3. Requisitos Funcionais 37
3.3.4. Arquitetura Técnica e Tecnológica 37
3.3.5. Interface de Utilizador 42
3.3.6. Motor de Análise (IA via Groq API) 42
3.3.7. Visualização e Exportação de Resultados 44
3.3.8. Resultados Esperados 44
3.3.9. Código fonte 45
3.3.10. Recomendações e Tendências Futuras 45
4. Testes e Discussão de Resultados 49
4.1. Etapas do processo de avaliação 49
4.2. Testes a políticas selecionadas 53
4.2.1. Teste 1 com a Política de Gestão de Acessos 53
4.2.2. Teste 2 com a Política de Fornecedores 56
4.2.3. Teste 3 com a Política de Fornecedores 58
4.3. Avaliação da Eficácia da Ferramenta NIS 2 Insight 61
5. Conclusões 63
5.1. Limitações do Sistema 64
5.2. Trabalhos Futuros 66
Referências Bibliográficas 69
Anexos 75
Anexo A - Relatório de análise à Política de Gestão de Acessos" do Banco Económico ... 75
Anexo B - Política de Fornecedores do Banco BPI 77
Anexo C - Política de Fornecedores da Adea Information Intelligence 79

Índice de Figuras

Figura 1 - Programa de Gestão de Riscos de Terceiros, retirado de [8] 3
Figura 2 - Uma visão geral de um cenário descritivo e metodológico de seguros cibernéticos, retirado de [15] 4
Figura 3 - DSRM Process Model [16] 6
Figura 4 - Artigos distribuídos por ano 12
Figura 5 - Desafios de Privacidade e Cibersegurança no Setor Bancário e Estratégias de Mitigação, retirado de [21] 13
Figura 6 - Esquema das Classes de Ameaças Cibernéticas Prevalentes no setor bancário, retirado de [17] 15
Figura 7 - Esquema das principais ameaças cibernéticas no setor financeiro, retirado de [17] 15
Figura 8 - Conceitos Básicos e Relações de Alto Nível de Gestão de Riscos de Cibersegurança, retirado de [25] 16
Figura 9 - Processo e Fases da Gestão de Riscos de Cibersegurança, retirado de [25] 17
Figura 10 - Diferentes tipos de técnicas de engenharia social, retirado de [27] 18
Figura 11 - Principais ameaças à segurança na cloud 19
Figura 12 - Atributos que impactam o desenvolvimento das políticas de cibersegurança, retirado de [3] 21
Figura 13 - Cenário FSUA, retirado de [50] 24
Figura 14 - Processo Genérico de IA, retirado de [13] 27
Figura 15 - Análise de coocorrência das palavras-chave de tendência [23] 28
Figura 16 - Arquitetura do Sistema 36
Figura 17 - Extração de texto do PDF com pdfjs-dist 38
Figura 18 - Cálculo de conformidade e atualização do gráfico 38
Figura 19 - Helpers de layout para relatório PDF (jsPDF) 39
Figura 20 - Heurística de deteção do tipo de política 40
Figura 21 - Fallback semântico baseado em palavras-chave 41
Figura 22 - Tratamento de erros e comunicação ao utilizador 41
Figura 23 - Interface de utilizador, destacando o layout e funcionalidades principais 42
Figura 24 - Fluxo de análise e decisão do motor IA NIS 2 Insight 44
Figura 25 - Fluxo de processamento da aplicação NIS 2 Insight 52
Figura 26 - Resultados da política de controlos de acessos do Banco Económico 54

Figura 27 - Resultados gráficos e recomendações da análise da Política de Gestão de Acessos 55
Figura 28 - Resultados da análise da Política de Fornecedores do Banco BPI 56
Figura 29 - Resultados gráficos e recomendações automáticas da análise da Política de Fornecedores 57
Figura 30 - Resultados globais da análise da Política de Fornecedores da Adea Information Intelligence 59
Figura 31 - Resultados gráficos e recomendações automáticas da análise da Política de Fornecedores (risco elevado) 60

Índice de Tabelas

Tabela 1 - Critérios de inclusão e exclusão 11
Tabela 2 - Processo de Filtragem 11
Tabela 3 - Comparação entre projeto ALYA, outras soluções e o projeto NIS 2 Insight 34

Acrónimos

ABAC - Attribute-Based Access Control

AES - Advanced Encryption Standard

AI - Artificial Intelligence

AI Act - Artificial Intelligence Act (Regulamento Europeu da IA)

API - Application Programming Interface

BPMN - Business Process Modeling and Notation

BCE - Banco Central Europeu

CIA - Confidencialidade, Integridade, Disponibilidade

COBIT - Control Objectives for Information and Related Technology

DAC - Discretionary Access Control

DoS - Denial of Service

DL - Deep Learning

DLP - Data Loss Prevention

DORA - Digital Operational Resilience Act

DSRM - Design Science Research Methodology

EU - European Union (União Europeia)

FSUA - Frictionless Secure User Authentication

GDPR / RGPD - General Data Protection Regulation / Regulamento Geral sobre a Proteção de Dados

GRC - Governance, Risk and Compliance

IAM - Identity and Access Management (Gestão de Identidades e Acessos)

IEEE - Institute of Electrical and Electronics Engineers

ISO/IEC 27001 - International Organization for Standardization / International Electrotechnical Commission 27001

KPIs - Key Performance Indicators (Indicadores-Chave de Desempenho)

LLM - Large Language Model (Modelo de Linguagem de Grande Escala)

MASVS - Mobile Application Security Verification Standard

MFA - Multi-Factor Authentication (Autenticação Multifator)

ML - Machine Learning (Aprendizagem Automática)

MTTD - Mean Time to Detect (Tempo Médio de Deteção)

MTTR - Mean Time to Respond (Tempo Médio de Resposta)

NIS - Network and Information Security Directive

NIS 2 - Network and Information Security Directive 2 (Diretiva (UE) 2022/2555)

NIST - National Institute of Standards and Technology

NLP - Natural Language Processing (Processamento de Linguagem Natural)

OWASP - Open Worldwide Application Security Project

PCI DSS - Payment Card Industry Data Security Standard

RBAC - Role-Based Access Control (Controlo de Acessos Baseado em Funções)

RegTech - Regulatory Technology

SDK - Software Development Kit

SLAs - Service-Level Agreements (Acordos de Nível de Serviço)

SLR - Systematic Literature Review (Revisão Sistemática da Literatura)

SOC - System and Organization Controls

SupTech - Supervisory Technology

TLS - Transport Layer Security

TPRM - Third-Party Risk Management (Gestão de Riscos de Terceiros)

XAI - Explainable Artificial Intelligence (IA Explicável)

ZTA - Zero Trust Architecture (Arquitetura de Confiança Zero)

CAPÍTULO 1

Introdução

Este capítulo apresenta o enquadramento inicial da presente investigação, dedicada à avaliação de riscos de cibersegurança no setor financeiro, com foco na gestão de fornecedores e no controlo de acessos. Começa por explorar o contexto e as motivações que justificam a escolha do tema, seguido da formulação de questões de investigação. Finalmente, é descrita a metodologia aplicada e o plano de trabalho adotado.

1.1. Contexto e Motivação

A transformação digital e a crescente adoção de tecnologias emergentes em múltiplos setores têm acrescentado um elevado grau de complexidade à cibersegurança. A atual era digital caracteriza-se pela interconexão de sistemas, pela utilização de Inteligência Artificial e pela crescente dependência de serviços baseados na *cloud*, fatores que ampliam a superfície de ataque e intensificam os riscos. Este cenário tem conduzido a um aumento significativo de vulnerabilidades, ameaças e potenciais alvos, sendo o setor financeiro especialmente visado em virtude da sensibilidade dos dados e da criticidade das suas operações [1].

A externalização de serviços e a gestão de fornecedores assumem, neste contexto, uma importância estratégica decisiva para instituições financeiras e tecnológicas [2]. Perante a constante evolução de políticas e regulamentações em matéria de cibersegurança, as organizações do setor financeiro são forçadas a implementar normas internas rigorosas, dinâmicas e permanentemente ajustáveis, com vista a prevenir ataques ou, pelo menos, a mitigar os seus efeitos. Assim, torna-se essencial adotar critérios exigentes na seleção e monitorização de fornecedores, bem como estabelecer políticas de controlo de acessos robustas [3]. Uma escolha inadequada de prestadores pode introduzir vulnerabilidades críticas e aumentar a dependência face a terceiros [2]. Do mesmo modo, a ausência de monitorização contínua compromete a deteção de falhas de conformidade e enfraquece a resiliência organizacional perante novas ameaças [3]. Acresce que as credenciais privilegiadas permanecem um dos vetores de ataque mais explorados no setor financeiro, justificando a necessidade de mecanismos de controlo de acessos eficazes [1].

A investigação recente evidencia que a aplicação de técnicas de IA em cibersegurança pode potenciar ganhos tangíveis de eficácia e eficiência. Os autores Ehsan Aghaei, Xi Niu, Waseem Shadid e Ehab Al-Shaer propuseram o *SecureBERT*, demonstrando que modelos de

linguagem treinados especificamente com terminologia e corpora de cibersegurança conseguem interpretar de forma mais precisa relatórios técnicos, políticas de segurança e informação crítica, superando modelos generalistas em tarefas como a deteção de vulnerabilidades e a análise de ameaças [4]. Noutro domínio, o ESASCF (Expert-System Automated Security Compliance Framework) apresentou uma abordagem assente em sistemas periciais para testes de vulnerabilidade e penetração, permitindo capturar e reutilizar conhecimento de especialistas certificados. Em estudos empíricos, esta ferramenta reduziu em cerca de 50% o tempo médio de execução de avaliações iniciais e em 20% o de novos testes, aumentando simultaneamente a cobertura de ativos analisados. Tal demonstra o potencial da automação inteligente na monitorização contínua e na *due diligence* de fornecedores [5]. De igual modo, o trabalho desenvolvido por Orlando Amaral, Sallam Abualhaija, Damiano Torre, Mehrdad Sabetzadeh e Lionel C. Briand evidenciou que a IA pode ser aplicada à verificação de completude de documentos regulatórios, assegurando que todos os elementos obrigatórios de diretivas, como o RGPD, estão presentes nas políticas organizacionais. Esta perspetiva é particularmente relevante para o contexto da NIS 2, onde a validação automatizada da cobertura documental poderá reduzir custos e reforçar a confiança no cumprimento normativo [6].

Paralelamente, têm sido estabelecidos referenciais internacionais que orientam a gestão de riscos cibernéticos. Entre os mais relevantes encontram-se o RGPD, a norma ISO/IEC 27001 e as diretrizes do National Institute of Standards and Technology (NIST) [4], [5], [7]. Estes referenciais desempenham um papel essencial na proteção de ativos sensíveis e na preservação da confiança de clientes e parceiros. Todavia, para além da adoção de normas, as organizações necessitam de instrumentos eficazes que possibilitem a monitorização contínua, a realização de auditorias e o reajuste dinâmico das suas políticas de segurança, assegurando simultaneamente conformidade regulamentar e mitigação de riscos operacionais e financeiros [9], [10].

Destaca-se ainda o papel da Inteligência Artificial, em particular das técnicas de aprendizagem automática (do inglês *machine learning)*, na monitorização e previsão de comportamentos de risco em fornecedores externos, promovendo a resiliência organizacional [11]. A crescente complexidade dos ecossistemas digitais e a necessidade de um acompanhamento permanente tornam inviável uma abordagem exclusivamente manual à aplicação de políticas de cibersegurança. Assim, soluções automatizadas e inteligentes constituem numa mais-valia para a análise eficiente de políticas de segurança, em especial no âmbito da gestão de fornecedores externos e do controlo de acessos [12], [13].

Ao identificar padrões e antecipar vulnerabilidades, uma ferramenta baseada em IA não só facilitaria a deteção de lacunas face às normas em vigor, como também forneceria

recomendações concretas para a mitigação de riscos. Adicionalmente, permitiria uma adaptação dinâmica às mudanças regulatórias e às ameaças emergentes, reforçando a postura de segurança das instituições financeiras. A Figura 1 apresenta o ciclo de gestão de riscos de terceiros (*Third-Party Risk Management*), que integra as principais etapas de um processo contínuo e estruturado de mitigação de riscos associados a fornecedores externos. O ciclo inicia-se com a identificação de fornecedores, segue-se a avaliação dos riscos inerentes à relação contratual e, posteriormente, a sua priorização consoante o grau de criticidade. A implementação de medidas de mitigação adequadas é acompanhada de monitorização contínua e, numa fase final, de reavaliação periódica, assegurando uma abordagem dinâmica e adaptativa [8].

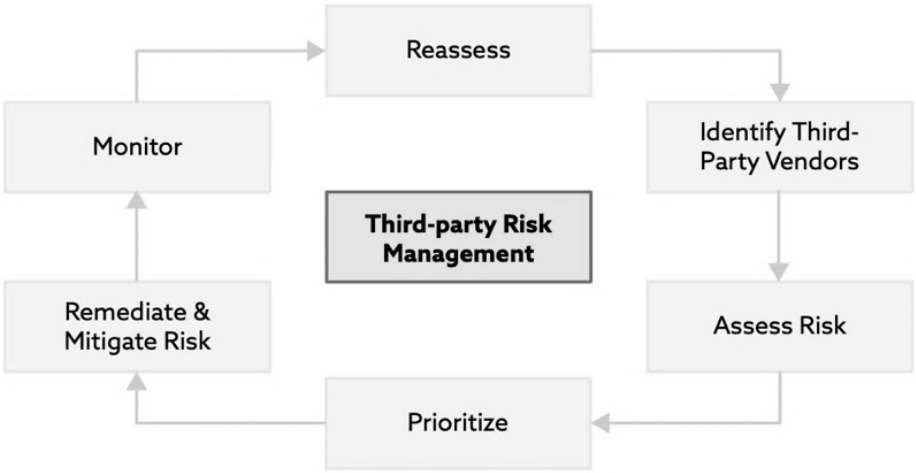

Figura 1 - Programa de Gestão de Riscos de Terceiros, retirado de [8]

A avaliação de riscos cibernéticos assume, deste modo, um papel central na estratégia de segurança do setor financeiro, não apenas para a proteção de ativos e a conformidade regulatória, mas também para a gestão financeira do risco. A quantificação dos riscos cibernéticos é determinante para a definição de estratégias de mitigação e para a decisão de recorrer a mecanismos como os seguros cibernéticos, que permitem transferir parte da exposição para terceiros. A Figura 2 ilustra os métodos e fatores utilizados na precificação destes seguros, demonstrando de que forma as seguradoras avaliam a frequência e a severidade dos riscos com base em variáveis quantitativas e qualitativas. Entre os critérios mais relevantes incluem-se o perfil da organização, o histórico de incidentes, a classificação setorial e os fatores de segurança adotados [14], [15]. Esta perspetiva evidencia a importância de uma gestão eficaz da cibersegurança, assente em ferramentas de monitorização contínua e mitigação proativa, que contribuem para reduzir a exposição a ameaças e otimizar os custos associados à proteção. No setor financeiro, esta necessidade revela-se ainda mais crítica, tendo em conta o elevado grau

de regulamentação e o impacto que um incidente cibernético pode ter na confiança do mercado e na estabilidade operacional [15].

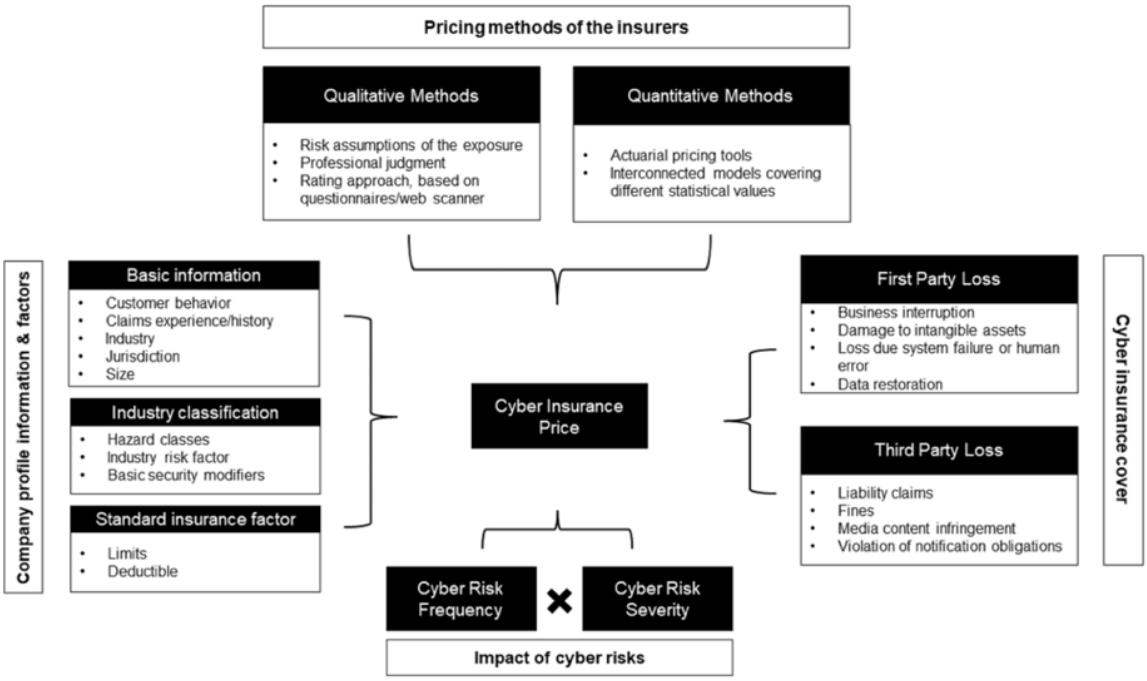

Figura 2 - Uma visão geral de um cenário descritivo e metodológico de seguros cibernéticos, retirado de [15]

1.2. Questões de Investigação

O contexto e as motivações acima referidos foram condensados na seguinte questão de investigação: Como é que a aplicação de Modelos de Linguagem de Grande Escala (LLMs) pode melhorar a eficiência e consistência das auditorias internas de cibersegurança, com foco na gestão de fornecedores externos e no controlo de acessos em instituições do setor financeiro?

1.3. Metodologia de Investigação

Dado o crescente risco de ameaças cibernéticas no setor financeiro, a avaliação de risco de cibersegurança tornou-se um elemento essencial para a continuidade e resiliência dos negócios. A solução foi desenhada para ser tecnologicamente flexível, suportando tanto a integração de modelos públicos acessíveis via API, como também a implementação de modelos privados *on-premises*. Esta flexibilidade foi testada durante o desenvolvimento, assegurando a escalabilidade e a resiliência necessárias para atender às exigências futuras.

No desenvolvimento deste trabalho, adotou-se a metodologia Design Science Research Methodology (DSRM), amplamente reconhecida pela sua capacidade de conceber soluções

práticas para problemas do mundo real, ao mesmo tempo em que assegura rigor científico [16]. A DSRM é particularmente valorizada no campo da pesquisa aplicada, pois permite a criação de artefactos inovadores, como ferramentas e sistemas, que resolvem desafios específicos de forma eficaz, sem abrir mão da base teórica e da comprovação empírica dos resultados. A sua aplicabilidade em ambientes dinâmicos e complexos, como o setor financeiro, torna-a uma escolha ideal para a construção de soluções tecnológicas que atendem a necessidades concretas e em constante evolução.

A aplicação da DSRM neste contexto permitiu a construção e avaliação de um protótipo inovador, que automatiza a análise de documentos técnicos com foco na avaliação da conformidade com a Diretiva Network and Information Security Directive 2 (NIS 2). A metodologia guiou a investigação por meio de uma abordagem prática e iterativa, onde, ao longo de várias fases, foi possível refinar e validar o artefacto desenvolvido. Esse processo resultou na criação de uma ferramenta que integra técnicas avançadas de Inteligência Artificial (IA), especificamente modelos de LLMs, com o objetivo de melhorar a eficiência e consistência nos processos de auditoria e avaliação de riscos cibernéticos [16].

Cada uma das fases da DSRM foi essencial para o sucesso da pesquisa. A primeira fase da DSRM envolveu a identificação do problema central da pesquisa: a crescente complexidade dos riscos cibernéticos no setor financeiro, especialmente na gestão de fornecedores externos e no controlo de acessos. Para isso, foi realizada uma análise aprofundada de riscos, destacando a necessidade de uma solução automatizada para identificar lacunas nas políticas do âmbito em causa. O objetivo era resolver a dificuldade das instituições financeiras em manter uma vigilância constante e produtiva sem sobrecarregar os recursos humanos, atendendo simultaneamente às exigências da NIS 2.

Com o problema claramente identificado, a fase de desenvolvimento concentrou-se na criação de uma solução tecnológica inovadora: uma ferramenta web baseada em IA e LLMs. A ferramenta foi projetada para automatizar a análise de documentos de conformidade, como políticas de segurança e contratos de fornecedores, com foco na Diretiva NIS 2. A flexibilidade da arquitetura da solução foi uma prioridade, permitindo a integração de modelos públicos e privados, o que a torna escalável e resiliente para as necessidades futuras do setor financeiro.

Após o desenvolvimento, a fase seguinte caracterizou-se pela realização de testes práticos para avaliar a eficácia da ferramenta na deteção de lacunas em políticas de cibersegurança. A ferramenta permitiu identificar inconsistências e pontos críticos de forma automatizada, proporcionando uma análise estruturada e replicável dos documentos. A fase de

demonstração foi essencial para validar a viabilidade da solução proposta, com resultados positivos indicando uma melhoria significativa na eficiência das auditorias internas.

Na fase de avaliação, a eficácia da ferramenta foi comprovada através da redução do tempo necessário na avaliação e identificação de lacunas nas políticas de cibersegurança, verificadas nos testes realizados. A avaliação mostrou que a solução automatizada não só aumentou a eficiência, mas também contribuiu para uma auditoria mais precisa e consistente, atendendo às expectativas de conformidade regulatória da NIS 2.

A última fase da DSRM, a comunicação, envolveu a documentação dos resultados e a elaboração de relatórios de avaliação detalhados. A comunicação foi fundamental para compartilhar os benefícios e os resultados da aplicação da solução, demonstrando como a automação inteligente pode melhorar a gestão de riscos cibernéticos no setor financeiro. A documentação também incluiu comparações entre os métodos manuais e a solução automatizada, evidenciando as melhorias trazidas pela utilização de IA e LLMs.

A Figura 3, ilustra o modelo de processo da DSRM, que descreve as principais fases do processo de pesquisa e desenvolvimento de artefactos. Essa representação visual ajuda a compreender de forma clara e sequencial como as atividades da DSRM se inter-relacionam para gerar soluções práticas e inovadoras [16].

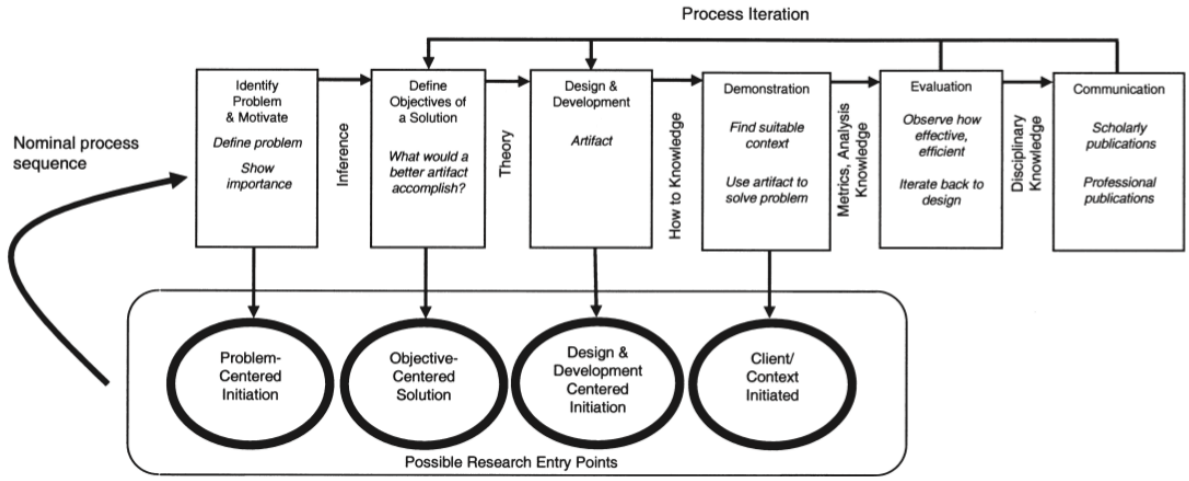

Figura 3 - DSRM Process Model [16]

A aplicação da metodologia DSRM foi crucial para a construção da ferramenta desenvolvida, garantindo que ela atendesse aos desafios práticos do setor financeiro e às exigências regulatórias da Diretiva NIS 2. Através das suas distintas fases mencionadas anteriormente, a DSRM orientou cada etapa do projeto, desde a identificação do problema até a validação do artefacto final, promovendo uma solução eficaz e alinhada com as necessidades do setor.

1.4. Estrutura do documento

O presente trabalho está organizado em cinco capítulos principais, seguidos de anexos complementares, de forma a garantir uma abordagem clara e objetiva ao tema investigado.

No capítulo 1, apresenta-se a introdução à pesquisa, contextualizando a problemática e a motivação que levou à escolha do tema. São também delineadas questões de investigação e a metodologia utilizada ao longo do estudo. Este capítulo serve como a base teórica e metodológica para a investigação subsequente.

O capítulo 2 dedica-se à revisão do Estado da Arte, onde se abordam os principais conceitos e desafios da cibersegurança no setor financeiro, com especial foco na gestão de fornecedores e no controlo de acessos. Também são discutidas as abordagens regulatórias aplicáveis, a aplicação de Inteligência Artificial em processos de auditoria e *compliance*, e as principais lacunas identificadas na literatura existente.

O capítulo 3 foca-se no desenvolvimento e validação do protótipo da plataforma NIS 2 Insight. Este capítulo inicia-se com uma análise de *benchmarking*, comparando a solução proposta com outras iniciativas relevantes. Segue-se uma descrição detalhada da arquitetura da plataforma, seus requisitos funcionais, o motor de análise baseado em IA e a interface de utilizador, com uma análise das expectativas e resultados esperados.

O capítulo 4 é dedicado aos testes realizados na plataforma, onde se explica o processo de avaliação, a análise dos critérios de conformidade e as métricas utilizadas. Também são apresentados os resultados obtidos a partir de testes a políticas reais, com destaque para a discussão da consistência entre as análises automatizadas e as realizadas manualmente.

No capítulo 5 são apresentadas as conclusões da investigação, incluindo um resumo dos principais resultados obtidos, as limitações identificadas ao longo do estudo e propostas para trabalhos futuros, que poderão explorar novas abordagens tecnológicas, bem como alargar a aplicação do protótipo desenvolvido a outros contextos regulatórios e de segurança.

No final desta dissertação encontram-se um conjunto de anexos que incluem documentação adicional relevante, como relatórios de análise e exemplos de políticas analisadas, que apoiam a replicabilidade e transparência dos resultados apresentados.

CAPÍTULO 2

Estado de Arte

Este capítulo tem como objetivo posicionar a proposta desta dissertação dentro do panorama atual da cibersegurança no setor financeiro, especialmente no que diz respeito à gestão de riscos associados a fornecedores e para os processos de controlo de acessos. A análise foca-se na aplicação de Inteligência Artificial, com ênfase na automação da análise de conformidade de políticas de cibersegurança, especialmente em relação aos requisitos regulatórios da Diretiva NIS 2.

A solução proposta visa resolver lacunas identificadas na literatura, como a complexidade e a ineficiência dos processos de auditoria e monitorização, que são fragmentados ou não totalmente automatizados. Este trabalho contribui para a transformação da forma como as organizações financeiras monitorizam e avaliam as políticas de segurança, utilizando Modelos de Linguagem de Grande Escala, proporcionando uma alternativa mais eficiente, consistente e em conformidade com as regulamentações vigentes.

2.1. Revisão Sistemática de Literatura

A revisão sistemática da literatura (SLR) teve como objetivo analisar a aplicação da IA na cibersegurança financeira, com um foco particular na gestão de fornecedores e no controlo de acessos, identificar as soluções existentes, avaliar as suas limitações e, principalmente, destacar as lacunas que justificam a necessidade de uma ferramenta automatizada, como a proposta nesta dissertação.

A análise revelou que, embora existam inovações em cibersegurança, as soluções atuais ainda não conseguem automatizar integralmente o processo de auditoria de conformidade, especialmente no que diz respeito aos requisitos regulatórios complexos, como os da Diretiva NIS 2. A falta de uma abordagem unificada e automatizada para esses processos continua a ser uma lacuna significativa.

Conforme indicado em estudos por Onimisi Dawodu (2024) é destacado que a vulnerabilidade dos fornecedores externos e as falhas nos processos de controlo de acessos são riscos críticos no setor bancário. No entanto, as soluções existentes para mitigar esses riscos continuam fragmentadas e não têm uma integração eficaz. Como resultado, o setor financeiro ainda carece de uma solução eficiente que assegure a conformidade contínua com as exigências de cibersegurança, como as estipuladas pela NIS 2 [17], [18], [19].

Por outro lado, a aplicação de IA oferece grande potencial para transformar os processos de auditoria de conformidade. Estudos, como o de Aghaei mostram como modelos especializados, como o *SecureBERT*, têm sido utilizados para melhorar a análise de conformidade, embora com um foco restrito a tipos específicos de documentos. Essas abordagens, no entanto, não integram completamente os processos de verificação regulatória no setor financeiro, limitando sua aplicabilidade em contextos mais amplos, como o exigido pela NIS 2 [4].

Neste sentido, a presente dissertação propõe uma ferramenta automatizada baseada em IA que permita auditar políticas de cibersegurança de forma eficaz e garantir a conformidade contínua com a NIS 2. A integração de LLMs surge como uma solução promissora para a análise de textos complexos, característicos das políticas de segurança, sendo este o alicerce do desenvolvimento do artefacto proposto [17], [18], [19].

Para assegurar uma revisão abrangente da literatura, a pesquisa foi conduzida nas principais bases de dados científicas, com destaque para a *Scopus* e a *Web of Science*, consideradas as fontes mais relevantes na área, complementadas pelo *IEEE Xplore*.

O processo de pesquisa iniciou-se com a utilização de palavras-chave selecionadas em cada repositório, visando artigos científicos, artigos de revistas, publicações em inglês e jornais. Foram aplicados filtros subsequentes, iniciando com uma pesquisa completa de palavras-chave no texto completo, seguida de uma pesquisa de palavras-chave nos resumos.

O terceiro filtro impôs uma restrição temporal, considerando apenas publicações entre 2019 e 2025. Esta decisão justifica-se pela rápida evolução da tecnologia na última década, em particular no domínio da Inteligência Artificial aplicada à cibersegurança, o que torna os estudos anteriores a 2018 pouco relevantes para o enquadramento atual. Além disso, trata-se de um tema emergente, cuja produção científica mais significativa e aplicável ao contexto desta dissertação surge sobretudo nos anos mais recentes.

Foram efetuadas verificações manuais para eliminar duplicados e garantir a exclusão de artigos repetidos nos quatro repositórios. Para ampliar a abrangência da seleção e garantir a inclusão de estudos relevantes e de qualidade, recorreu-se ao método de bola de neve (*snowballing*). Assim, através desta técnica, foi possível expandir a base de estudos, incluindo artigos que estivessem dentro do tema desejado, mas que não haviam sido encontrados inicialmente nas bases de dados pesquisadas. Com a aplicação do *snowballing*, também passaram a ser considerados artigos de outras bases de dados, como ArXiv e Springer, além das fontes já mencionadas.

Por fim, as referências resultantes deste processo foram organizadas e geridas na ferramenta *Mendeley*, que possibilitou a agregação de todos os artigos selecionados e a sua filtragem por ano, autor e título.

2.1.1. Critérios de inclusão e exclusão

Para garantir a exatidão e a precisão da SLR, foram meticulosamente concebidos critérios específicos de inclusão e exclusão. Estes critérios funcionam como referências cruciais, orientando o processo de seleção para garantir a relevância e a qualidade dos estudos escolhidos. Aplicados com precisão durante a pesquisa e a seleção da literatura, estes critérios sublinham a natureza sistemática e orientada da nossa análise exaustiva da literatura. A Tabela 1 que se segue fornece um retrato claro e transparente do processo de filtragem, detalhando o número de estudos selecionados em cada etapa crítica.

Tabela 1 - Critérios de inclusão e exclusão

INCLUSION	EXCLUSION
Full Text	Not in Full Text
Abstract	Not in abstract
From 2019 - Present Day	Before 2018 inclusive
Articles in English	Articles Not in English
Not Duplicate	Duplicate

Os resultados do processo de filtração podem ser observados na Tabela 2, onde são contabilizadas as diferentes etapas.

Palavras-chave: ("Cybersecurity" OR "Cyber Risk" OR "Information Security") AND ("Financial Sector" OR "Banking") AND ("Artificial Intelligence" OR "Machine Learning" OR "AI" OR "ML") AND ("Supplier Management" OR "Third-Party") AND ("Access Control" OR "Identity Management")

Tabela 2 - Processo de Filtragem

Filtragem	Full Text	2019 - 2025	Duplicates and Manual Filtering	Snowballing
IEEE	6	9	47	11
Scopus	129	81		
TOTAL				58

A escolha do período temporal de 2019 a 2025 para a SLR foi motivada pela rápida evolução tecnológica, pelas mudanças nas regulamentações e pela relevância das publicações mais recentes no campo da cibersegurança financeira. Estudos anteriores a esse período não refletiriam os avanços mais recentes da tecnologia, essenciais para a solução proposta.

Além disso, a Diretiva NIS 2, publicada em 2022 e aprovada a transposição para a lei portuguesa em setembro de 2025, introduziu novas exigências regulatórias, especialmente em relação à gestão de fornecedores e controlo de acessos, que não estavam presentes em publicações anteriores. Devido à sobreposição substancial de publicações em diversas bases de dados, alguns artigos foram identificados como duplicados e, consequentemente, eliminados.

Posteriormente, aplicou-se o método de *snowballing*, conforme mencionado anteriormente, com o objetivo de identificar publicações adicionais relevantes a partir das referências dos artigos inicialmente selecionados. Este processo permitiu incorporar novos estudos, incluindo alguns publicados fora do intervalo temporal inicialmente definido, quando estes apresentavam contributos teóricos ou metodológicos significativos para os objetivos da revisão.

Após seguir o protocolo predefinido e aplicar critérios de seleção rigorosos, obteve-se um conjunto refinado de 58 artigos únicos, que constitui a base desta revisão da literatura.

Para uma compreensão mais clara da quantidade de artigos incorporados na literatura, a Figura 4 ilustra a distribuição dos artigos selecionados por ano.

Figura 4 - Artigos distribuídos por ano

2.2. Desafios da Cibersegurança no setor financeiro

A cibersegurança no setor financeiro enfrenta desafios complexos devido à natureza sensível dos dados e à crescente digitalização das operações. A gestão de riscos cibernéticos é essencial

para mitigar as ameaças que o setor enfrenta, como ataques direcionados a dados financeiros, dados de clientes e sistemas críticos. Além disso, a crescente interdependência entre as instituições financeiras e os fornecedores externos amplia a superfície de ataque, tornando a gestão de fornecedores e o controlo de acessos áreas críticas que exigem soluções robustas de cibersegurança [17], [18], [19]. A Inteligência Artificial tem-se destacado como uma solução emergente para mitigar esses riscos, proporcionando uma análise preditiva e automatizada de ameaças [20]. A Figura 5 destaca a interação entre privacidade de dados e cibersegurança no setor bancário, evidenciando a necessidade de abordagens integradas para enfrentar essas ameaças [21].

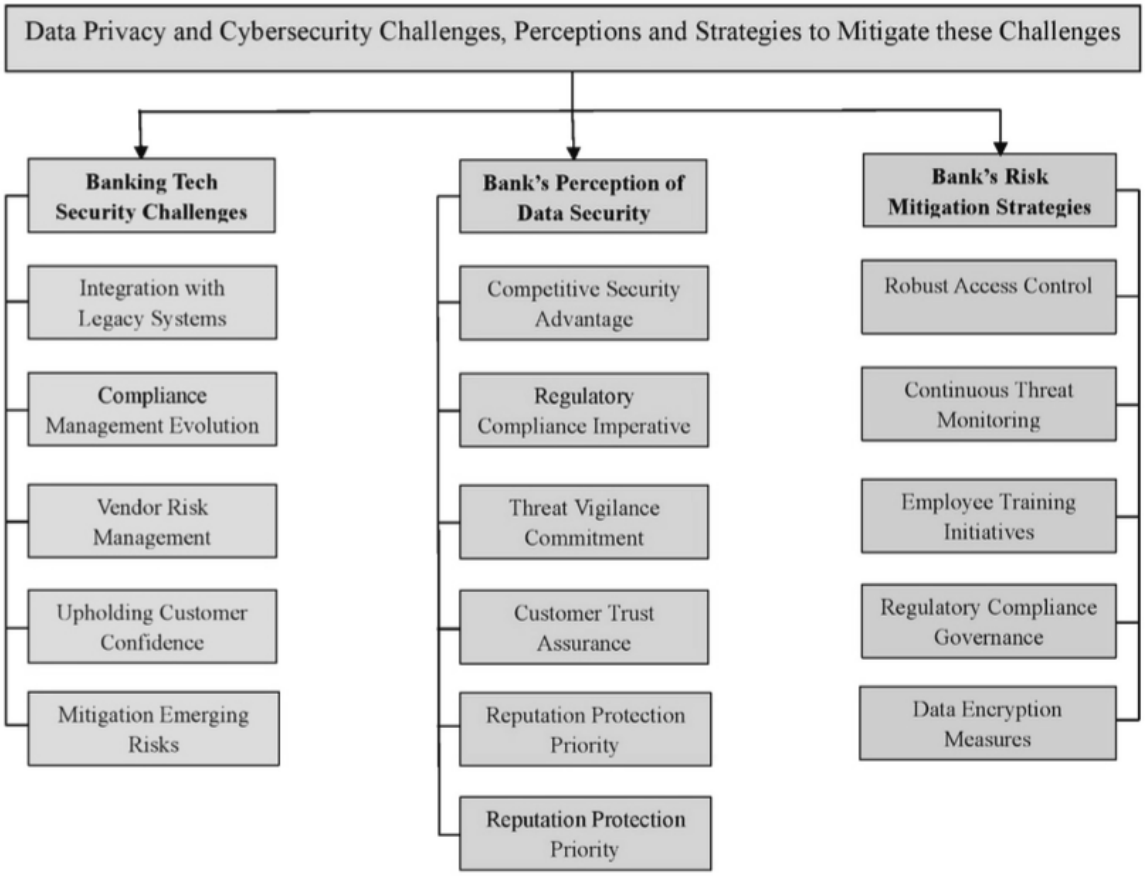

Figura 5 - Desafios de Privacidade e Cibersegurança no Setor Bancário e Estratégias de Mitigação, retirado de [21]

2.2.1. Gestão de Riscos e Avaliação de Ameaças em Cibersegurança

A gestão de riscos cibernéticos no setor financeiro é essencial para garantir a proteção de dados sensíveis e a continuidade operacional. Os riscos cibernéticos, que podem comprometer a segurança de ativos como sistemas financeiros, dados de clientes e reputação das instituições,

exigem uma abordagem rigorosa e estruturada [20]. Tais riscos são medidos pela probabilidade de ocorrência de um evento adverso e pelo impacto potencial, que pode resultar em danos consideráveis caso vulnerabilidades sejam exploradas, como evidenciado por eventos como o ataque à Target, onde falhas na segurança de fornecedores comprometeram dados de milhões de clientes [22].

A IA tem-se mostrado um aliado valioso na gestão de riscos, oferecendo a capacidade de analisar grandes volumes de dados em tempo real, detetar anomalias e padrões de ataque de forma proativa, permitindo respostas automatizadas rápidas a incidentes. Modelos de IA são capazes de identificar comportamentos e ameaças desconhecidas, melhorando a eficácia na prevenção e mitigação de riscos [23]. Dentro da gestão de riscos, existem várias metodologias que podem ser empregues para avaliar ameaças cibernéticas, que incluem avaliações quantitativas e qualitativas, modelagem de ameaças, análise de cenários e o uso de IA para análise preditiva. Essas metodologias contribuem para a deteção mais rápida e para uma postura proativa frente a riscos cibernéticos.

- As avaliações quantitativas atribuem valores numéricos aos fatores de risco, permitindo uma priorização dos riscos com base no seu impacto financeiro [1], [18]. Por outro lado, as avaliações qualitativas fazem uso de escala descritiva, como "alto", "médio" e "baixo", para medir a probabilidade e o impacto das ameaças [17]. Ambos os métodos são essenciais para priorizar esforços num contexto financeiro.
- Modelação de ameaças, destacando-se uma técnica crucial para identificar e classificar as ameaças potenciais que podem impactar os sistemas financeiros. Esta prática ajuda as instituições a compreenderem os riscos específicos e a prepararem-se adequadamente para mitigá-los. Este processo beneficia significativamente da IA, que permite automatizar a identificação de ameaças, fornecendo recomendações de forma mais rápida e com menos erros humanos [17], [24]. Este método está representado na Figura 6, que ilustra as diferentes classes de ameaças enfrentadas pelos bancos, incluindo ameaças internas e persistentes.

Figura 6 - Esquema das Classes de Ameaças Cibernéticas Prevalentes no setor bancário, retirado de [17]

Esta modelação permite às instituições financeiras implementar medidas preventivas personalizadas, adaptando-se às especificidades das suas operações e aumentando a resiliência cibernética.

- Análise de cenários: outra técnica importante envolve a criação de situações hipotéticas para avaliar como uma instituição financeira poderia reagir a diferentes tipos de incidentes cibernéticos. A IA pode ajudar na simulação de cenários complexos e na elaboração de planos de contingência, otimizando os recursos e permitindo respostas rápidas [18]. Este tipo de abordagem é crucial para prever impactos e formular planos de contingência eficazes. A Figura 7 ilustra as principais ameaças que afetam o setor financeiro, categorizando-as de forma a apoiar a tomada de decisões estratégicas e a alocação de recursos para a mitigação de riscos.

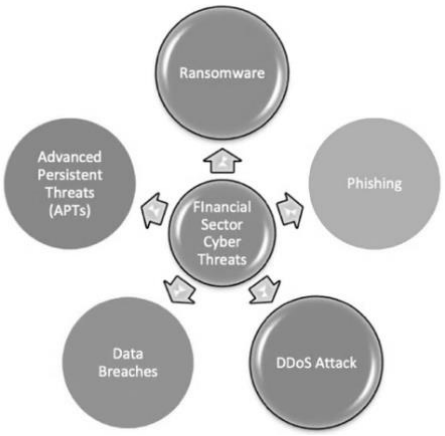

Figura 7 - Esquema das principais ameaças cibernéticas no setor financeiro, retirado de [17]

2.3. Gestão de Risco Integrada: Processos, IA e Cultura Organizacional

De acordo com o Quadro Nacional de Referência para a Cibersegurança (QNRCS) e a ISO/IEC 27005, a gestão de riscos de cibersegurança deve assentar num ciclo contínuo de identificação, análise, avaliação, tratamento e monitorização, permitindo decisões informadas e priorizadas. A Inteligência Artificial potência cada fase do ciclo, automatizando a deteção de vulnerabilidades, a análise de probabilidade/impacto e a monitorização em tempo real de eventos e controlos [25].

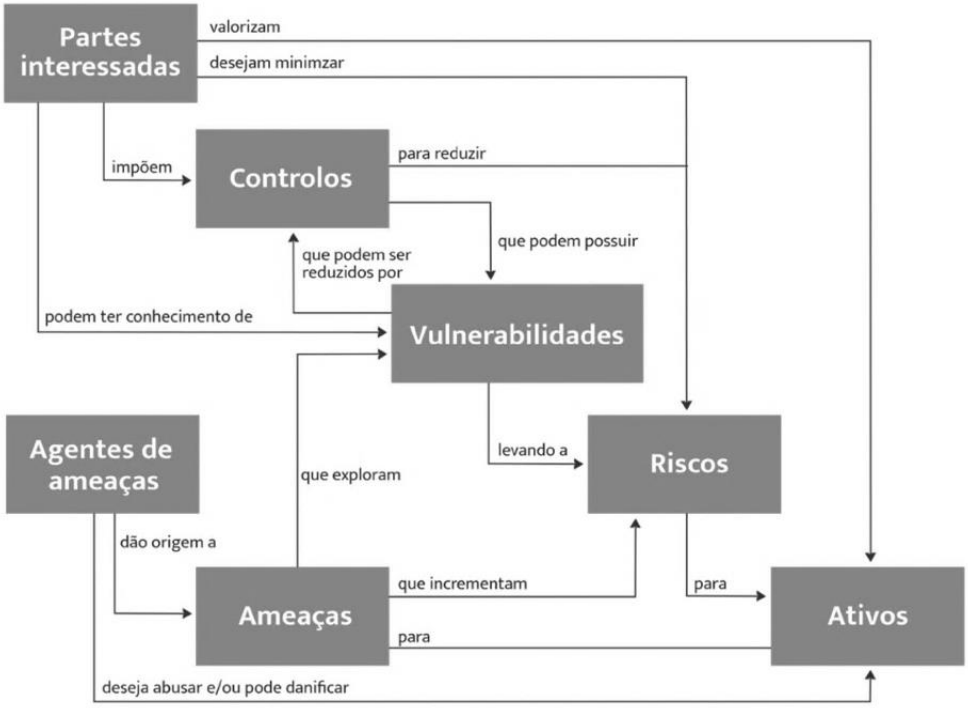

Figura 8 - Conceitos Básicos e Relações de Alto Nível de Gestão de Riscos de Cibersegurança, retirado de [25]

Conforme ilustrado pela Figura 8, o ciclo de gestão de riscos envolve fases interligadas, como a identificação de ameaças e vulnerabilidades, a análise da probabilidade de riscos e a priorização dos riscos mais críticos. O uso de IA no tratamento do risco, seja por mitigação, transferência, aceitação ou eliminação, contribui para uma abordagem proativa e em tempo real.

Além do ciclo contínuo de gestão de riscos, é fundamental garantir que a monitorização seja feita de forma automática e contínua (Figura 9). No contexto do setor financeiro, este modelo é essencial para fortalecer a resiliência cibernética e proteger os ativos organizacionais contra ameaças emergentes. A utilização de IA e aprendizado de máquina permite monitorizar constantemente os sistemas financeiros, detetando ameaças emergentes e fornecendo alertas em

tempo real, garantindo uma resposta imediata. Os testes de penetração, por exemplo, podem ser automatizados para garantir que os sistemas permaneçam seguros frente a novos tipos de ataques [26].

Figura 9 - Processo e Fases da Gestão de Riscos de Cibersegurança, retirado de [25]

Apesar do suporte tecnológico, a componente humana permanece determinante. Erros operacionais e a exploração de técnicas de engenharia social continuam a ser vetores recorrentes de intrusão; por isso, a eficácia do ciclo depende de uma cultura organizacional de consciencialização que reduza a superfície de ataque comportamental. Programas contínuos de formação e sensibilização devem abranger diferentes formas de ataque, como o *phishing*, em que os atacantes tentam obter credenciais ou informações sensíveis através de mensagens fraudulentas (emails, SMS ou chats) que imitam entidades legítimas; o *pretexting*, baseado na criação de pretextos convincentes, como alegadas validações de acessos ou auditorias urgentes, que induzem o colaborador a partilhar dados ou a executar ações de risco; e o *scareware*, que recorre a mensagens ou *pop-ups* alarmistas sobre infeções ou penalizações para pressionar o utilizador a instalar software malicioso ou a realizar pagamentos indevidos. A consciencialização destas técnicas é essencial, uma vez que exploram fragilidades humanas em

vez de vulnerabilidades técnicas, sendo por isso mais difíceis de mitigar apenas com ferramentas tecnológicas [27].

Neste sentido, programas de treino devem ser calibrados por métricas objetivas, como a taxa de cliques em simulações de *phishing*, o reporte de mensagens suspeitas e a adesão às políticas internas de segurança. Estes programas devem ainda ser integrados no ciclo de melhoria contínua da gestão de riscos, de forma a garantir que as equipas permaneçam atualizadas e capazes de responder a novas variantes de ataques. A Figura 10 apresenta as principais técnicas de engenharia social que os atacantes utilizam para manipular os comportamentos dos funcionários para obter informações confidenciais ou comprometer a segurança organizacional.

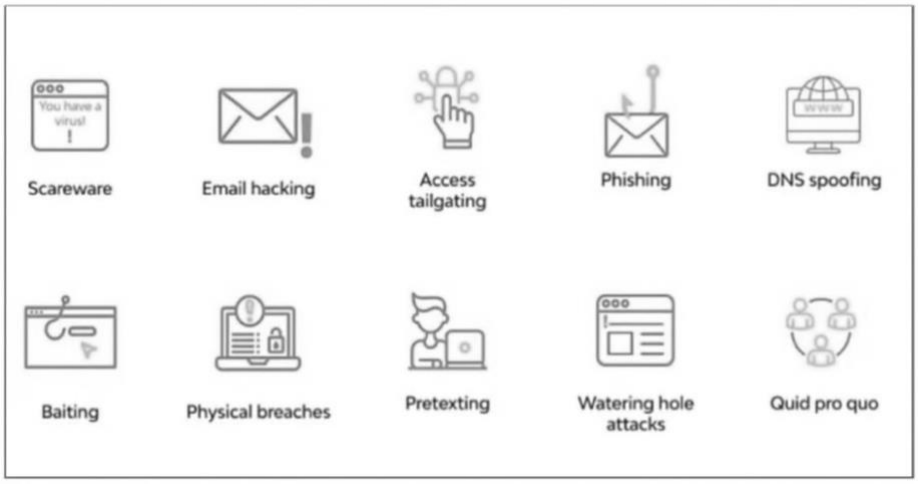

Figura 10 - Diferentes tipos de técnicas de engenharia social, retirado de [27]

As organizações enfrentam também várias ameaças à cibersegurança na *cloud*, que podem comprometer a confidencialidade, integridade e disponibilidade dos dados (CIA). As violações de dados são uma das maiores preocupações, ocorrendo devido a configurações incorretas, vulnerabilidades ou ataques direcionados. A encriptação é essencial e deve ser aplicada tanto em repouso como em trânsito, usando protocolos como TLS (Transport Layer Security) para comunicações e AES (Advanced Encryption Standard) para armazenamento, de modo a salvaguardar a informação mesmo em caso de acesso não autorizado [28], [29].

Os ataques de *malware* utilizam software malicioso para comprometer sistemas *cloud* através de *phishing* ou exploração de vulnerabilidades. A utilização de antivírus atualizado e medidas de segurança de rede são fundamentais. Já os ataques de negação de serviço (Denial of Service - DoS) visam indisponibilizar serviços, sendo fundamental implementar medidas de mitigação e monitorizar o tráfego [29], [30], [31].

Os ataques de *phishing* procuram obter credenciais através de engenharia social, sendo essencial sensibilizar utilizadores e implementar soluções *anti-phishing*. As ameaças internas, provenientes de funcionários negligentes ou mal-intencionados, podem ser mitigadas através do privilégio mínimo, monitorização e auditorias regulares. Vulnerabilidades de hardware e a proliferação de dispositivos *Internet of Things* (IoT) aumentam a superfície de ataque, tornando necessária a redundância de hardware e mecanismos de *failover* para manter a continuidade operacional [29], [32].

Estas ameaças principais à segurança na *cloud* e os respetivos vetores, de acordo com os grupos técnicos, humanos e híbridos, estão organizados na Figura 11.

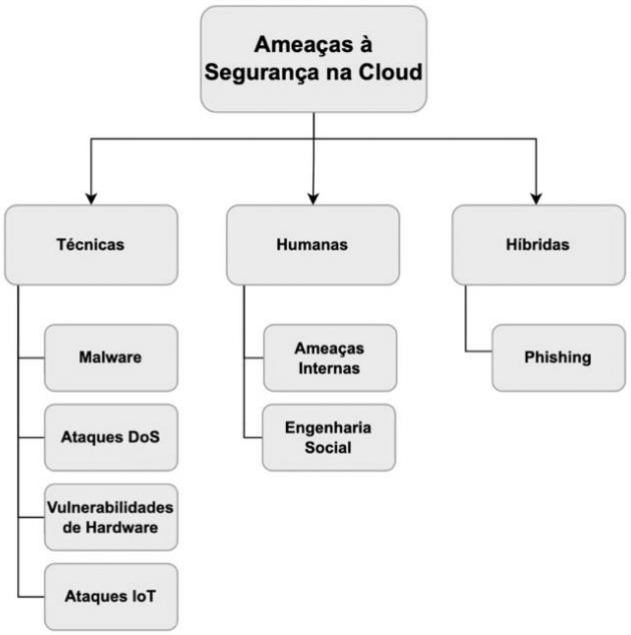

Figura 11 - Principais ameaças à segurança na *cloud*

2.4. Gestão de Risco e Fornecedores: Conformidade, Acessos e Supply Chain

Para além da proteção de sistemas internos, as instituições financeiras devem assegurar que terceiros e subfornecedores adotam práticas alinhadas com os mesmos padrões de segurança e regulamentação. Este contexto exige não apenas mecanismos de conformidade regulamentar, mas também processos estruturados de gestão de riscos de terceiros (TPRM) e de controlo de acessos, de forma a garantir a continuidade operacional, a confiança dos clientes e a resiliência do setor face a ameaças emergentes.

2.4.1. Enquadramento Regulatório Aplicado à Cadeia de Fornecimento

A conformidade regulatória é essencial para prevenir riscos legais e reforçar a cibersegurança através de auditorias que avaliam a eficácia dos controlos e a aderência aos padrões de segurança. Padrões como o RGPD, PCI DSS e ISO/IEC 27001 fornecem diretrizes para a proteção de dados e garantem que as instituições financeiras estejam preparadas para prevenir e responder a incidentes de segurança. Legislações e padrões como o RGPD, o *Payment Card Industry Data Security Standard* (PCI DSS) e a ISO/IEC 27001 fornecem diretrizes para a proteção de dados, garantindo que as instituições financeiras estejam preparadas para prevenir e responder a incidentes de segurança [21]. A conformidade também é desafiadora na gestão de fornecedores externos, pois envolve as práticas de terceiros, como a gestão de dados sensíveis e a manutenção de software atualizado [3], [7], [8].

Além disso, a análise de *Software Development Kits* (SDKs) é fundamental para identificar vulnerabilidades e garantir que a integração de fornecedores não comprometa a segurança do sistema. As auditorias de SDKs, incluindo a conformidade com normas como o OWASP MASVS (Mobile Application Security Verification Standard), são essenciais para verificar a segurança de componentes de terceiros [33]. O uso de ferramentas de análise automatizada não só garante conformidade, mas também reforça a confiança dos consumidores, protegendo dados financeiros sensíveis.

No entanto, um dos principais desafios é a complexidade na gestão de conformidade com múltiplos fornecedores e jurisdições. Tecnologias descentralizadas, como o *blockchain*, oferecem soluções inovadoras para rastrear e validar a conformidade dos fornecedores em tempo real, garantindo maior transparência e integridade dos dados em ambientes regulamentados [33], [34].

O desenvolvimento de políticas de cibersegurança em instituições financeiras é significativamente influenciado por um conjunto de atributos críticos que surgem como um padrão em vários países e setores [3]. Entre esses atributos, destacam-se a regulamentação de telecomunicações, redes, *cloud computing*, *e-commerce*, serviços bancários online, *smart grid*, direitos do consumidor, cibercrime, criptografia nacional, privacidade, roubo de identidade, assinatura digital, segurança de dados e controlo de tentativas de acesso indevidas. A Figura 12, ilustra os atributos que impactam o desenvolvimento de políticas de cibersegurança e a aplicação de *frameworks* de segurança em diferentes contextos [3].

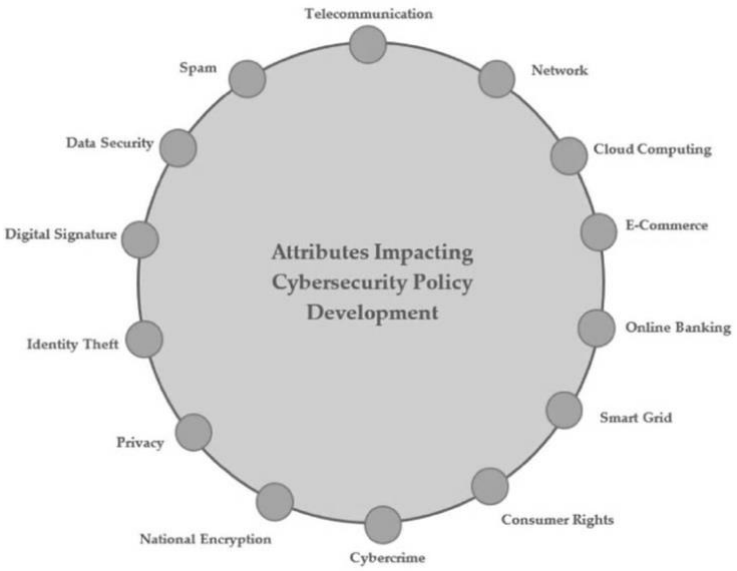

Figura 12 - Atributos que impactam o desenvolvimento das políticas de cibersegurança, retirado de [3]

Neste enquadramento mais amplo, destaca-se a Diretiva NIS 2 (Diretiva (UE) 2022/2555), que surge como resposta normativa da União Europeia para mitigar os riscos associados à digitalização e à crescente interdependência das cadeias de fornecimento no setor financeiro. A diretiva visa harmonizar os requisitos de cibersegurança entre Estados-Membros, alargando o âmbito da anterior NIS e impondo exigências mais rigorosas aos setores considerados críticos, incluindo o setor financeiro [35], [36].

A sua relevância é particularmente evidente na gestão de fornecedores e no controlo de acessos, uma vez que vulnerabilidades externas ou práticas inadequadas podem comprometer a segurança da informação e a continuidade operacional das instituições. A NIS 2 obriga à implementação de medidas de segurança robustas e de procedimentos de monitorização contínua, assegurando que todos os processos relacionados com terceiros respeitam padrões elevados de proteção [36].

Entre as obrigações do Artigo 21.º, destacam-se: a avaliação contínua dos riscos provenientes de fornecedores (*alínea d*), a gestão criteriosa de identidades e privilégios de acesso, incluindo políticas de controlo de acessos (*alínea i*), e a utilização de criptografia para proteção dos dados em trânsito e em repouso (*alínea h*). Estas exigências são complementadas por medidas contínuas de monitorização e auditorias periódicas para deteção de incidentes [36].

A seleção de fornecedores assume igualmente um papel central, sendo reforçada pela exigência de certificações de segurança (como a ISO/IEC 27001), pela definição de SLAs com cláusulas de segurança cibernética e por análises de risco contínuas, que devem considerar tanto

vulnerabilidades tecnológicas como riscos geopolíticos associados a fornecedores de fora da União Europeia [37], [38], [39].

Por fim, a NIS 2 interage de forma estreita com outras normas e regulamentos, como a ISO/IEC 27005 e o DORA (Digital Operational Resilience Act), promovendo uma abordagem holística à cibersegurança e a resiliência das organizações no setor financeiro. A sua implementação traz implicações práticas, como o reforço da avaliação de fornecedores com recurso a IA e ferramentas de monitorização em tempo real, a aplicação de políticas de controlo de acessos baseadas em risco e a obrigatoriedade de reportabilidade de incidentes (Artigos 23.º e 24.º), permitindo uma resposta mais rápida e eficiente a ataques [38], [39], [40].

2.4.2. Fluxos de Dados Transfronteiriços e Obrigações de Proteção

A conformidade também aborda os desafios dos fluxos de dados transfronteiriços, especialmente no que diz respeito à proteção de dados financeiros sensíveis num ambiente globalizado. Normas como o RGPD estabelece diretrizes rigorosas para a circulação de dados pessoais entre países e impõe requisitos como Cláusulas Contratuais-Tipo (CCTs) e Regras Vinculativas das Empresas (BCRs), garantindo um nível de proteção equivalente ao do Espaço Económico Europeu [41]. Para mitigar riscos associados a transferências internacionais de dados, é essencial adotar medidas técnicas avançadas, como encriptação ponta a ponta, anonimização de dados e Zero Trust Architecture (ZTA), além do uso de Data Loss Prevention (DLP) para monitorizar acessos e prevenir fugas de informação [30], [42].

Estas medidas tornam-se particularmente relevantes no setor financeiro, onde a sensibilidade dos dados e a confiança dos clientes são cruciais. A implementação de centros de dados regionais e auditorias regulares aos fornecedores são práticas essenciais para garantir a segurança e conformidade das transferências de dados num cenário globalizado.

2.4.3. TPRM: Ciclo de Gestão de Riscos de Terceiros e Controlo de Acessos

A gestão de riscos de terceiros (TPRM) é essencial para garantir que fornecedores e parceiros das instituições financeiras mantenham padrões de segurança alinhados com as exigências do setor [22]. A crescente dependência de serviços externos aumenta a superfície de ataque e pode introduzir vulnerabilidades críticas, comprometendo tanto a proteção de dados como a integridade operacional das instituições [19].

Este processo deve envolver a pesquisa detalhada do histórico do fornecedor, certificações de segurança como ISO 27001, SOC 1 ou SOC 2 (System and Organization

Controls), políticas de privacidade de dados e práticas de gestão de incidentes. Para além da análise inicial, deve-se verificar os antecedentes e práticas de segurança dos fornecedores antes da contratação, assegurando que estes cumpram com as exigências do setor [32]. A implementação de acordos de nível de serviço (SLAs) robustos também ajuda a definir expectativas claras sobre segurança, disponibilidade, desempenho dos serviços e responsabilidades em caso de violação [29], [32], [43].

Apesar destas medidas, as vulnerabilidades na cadeia de fornecimento tornam o setor financeiro especialmente suscetível a ameaças como *ransomware*, *malware* e *phishing*. Neste contexto, o controlo de acessos assume um papel central na proteção de dados sensíveis e sistemas críticos [44], [45]. Práticas como a autenticação multifator (MFA), o princípio do privilégio mínimo e a gestão de identidades (Identity Acess Management ou IAM) permitem reduzir a probabilidade de exploração de credenciais [28], [29], [30]. Complementarmente, a monitorização contínua da segurança e a realização de auditorias regulares são essenciais para detetar atividades suspeitas e assegurar que os fornecedores mantêm padrões adequados. A adoção de controlos de acesso mais granulares, como RBAC (baseado em funções) e ABAC (baseado em atributos), reforça a capacidade de restringir acessos indevidos e de preservar a confidencialidade [29], [30], [32].

De modo a alinhar estes mecanismos com as operações diárias, a integração de modelos BPMN (Business Process Modeling and Notation) tem-se revelado uma abordagem eficaz. O BPMN permite mapear os processos de negócio e inserir pontos de controlo de segurança diretamente nos fluxos operacionais, garantindo que a integridade e a confidencialidade da informação são mantidas ao longo das interações com fornecedores [31], [44], [46], [47]. Esta estratégia promove uma integração mais útil entre a gestão de fornecedores e a gestão de acessos, reforçando a resiliência operacional.

Contudo, mesmo com estas práticas consolidadas, a gestão de riscos de terceiros continua a enfrentar desafios significativos, nomeadamente a fragmentação dos processos de auditoria e a dificuldade em lidar com grandes volumes de informação. É neste enquadramento que a Inteligência Artificial surge como um recurso diferenciador. Técnicas baseadas em IA permitem analisar grandes conjuntos de dados relativos a fornecedores e parceiros, detetar anomalias, prever riscos emergentes e recomendar ações corretivas de forma mais célere e eficaz. Estudos recentes demonstram que algoritmos como Random Forest e XGBoost podem melhorar a deteção de vulnerabilidades e apoiar estratégias de mitigação de risco [48]. Paralelamente, a IA tem sido amplamente utilizada para automatizar auditorias de conformidade, reduzindo a intervenção manual e garantindo que as instituições financeiras

cumprem os requisitos regulatórios, minimizando o risco de incidentes legais ou operacionais [49].

A adoção de soluções suportadas em IA oferece não apenas maior eficiência, mas também transparência e segurança nas relações contratuais com fornecedores. Ao possibilitar monitorização contínua e a produção automatizada de evidências de conformidade, a IA reforça a resiliência da cadeia de fornecimento e contribui para mitigar riscos financeiros, jurídicos e operacionais em todo o ecossistema de terceiros.

2.4.3.1. Abordagens Emergentes: FSUA e Controlo de Acessos Discricionários

Além das práticas tradicionais de MFA e controlo de acessos, estratégias emergentes como a Autenticação Adaptativa (também conhecida pelo termo FSUA (Frictionless Secure User Authentication) tem-se mostrado uma estratégia avançada para reforçar a segurança em aplicações web e serviços na *cloud*. A Figura 13 ilustra o funcionamento do modelo FSUA, aplicado a serviços digitais. Segundo um estudo conduzido por Olanrewaju (2021), esta prática reduz o tempo de resposta e melhora a eficiência operacional, ao mesmo tempo em que fortalece a segurança, prevenindo acessos ilegítimos e aumentando a resistência a ataques de Denial of Service - DoS [50].

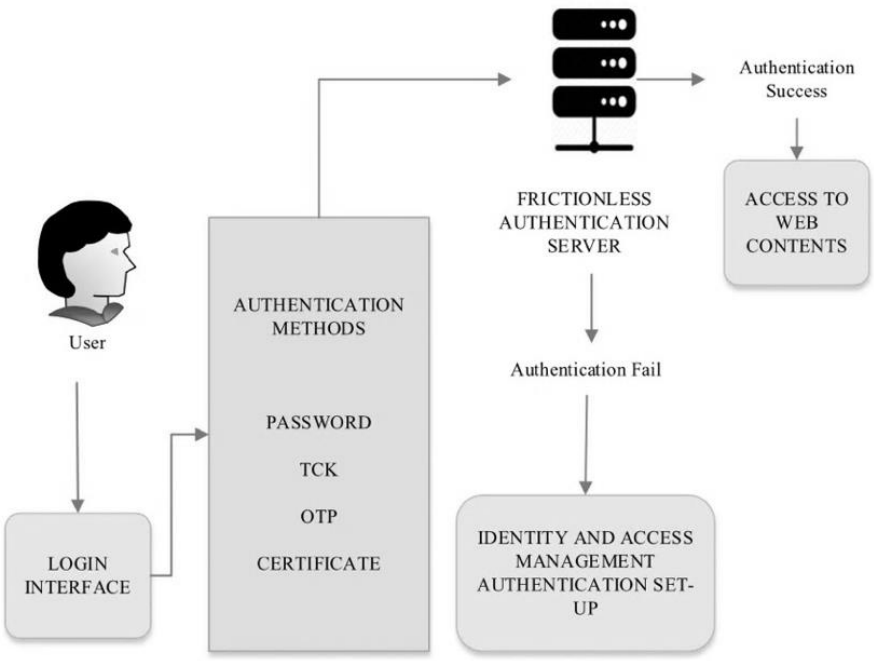

Figura 13 - Cenário FSUA, retirado de [50]

Uma outra forma de controlo de acesso é o Controlo de Acesso Discricionário (DAC). O DAC fornece acesso autorizado a itens aos utilizadores com base nas suas identidades ou grupos de utilizadores. Os utilizadores têm autonomia para delegar os seus direitos ou poder a qualquer outro utilizador, independentemente do seu papel na organização [51]. Graham e Denning criaram o DAC, um controlo de acesso que serve como base para sistemas de segurança. A gestão centralizada de acessos é um dos tipos frequentemente utilizado para controlo de acesso, sendo o DAC um exemplo. No entanto, é importante notar que no domínio da virtualização, os desafios de segurança surgem frequentemente devido ao acesso não autorizado a recursos [51].

2.5. KPIs para Avaliação de Políticas de Cibersegurança

A definição de indicadores-chave de desempenho (KPIs) é fundamental para a avaliação contínua da eficácia das políticas de cibersegurança no setor financeiro. Esses KPIs fornecem métricas que permitem às instituições financeiras monitorizar e identificar lacunas nas suas abordagens de segurança, facilitando a gestão proativa de riscos [52], [53], [54]. Entre os principais KPIs, destacam-se:

- Tempo Médio de Deteção (MTTD): Mede o tempo necessário para identificar uma ameaça cibernética.
- Tempo Médio de Resposta (MTTR): Avalia a rapidez na implementação de medidas corretivas. Taxa de Fugas de Dados: Reflete a frequência com que informações sensíveis são comprometidas.
- Taxa de Conformidade com Normas de Segurança: Mede a adesão a normativas como ISO/IEC 27001, PCI DSS e outras regulamentações relevantes.
- Tempo de Aplicação de *Patches*: Indica a rapidez com que vulnerabilidades conhecidas são corrigidas.

Estes KPIs devem ser alinhados com os objetivos estratégicos das instituições financeiras, utilizando a metodologia SMART (Specific, Measurable, Achievable, Relevant, Time-bound) para garantir uma gestão eficiente da segurança. *Dashboards* de monitorização em tempo real também desempenham um papel essencial, proporcionando visibilidade contínua e facilitando a avaliação de desempenho e relatórios [53].

A utilização de KPIs robustos não só fortalece a proteção de ativos críticos, mas também aumenta a confiança dos clientes, assegurando a conformidade regulatória e oferecendo um suporte fundamental para o planeamento estratégico contra as ameaças emergentes.

2.6. Exploração do Uso de Modelos de Governança de Cibersegurança

A governança da cibersegurança é fundamental na gestão de riscos do setor financeiro, assegurando a proteção de infraestruturas críticas e a conformidade regulatória. Modelos como COBIT, ISO 27001 e NIST oferecem referenciais importantes, mas a crescente complexidade das ameaças exige abordagens mais dinâmicas e orientadas por dados [55].

No âmbito da gestão de fornecedores e do controlo de acessos, um modelo eficiente deve contemplar a monitorização contínua com auditorias automatizadas (ISO/IEC 27005), a adoção de certificações SOC 1, SOC 2 e/ou SOC 3 para validar a resiliência de terceiros, e o recurso a IA na deteção de riscos e anomalias em tempo real. A utilização de métricas baseadas em dados permite ainda transformar informação técnica em indicadores estratégicos para apoiar a decisão [35].

A integração de IA em modelos de governança reforça a resiliência operacional, otimiza auditorias e incidentes, e contribui para uma abordagem mais proativa e estruturada à mitigação de riscos e ao cumprimento regulamentar.

2.7. Aplicação de Inteligência Artificial e Análise Preditiva

A Inteligência Artificial e a análise preditiva têm sido fundamentais para transformar a forma como as instituições financeiras lidam com a cibersegurança. A IA permite a deteção de vulnerabilidades e fraudes em tempo real, além de antecipar possíveis riscos associados a fornecedores externos. Utilizando modelos preditivos, a IA é capaz de analisar grandes volumes de dados em tempo real, identificando padrões e anomalias que poderiam passar despercebidos a análises manuais. Com isso, as instituições financeiras podem adotar uma postura proativa frente às ameaças cibernéticas e melhorar a resiliência organizacional [56].

Estudos como o de Awadallah destacam como a IA pode monitorizar e otimizar os fluxos de segurança das organizações, além de oferecer recomendações automatizadas para melhorar as políticas de cibersegurança [13]. A aplicação de LLMs, como ChatGPT, GPT, e BERT, tem sido convincente na análise de políticas de segurança e na deteção de vulnerabilidades, ajudando a identificar lacunas nas políticas de cibersegurança e formulando recomendações para sua melhoria contínua [23].

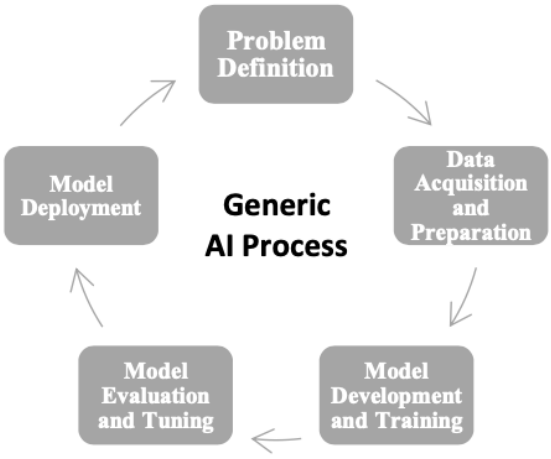

Figura 14 - Processo Genérico de IA, retirado de [13]

A IA também facilita o uso de *machine learning* (ML), que pode ser aplicado para identificar padrões comportamentais e prever fraudes e ataques em tempo real. A capacidade da IA de se adaptar constantemente a novos dados e cenários é um recurso valioso num ambiente de ameaças cibernéticas dinâmicas [57]. A Figura 14 ilustra o processo genérico de IA, destacando como a IA e ML podem ser integrados na gestão de cibersegurança para identificar ameaças e preservar a privacidade.

2.7.1. Tendências Futuras em Cibersegurança e IA

A análise das tendências emergentes em cibersegurança e IA é essencial para compreender as dinâmicas atuais do setor financeiro e identificar áreas prioritárias para investigação e desenvolvimento futuro.[10]. A Figura 15 apresenta uma rede de coocorrência de palavras-chave extraídas da literatura científica recente, destacando as principais interseções entre IA, cibersegurança, gestão de riscos e resiliência organizacional. A rede de coocorrência revela as fortes associações entre temas como segurança de redes, previsão de ataques, análise de padrões comportamentais e modelos preditivos. Estas áreas estão a tornar-se cada vez mais interligadas, com a IA a desempenhar um papel central na identificação de ameaças e na garantia de conformidade regulatória. A segmentação dos termos em clusters indica diferentes abordagens, como a aplicação de aprendizagem profunda (*deep learning)* para a deteção de anomalias, o uso de modelos preditivos para a gestão de riscos financeiros e a adaptação de técnicas de IA para reforçar a segurança digital em infraestruturas críticas [23].

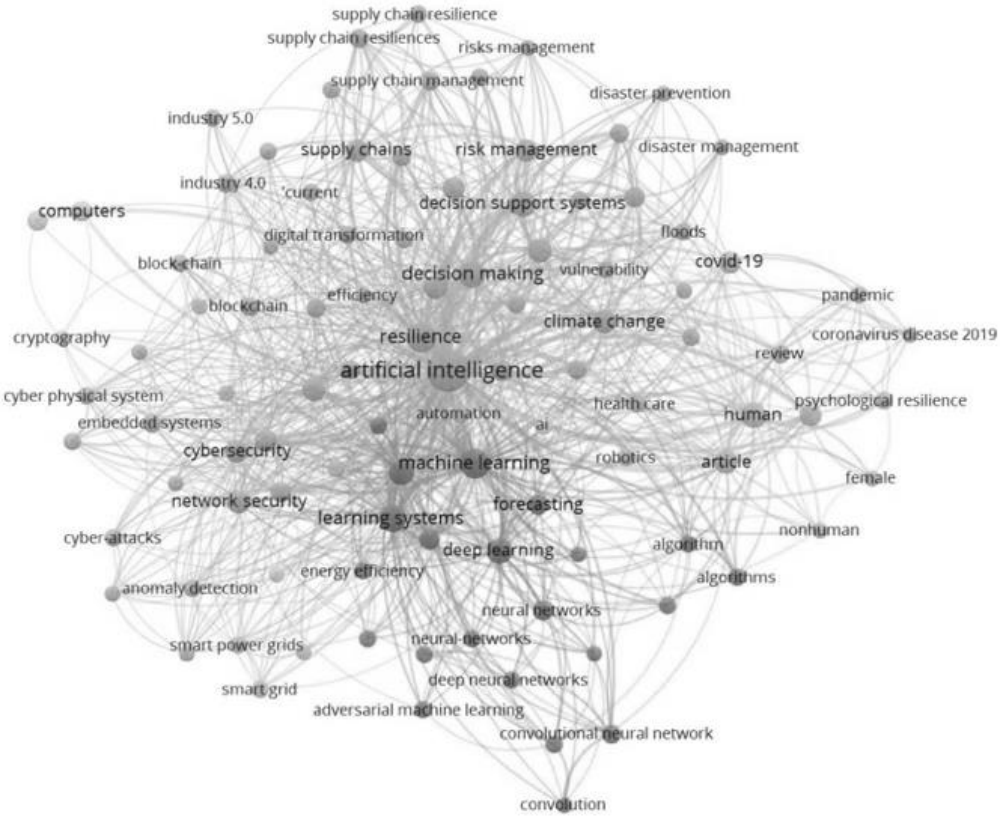

Figura 15 - Análise de coocorrência das palavras-chave de tendência [23]

2.8. Automação na Avaliação em Conformidade

A evolução tecnológica decorrente e a sua crescente interconectividade têm exacerbado as preocupações relativas à segurança e proteção de dados. Regulamentos complexos, como o GDPR e, no contexto desta investigação, a Diretiva NIS 2, exigem que as organizações estabeleçam controlos baseados no risco para proteger a confidencialidade, integridade e disponibilidade (CIA) dos seus ativos digitais. Para cumprir esses requisitos, as organizações dependem frequentemente da análise de documentos técnicos e políticas de segurança. No entanto, a verificação manual da completude e conformidade dessas políticas é morosa e propensa a erros, exigindo o desenvolvimento de métodos mais eficientes e custo-eficazes para lidar com as crescentes exigências regulatórias [5], [6], [36], [40].

A resposta a essa necessidade reside na automação de processos de auditoria e conformidade, que tradicionalmente consomem muitos recursos e são altamente repetitivos. A IA, juntamente com os LLMs, oferece uma solução eficiente, criando sistemas capazes de simular a experiência e julgamento humano, seja na auditoria de redes (Vulnerability

Assessment e Penetration Testing - VA/PT) ou na análise de documentos regulatórios e políticas de segurança [6], [58], [59].

A automação da avaliação de políticas requer, como passo preliminar, a formalização do conhecimento regulatório e técnico. Isso pode ser alcançado através da construção de artefactos de conhecimento e sistemas especialistas baseados em regras. Sistemas especialistas (ES) utilizam tecnologias de IA para simular o julgamento de um especialista humano. No domínio da segurança de rede, *frameworks* como o ESASCF demonstram como a IA, tipicamente baseada em regras, pode minimizar a intervenção humana e aumentar a eficiência na prática de *compliance* [4], [60], [61].

A análise da linguagem natural (NL) nas políticas é desafiadora devido à sua flexibilidade e aos problemas inerentes à qualidade textual, como a ambiguidade [6]. Modelos de linguagem, como BERT, desempenham um papel crucial na interpretação da entrada qualitativa e na sua transformação em representações quantitativas. A criação de um modelo de linguagem específico do domínio da cibersegurança, como o *SecureBERT*, é um exemplo de como a IA pode ser usada para melhorar a precisão da análise, capturando as conotações de texto no contexto de segurança digital [4].

CAPÍTULO 3

Desenvolvimento do Protótipo NIS 2 Insight e Validação

Após o enquadramento teórico e a revisão do estado da arte apresentados no capítulo anterior, que contextualizam a problemática e as abordagens atuais sobre cibersegurança no setor financeiro, este capítulo foca-se na aplicação prática dos conceitos discutidos. O objetivo principal desta secção é mostrar como as ideias exploradas podem ser traduzidas em soluções tangíveis, particularmente no contexto do reforço da cibersegurança no setor financeiro, que enfrenta constantes desafios relacionados com riscos de terceiros e com a proteção de infraestruturas críticas [36].

3.1. Análise de Benchmarking

A análise de benchmarking permite identificar boas práticas e soluções inovadoras de Inteligência Artificial já adotadas por instituições financeiras e académicas, servindo de referência para a proposta desenvolvida nesta dissertação. Esta avaliação crítica não se limita a descrever funcionalidades, mas procura compreender como cada solução contribui para a automação de auditorias, redução de erros humanos, melhoria da eficiência e suporte à conformidade regulatória.

Embora existam várias iniciativas emergentes no setor financeiro, destaca-se que ao longo da pesquisa efetuada o ALYA, plataforma desenvolvida internamente para o Banco de Portugal, revelou-se uma das soluções mais consolidadas identificadas no contexto bancário. Ainda assim, o foco principal desta dissertação recai sobre a NIS 2 Insight, uma plataforma concebida para automatizar a avaliação de conformidade de documentos críticos com a Diretiva NIS 2, com ênfase na gestão de riscos de fornecedores e no controlo de acessos. Esta plataforma é projetada para responder às necessidades específicas do setor financeiro, fornecendo recomendações práticas e relatórios claros que suportam decisões estratégicas de auditoria.

3.2. Análise detalhada das soluções

A análise de benchmarking contempla soluções com diferentes enfoques e níveis de maturidade, permitindo comparar abordagens comerciais, académicas e regulatórias. O objetivo é identificar lacunas existentes, destacar inovações e evidenciar como a NIS 2 Insight se diferencia por seu foco específico em conformidade normativa.

3.2.1. ALYA vs NIS 2 Insight

O ALYA, uma plataforma de *machine learning* (ML) e *deep learning* (DL) desenvolvida pelo Banco de Portugal, representa uma das soluções mais avançadas para a automação de auditorias financeiras. A plataforma permite analisar grandes volumes de documentos, automatizar tarefas repetitivas e reduzir o esforço humano, garantindo maior consistência e precisão na supervisão financeira. O impacto do ALYA é evidente na capacidade de fiscalizar contratos, minutas e responder a pedidos de informação de forma automática, acelerando processos que tradicionalmente exigiriam horas de trabalho humano.

Apesar do seu valor, ALYA apresenta limitações no contexto da Diretiva NIS 2. A sua abordagem é mais generalista, orientada à supervisão financeira e à análise de documentos regulatórios amplos, sem foco específico em conformidade normativa detalhada com NIS 2, gestão de fornecedores e controlo de acessos.

Por outro lado, a NIS 2 Insight apresenta vantagens decisivas:

- Avaliação detalhada de documentos críticos, incluindo políticas de segurança, contratos de fornecedores e normativos regulatórios, com identificação de lacunas e inconsistências.
- Emissão de recomendações normativas práticas, acionáveis diretamente em auditorias internas, permitindo aos auditores tomar decisões informadas de forma rápida e segura.
- Monitorização contínua de conformidade, garantindo que alterações nos documentos ou políticas sejam imediatamente detetadas e reportadas.
- Rapidez e eficiência, processando cada documento em menos de 10 segundos, mantendo a consistência da análise e reduzindo a probabilidade de erros humanos.

Dando um exemplo de cenário de aplicação, um banco que recebe diversas minutas de contratos de fornecedores pode utilizar a NIS 2 Insight para avaliar rapidamente cada documento, identificar cláusulas que não estejam em conformidade com a NIS 2 e propor ajustes específicos, poupando tempo e aumentando a segurança jurídica e operacional da instituição.

3.2.2. Comparação com outras soluções relevantes

Além do ALYA, várias outras soluções representam abordagens inovadoras, mas com focos diferentes:

- SecureBERT: foca-se na interpretação e análise de textos de cibersegurança, automatizando a extração de informações e entidades críticas. É especialmente útil para Cyber Threat Intelligence, mas não avalia diretamente a conformidade normativa de documentos ou contratos, limitando sua aplicabilidade para auditores e compliance officers.
- ESASCF: é uma *framework* destinada a auditorias técnicas de redes, incluindo testes de vulnerabilidade e penetração. Automatiza tarefas repetitivas e permite reutilizar o conhecimento de especialistas, aumentando a eficiência, mas não fornece recomendações aplicáveis à conformidade normativa nem avalia documentos regulatórios.
- ISOPlanner NIS 2: oferece suporte à criação de políticas e templates de conformidade, auxiliando gestores na implementação de boas práticas. Contudo, não realiza análise automática de documentos existentes e não identifica lacunas normativas específicas.
- CyberArrow / Exeon: soluções de monitorização de risco contínuo, com alertas automatizados e dashboards de conformidade, mas sem avaliação detalhada de políticas ou contratos, limitando a utilidade para auditores focados em NIS 2.
- Riskly: Foca-se na gestão de riscos, especialmente na avaliação e análise preditiva dos riscos financeiros e operacionais, através de modelos de IA. No entanto, o Riskly concentra-se mais na quantificação e monitorização de riscos gerais, sem um foco específico em conformidade normativa ou na análise de documentos críticos como contratos e políticas de fornecedores, que são a principal preocupação da NIS 2 Insight.

3.2.3. Diferenciação e Especificidade da NIS 2 Insight

A NIS 2 Insight destaca-se de todas as outras soluções analisadas, incluindo o Riskly, por integrar três elementos críticos:

- Análise documental detalhada de políticas e contratos de fornecedores, com foco direto na Diretiva NIS 2.
- Geração de recomendações normativas práticas que podem ser diretamente aplicadas nas auditorias, algo que nenhuma das outras soluções oferece com a mesma profundidade.
- Monitorização contínua de conformidade, assegurando que qualquer alteração nos documentos ou políticas seja detetada e imediatamente reportada, permitindo auditorias em tempo real.

Além disso, a rapidez da NIS 2 Insight permite a avaliação de cada documento em menos de 10 segundos, tornando-a uma solução extremamente eficiente e escalável para grandes volumes de documentos, algo que não é igualado pelas outras soluções. A Tabela 3 mostra como a NIS 2 Insight se posiciona como a melhor solução para a avaliação de conformidade normativa no setor financeiro, ao integrar uma análise detalhada de documentos, a geração de recomendações práticas e uma monitorização contínua de conformidade.

Tabela 3 - Comparação entre projeto ALYA, outras soluções e o projeto NIS 2 Insight

Área de Análise	**ALYA (Banco de Portugal)**	**Outras Soluções (SecureBERT, ESASCF, Rizly, etc.)**	**NIS 2 Insight**
Objetivo Principal	Automação de auditorias financeiras e análise de grandes volumes de documentos	SecureBERT: Processamento de CTI (Cyber Threat Intelligence); ESASCF: Auditorias técnicas e VA/PT	Avaliar a conformidade de documentos críticos com a Diretiva NIS 2, focando-se em gestão de riscos de fornecedores e controlo de acessos.
Tecnologias Utilizadas	ML/DL para análise de documentos e automação de tarefas repetitivas	BERT/RoBERTa**,** CLIPS**,** IA para análise de vulnerabilidades e monitorização contínua	LLMs**,** análise textual automatizada**,** PDF parsing e IA especializada para conformidade regulatória com NIS 2
Principais Funcionalidades	Fiscalização de contratos, resposta automática a pedidos de informação e minutas	SecureBERT: Extração de entidades e análise de vulnerabilidades; ESASCF: VA/PT, reutilização de expertise	Análise de documentos críticos, deteção de lacunas normativas, geração de relatórios estruturados e recomendações práticas acionáveis
Diferenciação/ Especificidade	Solução generalista, não especializada para NIS 2	SecureBERT: Foca-se em interpretação semântica de cibersegurança; ESASCF: Foca em auditorias técnicas	Avaliação detalhada de documentos normativos, recomendações normativas práticas, monitorização contínua de conformidade alinhada com a NIS 2
Abordagem Regulatória	Foca-se em supervisão financeira geral, sem aplicação específica para NIS 2	NIS 2, ISO 27001, mas não oferece avaliação normativa detalhada	Diretiva NIS 2, ISO/IEC 27001, DORA, RGPD: Foco exclusivo na conformidade normativa NIS 2
Público-Alvo	Auditores **e** supervisores financeiros	Analistas de cibersegurança**,** especialistas em redes**,** gestores de risco	Auditores **e** compliance officers**,** com foco em conformidade regulatória específica
Impacto	Eficiência em tarefas repetitivas**,** mas limitado em conformidade normativa	SecureBERT**:** Reduz dependência de especialistas em CTI**;** ESASCF**:** Reduz o tempo de auditorias técnicas até 50%	Rápido e eficiente (<10s por documento), relatórios estruturados**,** conformidade normativa detalhada e recomendações práticas

3.3. Estrutura da Plataforma Web

Com base nessa análise de *benchmarking*, o capítulo segue com a explicação detalhada do protótipo NIS 2 Insight, uma plataforma web projetada para automatizar a avaliação de conformidade de documentos críticos, como políticas de segurança e contratos de fornecedores, com as exigências da Diretiva NIS 2.

3.3.1. Introdução da Plataforma Web

A plataforma foi construída com base em tecnologias de ponta, em particular Modelos de Linguagem de Grande Escala, que permitem processar e analisar documentos complexos em tempo reduzido. Ao recorrer a IA, a ferramenta vai além de uma leitura literal dos documentos, sendo capaz de compreender contexto, identificar lacunas regulatórias e sugerir recomendações personalizadas [10].

O sistema identifica falhas relevantes, propõe recomendações de melhoria e apoia a tomada de decisão em contextos regulatórios e de *compliance*. Neste âmbito, destaca-se a utilização de LLMs, como os que suportam soluções do tipo ChatGPT.

Um aspeto emergente é a aplicação de *system prompts* e de mecanismos de customização baseados em regras, que orientam os modelos de linguagem para contextos organizacionais específicos. Esta prática, comum em soluções assentes em arquiteturas como GPT e LLaMA, assegura maior alinhamento com requisitos normativos e reforça a reprodutibilidade dos resultados, respondendo a uma lacuna frequentemente identificada em auditorias de conformidade.

3.3.2. Diagrama da Arquitetura

A arquitetura da NIS 2 Insight está estruturada de forma modular, dividindo-se em três blocos principais: interface de utilizador, motor de análise com Inteligência Artificial e camada de visualização e exportação. Esta estrutura modular permite que o sistema seja altamente flexível, escalável e fácil de manter, proporcionando um fluxo eficiente e claro para o processamento de documentos PDF, extração e normalização do conteúdo textual, e subsequente análise utilizando um modelo de linguagem avançado, o LLaMA 3 70B, através da API da Groq.

A escolha pela API da Groq foi uma decisão estratégica fundamentada em diversos critérios técnicos, operacionais e económicos. O modelo LLaMA 3 70B é extremamente avançado e possui uma grande capacidade de processamento, o que exige um poder

computacional significativo. Implementar este modelo localmente, com a infraestrutura necessária para o seu suporte, acarretaria custos elevados relacionados com a aquisição de hardware especializado, a gestão da infraestrutura e a manutenção contínua do sistema.

Optando pela API da Groq, a plataforma NIS 2 Insight beneficia de uma solução escalável, que permite o processamento eficiente de grandes volumes de dados sem a necessidade de investimento em infraestrutura própria. A Groq disponibiliza a capacidade computacional necessária e realiza a manutenção do modelo, o que reduz os custos operacionais da aplicação, permitindo que a equipa de desenvolvimento se concentre na melhoria da funcionalidade da plataforma e da experiência do utilizador.

Além disso, a API da Groq oferece flexibilidade e agilidade, permitindo que o sistema lide com volumes variáveis de dados sem preocupações com sobrecarga de recursos. Esta abordagem elimina a necessidade de investir em hardware caro e facilita a expansão do sistema conforme as necessidades do projeto aumentem. Em termos de segurança, a Groq segue rigorosos padrões de conformidade com as regulamentações, como o RGPD, garantindo que a aplicação NIS 2 Insight cumpra com os requisitos de privacidade e soberania de dados, sem comprometer a segurança dos documentos analisados.

Com esta arquitetura, a NIS 2 Insight torna-se uma solução eficiente e rentável, capaz de garantir desempenho e conformidade com as exigências da Diretiva NIS 2, enquanto se mantém aberta para integrações futuras com outras APIs ou modelos *self-hosted*, caso necessário.

Os fluxos e interações estão representados na Figura 16, diagrama que ilustra a arquitetura do sistema, com as interações entre a interface do utilizador, o motor de análise baseado na API Groq, e a camada de visualização/exportação.

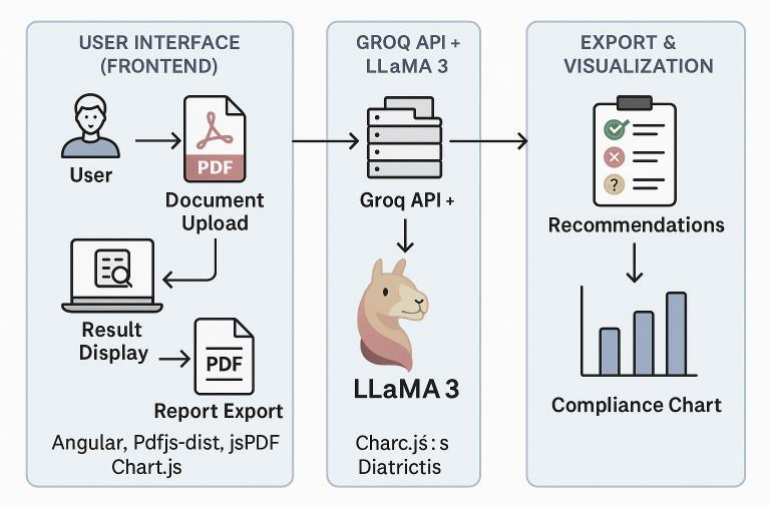

Figura 16 - Arquitetura do Sistema

3.3.3. Requisitos Funcionais

Os principais requisitos funcionais da plataforma NIS 2 Insight foram definidos com base nas necessidades práticas das equipas de auditoria e *compliance*, e visam atender às lacunas identificadas na revisão de literatura. Estes requisitos incluem:

- Submissão de documentos em formato PDF representando contratos, políticas internas ou relatórios normativos;
- Extração automática de texto dos documentos submetidos, utilizando a biblioteca pdfjs-dist;
- Realizar uma análise semântica automatizada com base nos princípios e obrigações da NIS 2, incluindo:
    - Gestão de riscos de terceiros;
    - Controlo de acessos;
    - Políticas de autenticação e encriptação;
    - Cláusulas contratuais obrigatórias.
- Identificação automática do tipo de política analisada (ex.: controlo de acessos, fornecedores, etc.);
- Gerar de recomendações específicas e contextualizadas para colmatar as falhas detetadas;
- Apresentação dos resultados em formato visual (lista de critérios, gráfico de barras com percentagem de conformidade, nível de risco);
- Gerar de relatórios formais em PDF com critérios e recomendações para consulta por equipas de *compliance*, TI ou auditoria.

Estes objetivos visam responder diretamente às lacunas identificadas na revisão de literatura, nomeadamente a ausência de ferramentas práticas e automatizadas de apoio à conformidade regulatória com a Diretiva NIS 2.

3.3.4. Arquitetura Técnica e Tecnológica

A aplicação foi construída utilizando uma arquitetura modular que assegura flexibilidade, escalabilidade e desempenho otimizado. As tecnologias selecionadas para o desenvolvimento da aplicação incluem:

- *Frontend*:
  - Angular
    - Estrutura SPA (Single Page Application) moderna e modular;
  - `pdfjs-dist`: Para assegurar um pré-processamento eficiente e previsível, a aplicação implementa uma rotina de extração textual baseada na biblioteca `pdfjs-dist`, recorrendo ao seu módulo principal `pdfjsLib`. Este módulo permite carregar e percorrer cada página do documento PDF, extraindo o respetivo conteúdo textual através da função `getTextContent()`.

    A Figura 17 apresenta o método responsável por processar o documento, concatenando o texto de todas as páginas e aplicando um limite de 30 páginas e 15.000 caracteres, de forma a garantir desempenho estável e tempos de resposta adequados durante a análise efetuada pelo modelo de linguagem.

```
async extractTextFromPdf(file: File): Promise<string> {
  const arrayBuffer = await file.arrayBuffer();
  const pdf = await (pdfjsLib as any).getDocument({ data: arrayBuffer }).promise;
  let fullText = '';
  const maxPages = Math.min(pdf.numPages, 30);
  for (let i = 1; i <= maxPages; i++) {
    const page = await pdf.getPage(i);
    const content = await page.getTextContent();
    const pageText = content.items.map((item: any) => item.str).join(' ');
    fullText += pageText + '\n';
  }
  return fullText.slice(0, 15000);
}
```

Figura 17 - Extração de texto do PDF com pdfjs-dist

  - ng2-charts (Chart.js): A métrica de conformidade é derivada do estado de cada critério, mapeado para {1, 0.5, 0}. A percentagem global alimenta a visualização (Chart.js/ng2-charts) e o alerta de risco. A Figura 18 seguinte apresenta o cálculo e a atualização do *dataset*.

```
//  Métrica de conformidade e gráfico
this.nis2Data = this.nis2CriteriaStatus.map(i =>
  i.status === 'conforme' ? 1 : i.status === 'insuficiente' ? 0.5 : 0
);
this.nis2Percent = Math.round(
  (this.nis2CriteriaStatus.filter(i => i.status === 'conforme').length / this.nis2CriteriaStatus.length) * 100
);
if (this.nis2Percent === 100) this.noRecommendations = true;

// // Atualiza labels e dataset
this.nis2Labels = this.nis2CriteriaStatus.map(c => c.label);
this.nis2Chart = {
  ...this.nis2Chart,
  data: {
    ...this.nis2Chart.data,
    labels: this.nis2Labels,
    datasets: [{ ...this.nis2Chart.data.datasets[0], data: this.nis2Data }]
  }
};
```

Figura 18 - Cálculo de conformidade e atualização do gráfico

- `jsPDF`: Para a criação automática de relatórios formais, a aplicação recorre à biblioteca `jsPDF`, que permite gerar documentos PDF diretamente no *frontend* de forma dinâmica e personalizada.

  O processo tem início com a instrução `const doc = new jsPDF();`, responsável pela criação de uma nova instância do documento em memória, esta instância é o objeto central através do qual são adicionados todos os elementos textuais e gráficos.

  A partir desta estrutura base, o sistema define margens, espaçamento, tipografia e cores, registando fontes personalizadas como a `DejaVuSans` para garantir compatibilidade com caracteres acentuados e símbolos específicos da língua portuguesa.

  Para assegurar consistência visual e evitar duplicação de código, foram também criadas funções auxiliares (*helpers*), designadas `write`, `writeH` e `writeList`, responsáveis pela formatação de texto, títulos e listas de forma uniforme em todo o relatório.

  A Figura 19 apresenta o excerto do código responsável pela estruturação do relatório PDF e pela definição dos *helpers* de formatação utilizados na aplicação.

```
const write = (
  txt: string,
  opts?: { x?: number; gap?: number; color?: [number, number, number]; fontSize?: number; bold?: boolean }
) => {
  const x = opts?.x ?? margin.left;
  const gap = opts?.gap ?? lineGap;
  if (opts?.fontSize) doc.setFontSize(opts.fontSize); else doc.setFontSize(11);
  doc.setFont('DejaVuSans', opts?.bold ? 'bold' : 'normal');
  if (opts?.color) doc.setTextColor(...opts.color); else doc.setTextColor(0,0,0);

  const availWidth = maxWidth - (x - margin.left);
  const lines = doc.splitTextToSize(txt, availWidth);

  lines.forEach((ln: string) => {
    ensureSpace(gap);
    doc.text(ln, x, y);
    y += gap;
  });
};

const writeH = (txt: string, level: 1 | 2 = 1) => {
  y += level === 1 ? 0 : sectionGap;
  write(txt, { fontSize: level === 1 ? 16 : 13, bold: true, gap: lineGap + 1 });
};

const writeList = (title: string, items?: string[]) => {
  if (!items || !items.length) return;
  write(title, { bold: true });
  const bulletX = margin.left + 4;
  items.forEach((it) => write('• ' + it, { x: bulletX }));
  y += smallGap;
};
```

Figura 19 - *Helpers* de *layout* para relatório PDF (jsPDF)

- *Backend*:

  A camada de *backend* é responsável pela comunicação direta com a API da Groq, que disponibiliza o modelo LLaMA 3 70B utilizado para a inferência linguística. É nesta fase que o texto extraído do documento é preparado e enviado ao modelo, juntamente com o *prompt* estruturado que contém os critérios de conformidade da Diretiva NIS 2.

  Antes de invocar o modelo, a aplicação executa uma etapa intermédia de classificação do documento, através de uma heurística lexical simples, implementada no *frontend* com *TypeScript*. Este mecanismo analisa a ocorrência de termos-chave (por exemplo, *"*controlo de acessos" ou *"*fornecedor*"*) para determinar automaticamente o tipo de política em avaliação. A Figura 20 ilustra o excerto de código responsável por esta heurística de deteção, onde se verifica a lógica condicional que identifica o tipo de documento e ajusta dinamicamente a grelha de critérios e palavras-chave (*keywords*) aplicáveis. Esta identificação prévia permite garantir maior precisão na análise e reduzir falsos positivos durante o processo de inferência.

```
// --- Deteção do tipo de política
let tipo: 'fornecedor' | 'controlo' | 'desconhecido' = 'desconhecido';
const lowerText = text.toLowerCase();
if (lowerText.includes('controlo de acessos') || lowerText.includes('controlo de acesso')
  || lowerText.includes('acessos') || lowerText.includes('acesso')) {
  tipo = 'controlo';
} else if (lowerText.includes('fornecedor') || lowerText.includes('fornecedores')) {
  tipo = 'fornecedor';
}
this.policyType = tipo;
```

Figura 20 - Heurística de deteção do tipo de política

- Pré-processamento: A fase de pré-processamento é essencial para normalizar e estruturar o texto antes de ser analisado pelo modelo de linguagem. Nesta etapa são utilizadas bibliotecas de normalização de texto, como `diacritics`, para remover acentuação e garantir uniformidade lexical; expressões regulares (*regex*), que permitem identificar padrões como listas numeradas ou secções de critérios; e um algoritmo de *fallback* semântico, que assegura a interpretação correta mesmo quando a resposta do modelo não segue o formato esperado.

  A Figura 21 apresenta o excerto do código que implementa este algoritmo de *fallback* semântico, responsável por comparar frases afirmativas e negativas (por exemplo, *"existe"*, *"implementado"*, *"não existe"*, *"ausente"*) para inferir

automaticamente o grau de conformidade de cada critério, mesmo quando o modelo não devolve a estrutura padronizada.

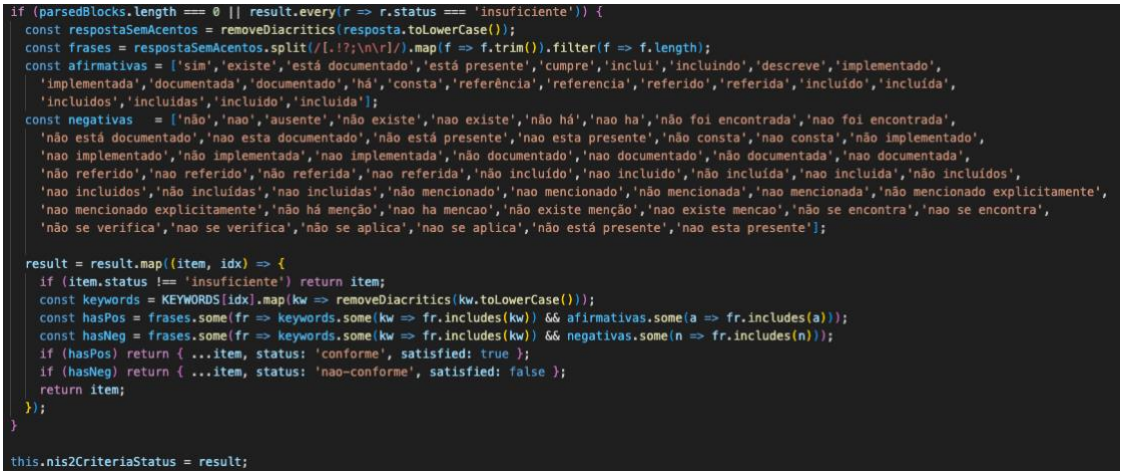

Figura 21 - Fallback semântico baseado em palavras-chave

Por fim, o sistema inclui mecanismos de tratamento de erros e validação de segurança, que asseguram uma comunicação robusta com a API da Groq. Situações como a descontinuação do modelo, credenciais inválidas ou falhas de rede são detetadas e comunicadas ao utilizador através de mensagens descritivas, evitando interrupções inesperadas e garantindo uma experiência fluida. A Figura 22 apresenta o excerto de código que implementa este comportamento, localizado na fase final da chamada HTTP. Nesta secção, são verificados códigos de erro específicos (como `401`, `403` ou `model_decommissioned`), e são geradas mensagens adequadas em `this.errorMsg`, que são depois exibidas na interface, assegurando que o utilizador compreende o motivo da falha e pode reagir de forma informada.

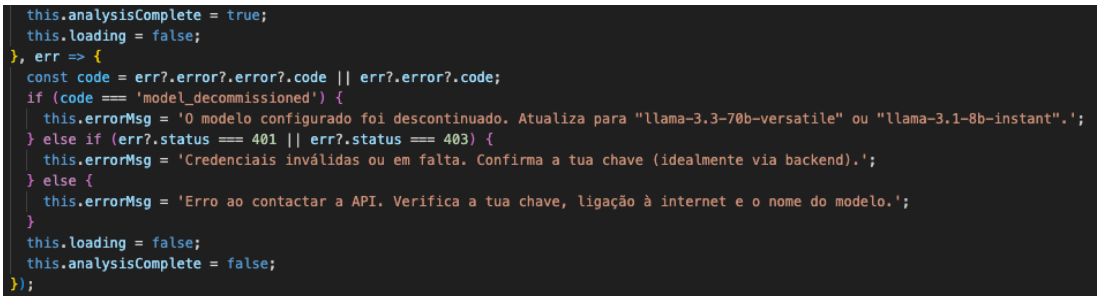

Figura 22 - Tratamento de erros e comunicação ao utilizador

Este desenho técnico garante que a plataforma seja eficiente em termos de desempenho e facilidade de manutenção, enquanto oferece flexibilidade para integrações futuras, por exemplo, com modelos privados *self-hosted* ou plataformas de Governança, Risco e Conformidade (GRC) corporativas.

3.3.5. Interface de Utilizador

A interface foi desenvolvida para ser simples, intuitiva e responsiva (Figura 23). O utilizador apenas necessita carregar o documento, após o qual a análise é realizada automaticamente. A ênfase recai na usabilidade, uma vez que a solução é destinada não só a especialistas em TI, mas também a profissionais de *compliance* sem formação técnica em IA. As principais funcionalidades da interface incluem:

- *Drag & drop* de ficheiros.
- Barra de progresso durante a extração do texto.
- Visualização do nível de risco por cores (verde, amarelo, vermelho).
- Botão de exportação imediata de relatórios formais.

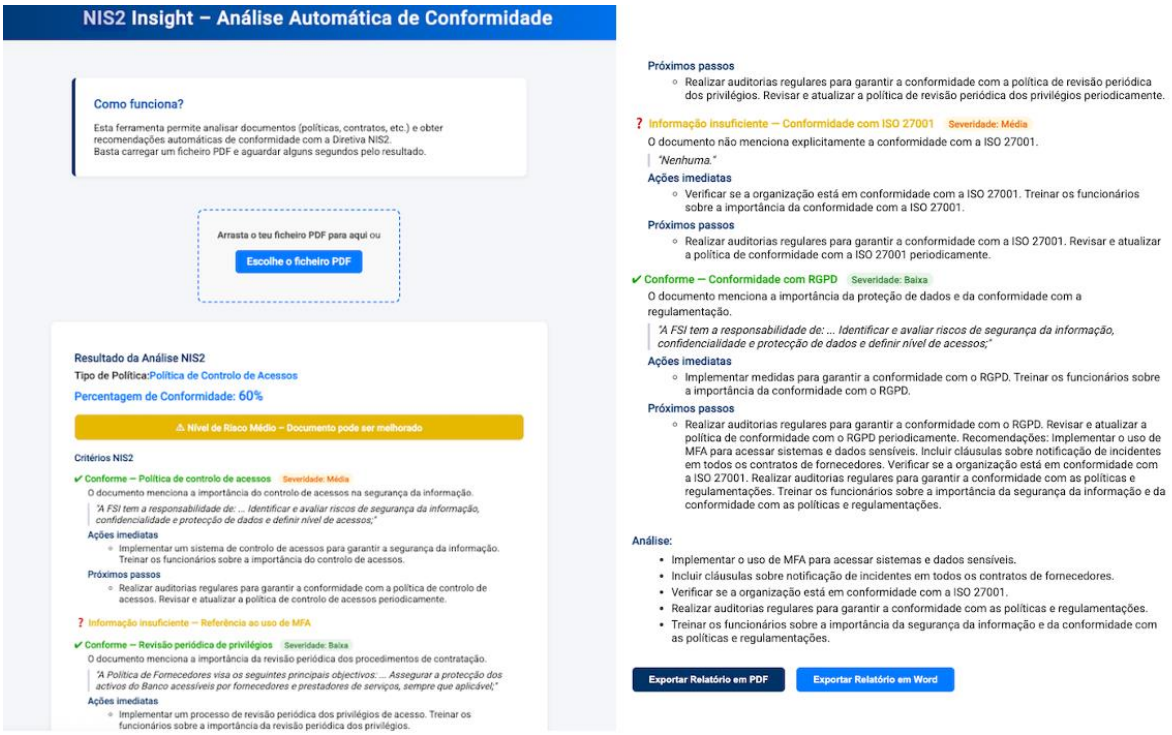

Figura 23 - Interface de utilizador, destacando o *layout* e funcionalidades principais

3.3.6. Motor de Análise (IA via Groq API)

A camada de análise constitui o núcleo inteligente da plataforma, sendo responsável por transformar o texto extraído do documento em informação estruturada e avaliável de acordo com os critérios da Diretiva NIS 2.

Esta componente combina a capacidade interpretativa de um modelo de Linguagem de Grande Escala (LLaMA 3 70B) com um conjunto de regras programáticas complementares, garantindo equilíbrio entre automatização e controlo semântico.

O processo de análise segue quatro fases principais:

- Preparação e envio do texto - O conteúdo pré-processado é enviado à API da Groq acompanhado de um *prompt* estruturado, que define os oito critérios de conformidade a avaliar. Este *prompt* padronizado orienta o modelo a devolver respostas num formato previsível, facilitando o tratamento posterior dos resultados.
- Interpretação da resposta - A resposta textual gerada pelo modelo é interpretada pela aplicação através de um *parser* baseado em expressões regulares. O *parser* refere-se a um componente de software responsável por analisar e estruturar informação textual de forma sistemática. No contexto da plataforma NIS 2 Insight, o *parser* identifica padrões e seções delimitadas (como listas numeradas ou campos específicos, por exemplo *Justificação*, *Evidência* ou *Ações imediatas*), convertendo a saída textual do modelo num formato estruturado de dados (objetos e variáveis). Em termos práticos, o *parser* irá funcionar como uma ponte entre a linguagem natural e a lógica do sistema, permitindo que o texto produzido pela IA seja transformado em informação utilizável e quantificável.
- Avaliação e categorização - Cada critério é classificado como *conforme*, *não conforme* ou *insuficiente* com base nas expressões identificadas pelo modelo. Nos casos em que a resposta não segue o formato esperado, aplica-se um mecanismo de validação semântica (*fallback*), que analisa frases afirmativas e negativas para inferir o estado de conformidade. Este comportamento assegura a robustez do sistema e evita perda de informação relevante.
- Cálculo da conformidade global - Após a análise de todos os critérios, o sistema calcula a percentagem total de conformidade e atualiza os elementos visuais da interface (gráfico e indicadores de risco). Esta percentagem serve como índice quantitativo de maturidade NIS 2, orientando as equipas de auditoria na priorização das ações corretivas.

A Figura 24 sintetiza este processo de raciocínio em quatro etapas, desde a receção do texto até à geração do relatório final.

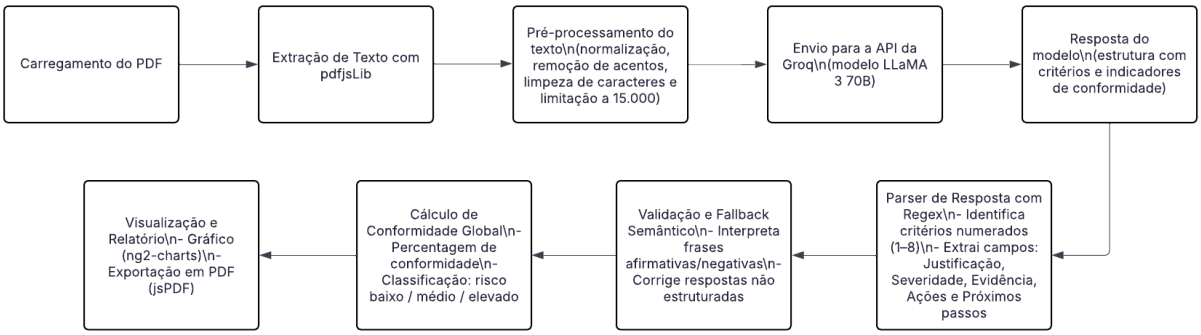

Figura 24 - Fluxo de análise e decisão do motor IA NIS 2 Insight

3.3.7. Visualização e Exportação de Resultados

Depois de concluída a análise, os resultados são apresentados ao utilizador de forma clara e visualmente apelativa. A aplicação calcula a percentagem de conformidade com base no número de critérios assinalados como "conforme" e apresenta essa informação em duas formas complementares:

- Lista de critérios com ícones e respetivo estado;
- Alerta do nível de risco a cores (verde, amarelo e vermelho);
- Recomendações automáticas organizadas por secções: pontos positivos, pontos de melhoria e sugestões finais;
- Relatório PDF gerado com jsPDF, com cabeçalho institucional, separador por critérios e recomendações detalhadas.

Deste modo, a ferramenta não só identifica falhas, mas também fornece orientações práticas de mitigação, facilitando a integração dos resultados em planos de ação.

3.3.8. Resultados Esperados

A implementação da ferramenta visa alcançar diversos objetivos:

- Reduzir o tempo de análise e o custo das auditorias internas, promovendo uma análise automatizada e eficiente;
- Aumentar a consistência e qualidade das avaliações de conformidade;
- Apoiar equipas não especializadas na interpretação das obrigações da NIS 2, facilitando a compreensão e tomada de decisão;
- Promover uma cultura de conformidade proativa, com base em recomendações claras e objetivas.

3.3.9. Código fonte

O respetivo código fonte da NIS 2 Insight pode ser consultado através do seguinte repositório GitHub respetivamente:

- https://github.com/joaoantas05/iscte_nis2insight

3.3.10. Recomendações e Tendências Futuras

A análise comparativa entre a plataforma como o ALYA e a proposta NIS 2 Insight evidencia que a IA pode desempenhar um papel estruturante na transformação da cibersegurança no setor financeiro. No entanto, a adoção de tais soluções requer um conjunto de recomendações estratégicas e de linhas de evolução futura, que permitam assegurar não apenas ganhos de eficiência, mas também segurança, conformidade regulatória e sustentabilidade tecnológica.

As recomendações apresentadas a seguir resultam da articulação entre os resultados obtidos neste estudo, as melhores práticas internacionais (NIST, ISO/IEC 27001), e os regulamentos europeus emergentes, nomeadamente a Diretiva NIS 2, o Digital Operational Resilience Act (DORA) e o AI Act.:

- Reforço da Automação na Gestão de Riscos: A utilização de IA deve evoluir de um papel meramente assistivo para uma abordagem proativa e preditiva na gestão de riscos de terceiros.
- Em vez de apenas verificar se as políticas estão ou não conformes, os modelos podem ser treinados para antecipar vulnerabilidades futuras com base em dados históricos de incidentes, falhas contratuais ou auditorias anteriores.
- Exemplo: um fornecedor que, em três auditorias consecutivas, apresenta lacunas na notificação de incidentes deve ser identificado como risco emergente, mesmo que o contrato atual cumpra formalmente os requisitos.
- Esta prática aproxima-se do conceito de *continuous risk assessment*, defendido pelo NIST Cybersecurity Framework, e é particularmente relevante num setor como o financeiro, onde a cadeia de fornecimento é frequentemente o elo mais frágil.
- Monitorização Contínua e Auditoria Inteligente: As auditorias anuais ou semestrais, embora necessárias, são insuficientes perante o ritmo acelerado das ameaças cibernéticas.

- A tendência futura aponta para auditorias inteligentes e contínuas, apoiadas por algoritmos de deteção de anomalias em tempo real.
- Isso implica que a avaliação da conformidade com a NIS 2 não seja um exercício pontual, mas sim um processo permanente, com geração de alertas e relatórios sempre que um documento for atualizado ou um novo fornecedor contratado.
- Exemplo: se uma política de acessos for alterada e deixar de mencionar o uso de MFA, o sistema deverá assinalar de imediato a falha e sugerir correções, sem necessidade de esperar pela próxima revisão anual.
- Esta abordagem reduz o chamado *compliance gap*, garantindo que as instituições mantêm conformidade dinâmica e não apenas estática.
- Adoção de Modelos de IA Explicáveis e Transparentes: Um dos grandes desafios das soluções atuais, como a NIS 2 Insight em versão inicial, é a dependência de APIs públicas de fornecedores externos (Groq, OpenAI, etc.).
- Esta dependência levanta questões de segurança e soberania digital, dado que documentos internos e sensíveis podem ser processados fora do controlo da organização.
- Para ultrapassar esta limitação, recomenda-se a evolução para a utilização de LLMs privados (*self-hosted*), executados em infraestruturas próprias ou em *clouds* soberanas europeias, em conformidade com o RGPD e com o AI Act.
- Modelos como o LLaMA (Meta)**,** Falcon (TII) ou Mistral podem ser ajustados ao contexto regulatório europeu e afinados (fine-tuned) com documentos financeiros reais, aumentando a precisão na análise de conformidade.
- Adicionalmente, a tendência regulatória aponta para a exigência de explicabilidade e auditabilidade dos modelos, algo que só é viável quando a instituição detém controlo total sobre a arquitetura e o ciclo de vida da IA.
- Integração de Normas e Melhores Práticas: Promover a interoperabilidade entre sistemas de segurança, alinhando a gestão de fornecedores às normas ISO/IEC 27001, RGPD e às diretrizes do NIST, garantindo um nível de conformidade elevado e consistente.
- Resiliência e Adaptação a Novas Ameaças: Desenvolver estratégias flexíveis de cibersegurança que combinem modelos tradicionais com abordagens inovadoras, como Zero Trust e autenticação adaptativa, para responder eficazmente a novas tipologias de ataques cibernéticos.

A evolução contínua das tecnologias de IA e ML representa uma oportunidade para transformar a cibersegurança no setor financeiro. A integração de soluções inteligentes não só fortalece a proteção dos sistemas contra ameaças emergentes, como também permite uma gestão mais eficiente dos riscos associados a fornecedores externos e acessos críticos, promovendo uma transformação digital sustentável e alinhada com os desafios regulatórios e tecnológicos do futuro.

CAPÍTULO 4

Testes e Discussão de Resultados

Para validar a eficácia e a aplicabilidade do protótipo desenvolvido, foi conduzida uma fase experimental baseada na análise de documentos organizacionais reais. O objetivo consistiu em verificar até que ponto a plataforma NIS 2 Insight é capaz de identificar, de forma automática, consistente e reprodutível, evidências de conformidade com os critérios estabelecidos pela Diretiva NIS 2, com ênfase nas áreas de gestão de fornecedores e controlo de acessos. Foram selecionados documentos normativos de referência, designadamente políticas internas de segurança, políticas de gestão de acessos e documentos contratuais com terceiros, pertencentes a uma instituição financeira, de modo a avaliar o desempenho da ferramenta em contextos com elevada exigência regulatória e robustez formal.

4.1. Etapas do processo de avaliação

A interpretação dos resultados obtidos pelo protótipo NIS 2 Insight assenta num conjunto de métricas definidas de forma a tornar a avaliação objetiva, transparente e replicável. Estas métricas são calculadas em várias etapas:

1. Identificação de critérios aplicáveis

Numa primeira fase, a aplicação determina o tipo de política em análise (p. ex., controlo de acessos, fornecedores ou desconhecido). Este mapeamento é obtido por heurísticas léxicas (palavras-chave, normalização de acentos) e permite selecionar automaticamente o conjunto de critérios da NIS 2 mais relevantes ao domínio do documento.

- Exemplo: para controlo de acessos, os critérios incluem política formal de acessos, referência a MFA, revisão periódica de privilégios e conformidade normativa; para fornecedores, incluem avaliação de fornecedores, cláusulas de confidencialidade e responsabilidade, notificação de incidentes e referências a ISO 27001/RGPD.

Esta adaptação por contexto é reforçada por ficheiros de regras e *prompts* especializados que orientam o LLM para o vocabulário normativo e os requisitos do Artigo 21.º da NIS 2. Tal orientação reduz ambiguidade semântica, aumenta a consistência entre execuções e facilita, no futuro, a parametrização por setor (banca, seguros, *fintech*).

2. Classificação de critérios

Cada critério é avaliado e classificado automaticamente como:

- Conforme (valor = 1) → quando o documento contém referência explícita ao requisito ou quando o modelo identifica evidência inequívoca;
- Não conforme (valor = 0) → quando não existe menção ou há indicação clara de ausência;
- Informação insuficiente (valor = 0,5) → quando existem indícios parciais, mas não há referência suficiente para confirmar a conformidade.

A decisão resulta de três mecanismos complementares, aplicados em cascata:

- Correspondência direta a expressões explícitas devolvidas pelo LLM (e.g., "Conforme", "Não conforme", "Informação insuficiente").
- *Parsing* estruturado por *regex* quando a resposta vem em lista numerada ou com rótulos previsíveis (captura de "N. <Critério>: <emoji/estado> + blocos de Justificação/Severidade/Evidência/Ações").
- *Fallback* semântico por palavras-chave afirmativas/negativas e sinónimos ("existe", "implementado", "documentado" vs. "não existe", "ausente", "não implementado"), útil quando o LLM produz texto mais descritivo.

Este desenho a três níveis mitiga variações na redação da resposta do modelo e aumenta a robustez do classificador ao estilo do documento.

3. Cálculo da percentagem de conformidade

Uma vez atribuídos valores a cada critério, calcula-se a percentagem de conformidade através da seguinte fórmula:

$$\text{Conformidade (\%)} = \frac{\sum_{i=1}^{N} vi}{N} \times 100,$$

onde:

- N = número total de critérios aplicáveis;
- v_i = valor atribuído a cada critério (1, 0 ou 0,5).

Exemplo: para 4 critérios avaliados (✓, ✗, ✗, ✓), somamos os valores:

$$✓ = 1,\ ✗ = 0,\ ✗ = 0,\ ✓ = 1 \rightarrow \text{soma} = 2.$$

$$\text{Conformidade (\%)} = \frac{2}{4} \times 100 = 50\%.$$

Importa reforçar que para o valor 0,5 para ? reflete a presença de indícios parciais, incentivando completude documental sem penalizar em excesso a ausência de evidência explícita.

4. Determinação do nível de risco

A percentagem calculada é convertida num nível de risco categórico através de uma escala semafórica:

- Verde (baixo risco): ≥ 80% de conformidade;
- Amarelo (risco médio): 50-79% de conformidade;
- Vermelho (risco elevado): < 50% de conformidade.

Esta escala simplifica a priorização de ações e facilita comunicação executiva de resultados.

5. Geração de recomendações

Para cada critério avaliado como ✗ ou ?, a aplicação associa recomendações específicas, baseadas em boas práticas de cibersegurança e nas obrigações da NIS 2. Estas recomendações são apresentadas em três secções:

- Pontos positivos: aspetos já em conformidade;
- Pontos de melhoria: lacunas identificadas;
- Sugestões finais: recomendações práticas de implementação p. ex., “ativar MFA em contas privilegiadas”, “introduzir cláusula de auditoria em contratos”.

As recomendações são orientadas por boas práticas (NIS 2, ISO/IEC 27001, RGPD) e ajustadas ao tipo de política que é detetada.

6. Visualização e exportação

Os resultados são apresentados ao utilizador em três camadas complementares:

- Lista de critérios com ícones (✓, ✗, ?) e respetiva justificação;
- Gráfico de barras com percentagem de conformidade;
- Alerta de risco por cor (verde, amarelo, vermelho).

Adicionalmente, disponibiliza-se exportação para PDF/Word, contendo percentagem global, nível de risco, detalhes por critério e recomendações, um formato adequado a auditorias internas e dossiês de conformidade.

A Figura 25 apresenta o fluxo de processamento da aplicação NIS 2 Insight, evidenciando as principais etapas desde a submissão do documento até à exportação do relatório final.

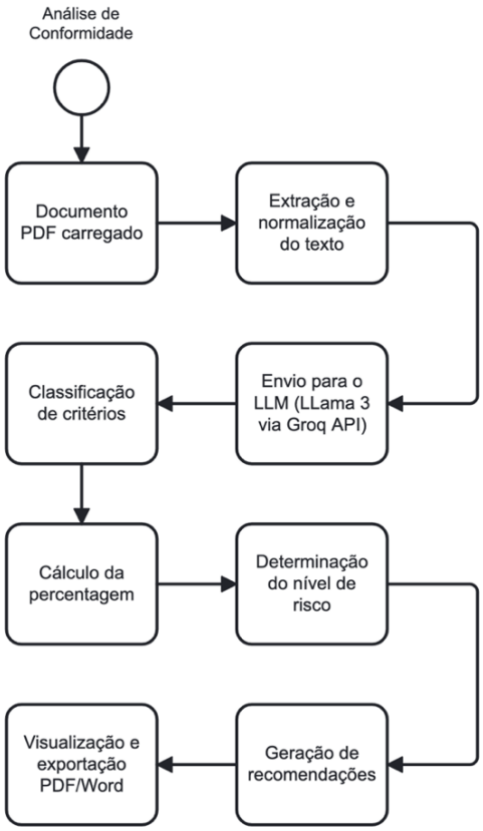

Figura 25 - Fluxo de processamento da aplicação NIS 2 Insight

O diagrama ilustra o *pipeline* completo: submissão do documento PDF, extração e normalização do texto, envio ao modelo de linguagem (LLaMA 3 via API Groq), classificação automática dos critérios (✓, ✗, ?), cálculo da percentagem de conformidade, determinação do nível de risco, geração de recomendações e visualização/exportação em relatório.

A aplicação atinge os seus valores de conformidade através de um processo transparente, normatizado e reprodutível, assegurando que documentos diferentes seguem a mesma lógica de cálculo. Este mecanismo garante comparabilidade e consistência nos resultados.

Contudo, salienta-se que a interpretação está dependente da terminologia utilizada no documento: a ausência de termos explícitos (por exemplo, "MFA") conduz a uma classificação de não conformidade, mesmo que existam controlos equivalentes descritos de forma implícita. Assim, a ferramenta deve ser entendida como um apoio à análise regulatória, e não como substituto de auditorias formais, constituindo um complemento útil e eficiente para equipas de *compliance* e cibersegurança.

4.2. Testes a políticas selecionadas

Cada ensaio compreendeu as seguintes etapas: submissão do documento à aplicação; extração automática do conteúdo textual; análise com recurso a modelo de Linguagem de Grande Escala (LLM), interpretação e estruturação dos resultados e, por fim, comparação destes resultados com a leitura humana. O desenho experimental procurou, assim, conciliar avaliação quantitativa (métricas e percentagens de conformidade) com avaliação qualitativa (coerência das justificações, utilidade das recomendações, clareza na visualização e no relatório).

4.2.1. Teste 1 com a Política de Gestão de Acessos

O primeiro ensaio de validação da plataforma NIS 2 Insight foi conduzido com a "Política de Gestão de Acessos" do Banco Económico (versão 1.0, novembro de 2024), documento organizacional que define princípios, responsabilidades e procedimentos relativos ao controlo de acessos. Este documento contempla medidas de autenticação, segregação de funções, gestão de privilégios e alinhamento normativo com a ISO/IEC 27001:2022, constituindo um bom caso de estudo para aferir a capacidade da ferramenta em identificar critérios de conformidade com a Diretiva NIS 2.

Após a submissão do ficheiro PDF na aplicação, a plataforma procedeu à extração automática do texto e à sua análise com recurso ao modelo LLaMA 3 70B. O sistema classificou automaticamente o documento como Política de Controlo de Acessos, atribuindo uma percentagem global de conformidade de 60% e categorizando-o como de risco médio, com a indicação de que o documento poderia ser melhorado.

A Figura 26 ilustra a interface da ferramenta após a submissão do documento, evidenciando o processo de upload e a deteção automática do tipo de política, bem como, os resultados da análise, apresentados em formato textual estruturado. A plataforma assinalou como conforme a existência de uma política de controlo de acessos, bem como a revisão periódica de privilégios e a referência explícita à ISO 27001. Assinalou como informação insuficiente a menção ao uso de autenticação multifator (MFA), justificando que a formulação encontrada no documento não estabelecia critérios mandatórios. Por fim, classificou como não conforme a referência ao RGPD, uma vez que não foram identificadas menções diretas ao regulamento.

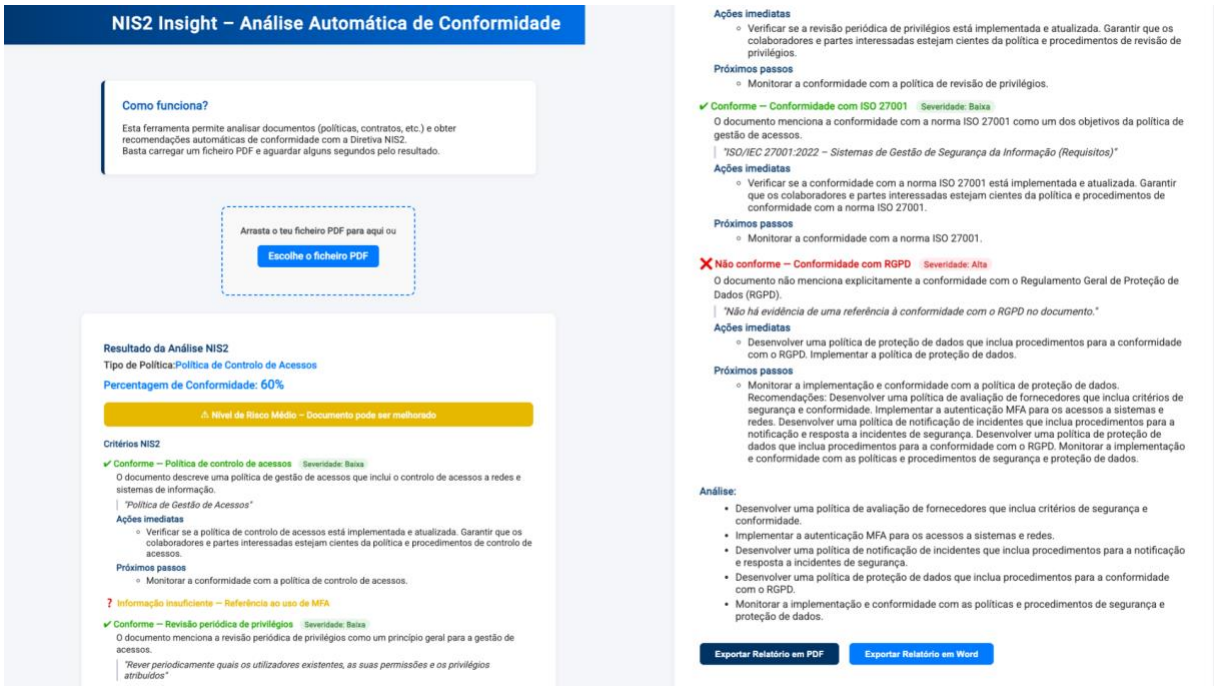

Figura 26 - Resultados da política de controlos de acessos do Banco Económico

A comparação entre a análise automatizada e a leitura manual do documento confirmou a coerência da classificação nos critérios de política de acessos, revisão de privilégios e ISO 27001, que estão de facto documentados. Quanto ao critério MFA, verificou-se que a política contém apenas uma recomendação genérica (“sempre que possível”) sem imposição obrigatória para determinados perfis ou sistemas, justificando a marcação como “informação insuficiente”. Relativamente ao RGPD, confirmou-se a ausência de qualquer referência explícita, reforçando a pertinência da classificação “não conforme”.

A Figura 27 apresenta a síntese analítica produzida pela aplicação, onde são listadas recomendações adicionais e representada graficamente a conformidade do documento com os

critérios da NIS 2. No painel de recomendações, a plataforma sugere a criação de políticas complementares, como a implementação de autenticação multifator (MFA) em acessos a sistemas e redes, a definição de procedimentos de notificação e resposta a incidentes de segurança, e a integração de cláusulas contratuais e normativas relacionadas com a proteção de dados pessoais em conformidade com o RGPD. Estas recomendações surgem como resultado direto das lacunas detetadas na análise textual, correspondendo a áreas onde a política em avaliação não apresenta evidência suficiente ou não faz qualquer referência normativa.

Figura 27 - Resultados gráficos e recomendações da análise da Política de Gestão de Acessos

O gráfico de barras incluído na mesma figura apresenta a distribuição dos resultados por critério avaliado. Observa-se que a política foi considerada conforme relativamente à existência de uma política formal de controlo de acessos, à revisão periódica de privilégios e à referência explícita à ISO 27001. Em contrapartida, obteve a classificação de informação insuficiente no que respeita à utilização de MFA, o que explica a menor altura da barra correspondente, refletindo uma implementação incompleta ou não obrigatória. Por fim, no critério de conformidade com o RGPD, a barra apresenta valor nulo, traduzindo a ausência de evidência no documento de qualquer referência explícita ao regulamento europeu de proteção de dados.

Em síntese, este primeiro ensaio demonstra que a ferramenta é capaz de identificar corretamente o tipo de documento e mapear os principais critérios de conformidade com a NIS 2. Os resultados produzidos mostraram-se consistentes com a evidência textual e ofereceram recomendações práticas, revelando que o sistema pode apoiar equipas de auditoria e *compliance* ao fornecer uma avaliação inicial estruturada, clara e exportável, complementada pela possibilidade de geração automática de relatórios em formato PDF ou Word, facilitando a integração nos processos formais de reporte regulatório (Anexo A).

4.2.2. Teste 2 com a Política de Fornecedores

O segundo ensaio experimental foi realizado com a Política de Fornecedores do Banco BPI, documento normativo que estabelece princípios, responsabilidades e cláusulas contratuais a observar na relação com terceiros. O documento insere-se no âmbito do Código de Conduta de Fornecedores, que define critérios para a seleção e avaliação de parceiros externos, incluindo aspetos éticos, sociais, ambientais e de governação, bem como obrigações de confidencialidade, notificação de incidentes e proteção de dados pessoais. Pela sua natureza e abrangência, trata-se de um documento diretamente relacionado com requisitos da Diretiva NIS 2, nomeadamente no que respeita à gestão de riscos da cadeia de fornecimento (supply chain security).

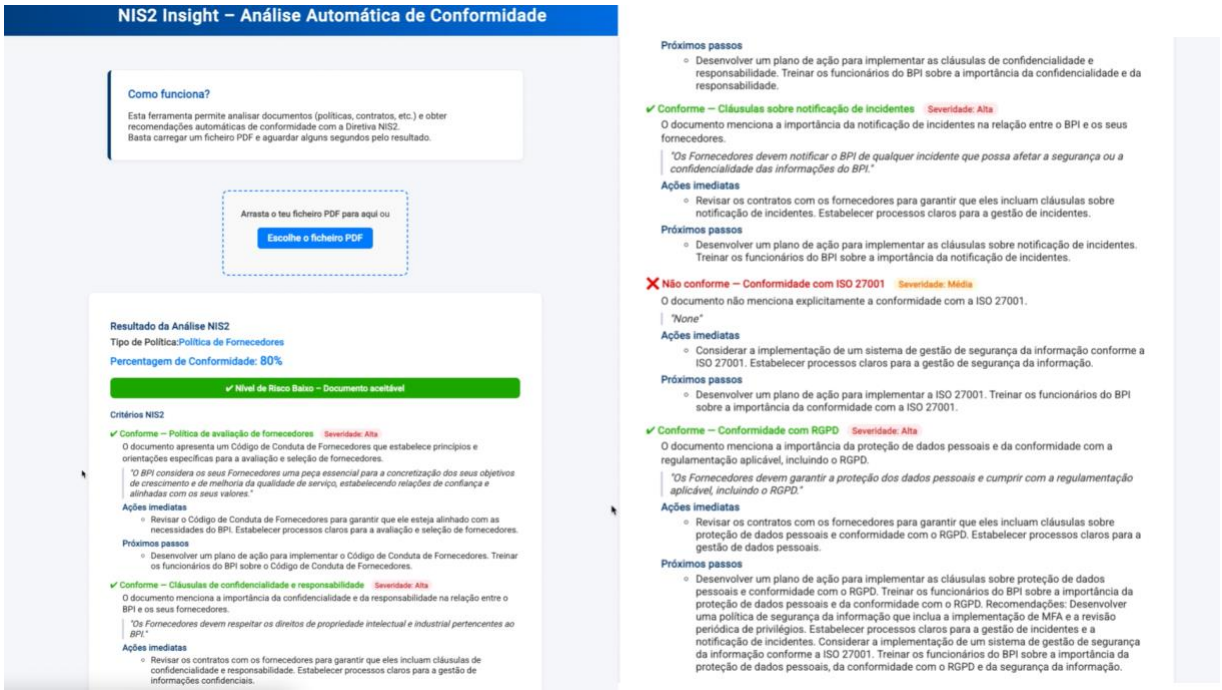

Figura 28 - Resultados da análise da Política de Fornecedores do Banco BPI

Após a submissão do ficheiro na aplicação, o sistema classificou automaticamente o documento como Política de Fornecedores, atribuindo-lhe uma percentagem global de

conformidade de 80% e categorizando-o como de risco baixo, considerando-o um documento aceitável. A Figura 28 apresenta o resultado global, com indicação do nível de risco e a lista inicial dos critérios avaliados.

A plataforma assinalou como conforme a política de avaliação de fornecedores, as cláusulas de confidencialidade e responsabilidade, as cláusulas sobre notificação de incidentes e a conformidade com o RGPD. Contudo, classificou como não conforme o critério de conformidade com a norma ISO 27001, justificando a ausência de evidência explícita no documento. Esta avaliação reflete a abrangência da política em matéria de governação da cadeia de fornecimento, mas também a sua limitação em remeter para standards internacionais de segurança da informação.

A Figura 29 apresenta a síntese gráfica dos resultados, onde se observa que quatro dos cinco critérios foram classificados como conformes, enquanto apenas a referência à ISO 27001 foi considerada não conforme. O painel de análise inclui ainda recomendações adicionais, entre as quais destaca-se a necessidade de elaborar uma política de segurança da informação que inclua a implementação de MFA e a revisão periódica de privilégios, bem como a definição de procedimentos que assegurem a notificação de incidentes. É igualmente sugerida a implementação de um sistema de gestão de segurança da informação conforme a ISO 27001, assim como a importância da formação dos colaboradores sobre a proteção de dados pessoais, a conformidade com o RGPD e a segurança da informação.

Figura 29 - Resultados gráficos e recomendações automáticas da análise da Política de Fornecedores

A comparação entre a leitura manual e a análise automática confirma que os critérios avaliados como conformes estão, de facto, contemplados no documento, nomeadamente a existência de princípios explícitos para a seleção de fornecedores, cláusulas de confidencialidade e proteção de dados, e disposições sobre notificação de incidentes. A ausência de qualquer referência explícita à norma ISO 27001 justifica a classificação negativa nesse critério, revelando uma oportunidade clara de reforço documental. Os resultados da análise também serão possíveis consultar através da geração automática de relatórios em formato PDF ou Word (Anexo B).

Em síntese, este ensaio mostra que a ferramenta é capaz de reconhecer e interpretar de forma consistente elementos-chave relacionados com a gestão de fornecedores e com a segurança da cadeia de abastecimento, fornecendo uma avaliação estruturada e recomendações práticas que podem ser diretamente aplicadas em processos de auditoria e *compliance*.

4.2.3. Teste 3 com a Política de Fornecedores

O terceiro ensaio de validação da plataforma NIS 2 Insight foi conduzido com outra versão da Política de Fornecedores da Adea Information Intelligence, desta vez um documento mais limitado em termos de abrangência e de referências normativas. O seu conteúdo centra-se sobretudo em aspetos de avaliação contínua do desempenho dos fornecedores, mas apresenta lacunas evidentes no que respeita a cláusulas contratuais críticas, requisitos normativos internacionais e obrigações legais, o que o torna um caso relevante para testar a sensibilidade da ferramenta na deteção de insuficiências documentais.

Após a submissão do ficheiro na aplicação, a plataforma classificou-o como Política de Fornecedores, atribuindo-lhe apenas 20% de conformidade e categorizando-o como documento de risco elevado, assinalado com falhas críticas. A Figura 30 mostra o resultado global da análise, em que se destaca a percentagem reduzida de conformidade e a indicação do nível de risco associado.

Na análise detalhada, apenas o critério relativo à existência de uma política de avaliação de fornecedores foi considerado conforme, uma vez que o documento prevê um sistema de avaliação contínua e indicadores de satisfação. Contudo, todos os restantes critérios revelaram problemas: as cláusulas de confidencialidade e responsabilidade foram classificadas como não conformes, por não existirem referências explícitas no texto; a conformidade com a norma ISO 27001 foi assinalada como de informação insuficiente, pela ausência de menções normativas;

e a conformidade com o RGPD foi avaliada como não conforme, dada a inexistência de qualquer referência a medidas de proteção de dados ou obrigações legais relacionadas.

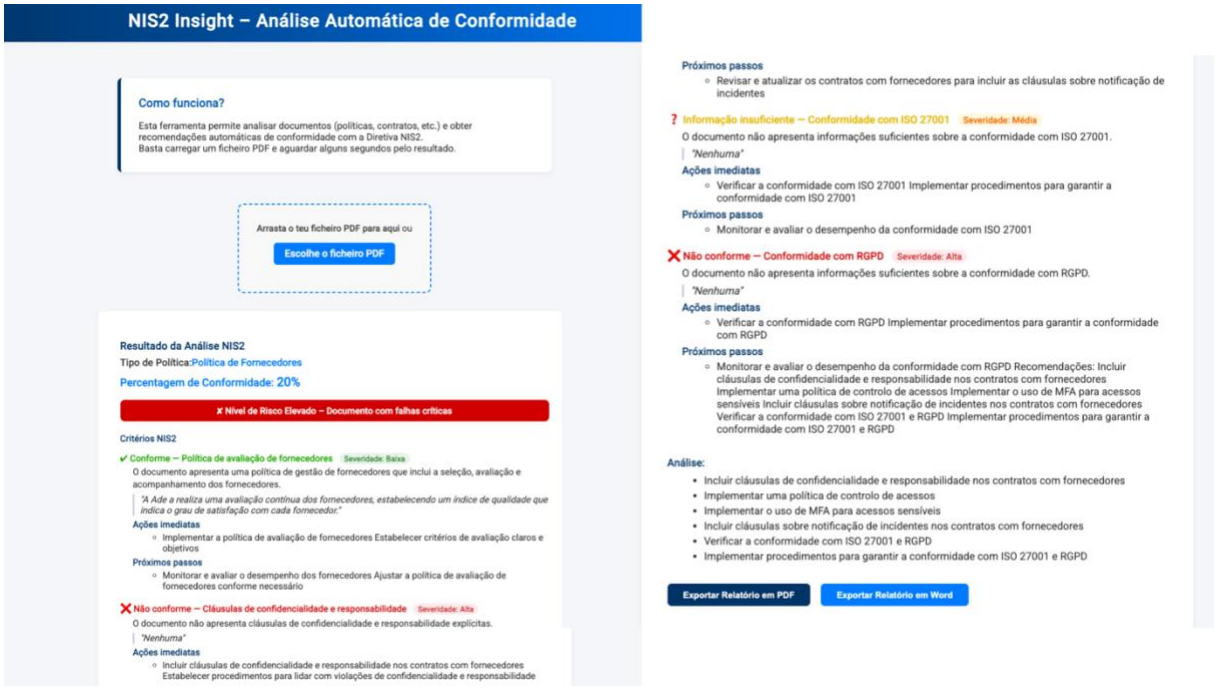

Figura 30 - Resultados globais da análise da Política de Fornecedores da Adea Information Intelligence

A Figura 31 apresenta a síntese gráfica dos resultados, evidenciando que apenas um critério foi considerado conforme, enquanto três foram avaliados como não conformes ou insuficientes. O painel de recomendações sugere a inclusão urgente de cláusulas de confidencialidade e responsabilidade nos contratos, a criação de uma política de controlo de acessos, a implementação de MFA para acessos sensíveis, a definição de cláusulas de notificação de incidentes e a introdução de referências explícitas tanto à ISO 27001 como ao RGPD.

Figura 31 - Resultados gráficos e recomendações automáticas da análise da Política de Fornecedores (risco elevado)

A análise manual confirmou a pertinência das classificações atribuídas pela aplicação. Embora o documento reconheça a necessidade de monitorizar o desempenho de fornecedores, não estabelece cláusulas robustas que assegurem confidencialidade, responsabilidade e proteção de dados, nem integra alinhamento com standards internacionais. Estas falhas explicam a avaliação de risco elevado, traduzida numa conformidade global de apenas 20%.

Em síntese, este terceiro ensaio evidencia a capacidade da plataforma em sinalizar documentos frágeis ou incompletos, fornecendo recomendações claras que orientam para a necessidade de reforço normativo e contratual. O resultado demonstra que a ferramenta não apenas valida boas práticas já existentes, mas também identifica, de forma estruturada, lacunas críticas que comprometem a conformidade com a Diretiva NIS 2, fornecendo assim um guião de melhoria para organizações cuja documentação ainda se encontra em fases preliminares de maturidade (Anexo C).

4.3. Avaliação da Eficácia da Ferramenta NIS 2 Insight

A ferramenta NIS 2 Insight demonstrou uma eficácia significativa na melhoria do processo de auditoria de cibersegurança. Ao automatizar a análise de documentos, a plataforma permitiu uma execução mais rápida das auditorias, sem comprometer a precisão das análises. Cada política é analisada em menos de 10 segundos, evidenciando a eficiência do sistema na avaliação de múltiplos documentos de forma mais ágil. A sua capacidade de identificar lacunas nas políticas de cibersegurança foi evidenciada em testes práticos, como na análise da "Política de Gestão de Acessos", onde detetou falhas importantes, como a ausência de autenticação multifatorial obrigatória. Além disso, a ferramenta proporcionou análises consistentes e uniformes, minimizando variações subjetivas comuns nas auditorias manuais. Ao fornecer recomendações claras para a melhoria das políticas e garantir a conformidade com a Diretiva NIS 2, a ferramenta mostrou-se uma solução eficiente, precisa e de grande valor para as instituições financeiras na gestão de riscos cibernéticos.

Deste modo, os resultados obtidos demonstram que a plataforma NIS 2 Insight melhora de forma simultânea a eficiência e a consistência das auditorias internas de cibersegurança, particularmente nos domínios do controlo de acessos e da gestão de fornecedores externos. A padronização dos critérios de avaliação, aliada à rapidez de processamento e à geração automática de recomendações, confirma o potencial dos LLMs como ferramentas de apoio à auditoria regulatória, reforçando a qualidade e a uniformidade das análises sem eliminar a necessidade de validação humana especializada.

CAPÍTULO 5

Conclusões

A presente dissertação teve como principal objetivo desenvolver uma solução baseada em Inteligência Artificial para a avaliação de conformidade de políticas de cibersegurança, com foco específico na gestão de fornecedores e no controlo de acessos no setor financeiro, à luz das exigências da Diretiva NIS 2.

Através da construção de um protótipo web, suportada por LLMs, demonstrou-se a viabilidade de automatizar a análise de documentos técnicos, identificar lacunas regulatórias e sugerir recomendações personalizadas. Este sistema permitiu aumentar a eficiência e a consistência dos processos de auditoria, mesmo em contextos onde o conhecimento especializado em cibersegurança pode ser limitado.

Relativamente à questão de investigação formulada, os resultados obtidos permitem concluir que a aplicação de LLMs melhora de forma significativa a eficiência e a consistência das auditorias internas de cibersegurança em instituições do setor financeiro, particularmente nos domínios da gestão de fornecedores externos e do controlo de acessos. A automatização da análise documental reduziu o esforço manual e o tempo de avaliação, assegurando simultaneamente uma aplicação uniforme dos critérios da Diretiva NIS 2 a documentos distintos. Adicionalmente, a utilização de *prompts* especializados e regras normativas explícitas contribuiu para avaliações mais homogéneas e reproduzíveis, mitigando a subjetividade inerente às auditorias tradicionais e reforçando a capacidade das instituições em identificar lacunas críticas de conformidade e priorizar ações corretivas.

Os resultados obtidos mostram que a integração de IA na gestão de riscos cibernéticos representa um avanço significativo para instituições financeiras, contribuindo para uma postura mais proativa e alinhada com os regulamentos europeus emergentes. A ferramenta criada revelou-se particularmente útil na análise de cláusulas contratuais, políticas de acesso e medidas de segurança aplicadas a terceiros, domínios muitas vezes negligenciados nas abordagens tradicionais.

Para além do contributo prático, este trabalho evidencia a relevância de uma arquitetura flexível e modular, preparada para evoluir com a rápida transformação dos modelos de IA. A capacidade de configuração dos LLMs, a utilização de *system prompts* e a possibilidade de integração com regras internas organizacionais reforçam não só a solidez técnica da solução, mas também a sua viabilidade comercial e aplicabilidade em diferentes contextos regulatórios.

Do ponto de vista científico, esta investigação contribui para a literatura emergente, ao explorar como os LLMs podem ser aplicados de forma estruturada à conformidade regulatória e à gestão de riscos de cibersegurança. Através da metodologia de investigação adotada, Design Science Research Methodology (DSRM), foi possível conceber, implementar e validar um artefacto tecnológico que responde a um problema prático relevante, enquanto abre caminho para futuras linhas de investigação.

Os resultados apresentados nesta dissertação foram posteriormente consolidados e validados através da elaboração e submissão do artigo *"NIS 2 Insight: An AI-Based Approach for Automating Regulatory Compliance Assessment in the Financial Sector"*. Este trabalho permitiu enquadrar a solução proposta num contexto académico mais alargado, reforçando a validade externa dos resultados obtidos e evidenciando a aplicabilidade prática da utilização de LLMs na automatização da avaliação de conformidade regulatória no setor financeiro. A publicação do artigo constitui, assim, um indicador adicional da relevância científica do artefacto desenvolvido e da sua contribuição para o domínio emergente da RegTech aplicada à cibersegurança.

Contudo, reconhece-se que o protótipo apresenta algumas limitações, como a dependência de instruções claras nos documentos analisados e a necessidade de revisão humana em situações ambíguas ou juridicamente complexas. Ainda assim, o projeto demonstrou o potencial da IA como aliada estratégica na cibersegurança, abrindo espaço para novas abordagens de automação e monitorização contínua em ambientes regulados.

Conclui-se, assim, que a aplicação de ferramentas de IA pode contribuir de forma decisiva para a evolução dos modelos de conformidade no setor financeiro, tornando os processos mais ágeis, transparentes e eficazes. A solução desenvolvida constitui um contributo relevante para o reforço da resiliência digital das instituições financeiras, enquanto abre novas oportunidades para investigações futuras e para a integração desta tecnologia em ecossistemas empresariais reais.

5.1. Limitações do Sistema

Apesar da plataforma NIS 2 Insight ter sido desenvolvida para automatizar a avaliação de conformidade com a Diretiva NIS 2 e apresentar um desempenho robusto em diversos cenários, o sistema apresenta algumas limitações que podem impactar a sua aplicação em determinados contextos ou com documentos que não se ajustem completamente ao formato esperado.

O sistema foi projetado para funcionar com documentos em formato PDF que apresentem uma estrutura bem definida (por exemplo, listas numeradas, subtítulos, etc.). No entanto, documentos mal estruturados ou com formatação inconsistente podem dificultar a extração precisa de texto utilizando a biblioteca pdfjs-dist. Isso pode resultar em perda de dados importantes ou erros na interpretação do conteúdo. Embora o sistema utilize um mecanismo de *fallback* semântico para lidar com essa situação, a qualidade do texto extraído é um fator determinante para a precisão da análise.

A escolha do modelo LLaMA 3 70B da Groq é um dos principais pontos fortes do sistema devido à sua capacidade de processar grandes volumes de texto e gerar respostas relevantes. No entanto, o modelo também apresenta algumas limitações:

- Contexto limitado: O LLaMA 3 70B possui um limite de *tokens* (palavras ou pedaços de palavras) que pode processar de cada vez. Embora esse limite seja suficientemente alto para a maioria dos documentos, documentos muito longos ou com estruturas complexas podem ultrapassar esse limite, comprometendo a qualidade da resposta.
- Treinamento específico: O modelo pode não ter sido treinado especificamente para lidar com todos os termos técnicos ou jargões usados em documentos jurídicos e regulatórios, o que pode resultar numa interpretação incorreta de certos critérios ou falta de precisão na análise.

Atualmente, o sistema está focado apenas na conformidade com a Diretiva NIS 2, o que limita sua aplicabilidade a outros tipos de normativas ou *frameworks* regulatórios. Embora seja possível realizar ajustes ao modelo para aplicar outras normas, a personalização de todo o sistema (incluindo as palavras-chave, a heurística e os critérios de conformidade) exigiria um esforço significativo de reprogramação. Este aspeto restringe a escalabilidade do sistema a outros domínios regulatórios.

A aplicação depende de conectividade estável à API da Groq para processamento da análise, o que significa que a sua performance está limitada pela qualidade da ligação à internet e pela disponibilidade do serviço. Em cenários de conexão lenta ou interrupções temporárias no serviço da Groq, o sistema pode apresentar atrasos na análise ou até falhar ao tentar processar o documento.

Relativamente à interface da aplicação, embora tenha sido projetada para ser simples e intuitiva, a experiência do utilizador pode ser prejudicada em ambientes com recursos limitados, como dispositivos móveis com pouca capacidade de processamento ou conexões lentas à internet. A visualização de grandes conjuntos de dados, como gráficos complexos e

listas de conformidade, pode ser demorada ou dificultar a interatividade. Além disso, a plataforma não oferece atualmente suporte a personalizações extensivas na interface (por exemplo, a escolha de temas ou a modificação de gráficos), o que limita a flexibilidade para diferentes utilizadores.

5.2. Trabalhos Futuros

Apesar dos objetivos desta dissertação terem sido atingidos de forma satisfatória, é importante reconhecer que o protótipo desenvolvido representa apenas um primeiro passo de um percurso mais vasto, com grande potencial de aprofundamento e consolidação. Os trabalhos futuros poderão seguir várias direções complementares, todas elas convergindo para o fortalecimento da plataforma e para a sua maturidade como solução prática de apoio à conformidade regulatória e à cibersegurança no setor financeiro.

Um dos primeiros passos recomendados passa pela validação do protótipo em contextos reais, aplicando-o a documentos provenientes de diferentes instituições financeiras. Esta validação permitirá aferir a robustez do sistema perante estilos de escrita variados, diferentes níveis de complexidade jurídica e múltiplos formatos de ficheiros, incluindo PDFs digitalizados ou sujeitos a reconhecimento ótico de caracteres. Mais do que uma mera prova técnica, esta etapa será fundamental para compreender como a ferramenta se comporta em cenários reais de auditoria e *compliance*, onde a heterogeneidade dos documentos é a norma e não a exceção. Paralelamente, a aplicação em contexto real proporcionará a recolha de feedback de utilizadores técnicos, como equipas de cibersegurança e TI, e de utilizadores não técnicos, como profissionais de *compliance* e auditoria, permitindo refinar a usabilidade, a clareza das recomendações e o valor prático dos relatórios produzidos.

Outro vetor de evolução prende-se com a explicabilidade das decisões do sistema. Embora o protótipo já ofereça justificações textuais e excertos de evidência, existe um espaço considerável para aprofundar a adoção de técnicas de XAI. Futuros desenvolvimentos poderão incorporar modelos visuais que destaquem trechos específicos do documento que suportaram cada classificação, representações probabilísticas que expressem o grau de confiança associado a cada decisão e explicações contrastivas, que ajudem o utilizador a perceber não apenas porque um critério foi classificado como conforme, mas também porque não foi considerado não conforme. Este reforço da explicabilidade será determinante para aumentar a confiança dos utilizadores e alinhar a plataforma com os requisitos emergentes do AI Act, que impõe padrões rigorosos de transparência e auditabilidade para sistemas de IA em contextos de elevado risco.

A dimensão multilingue constitui igualmente um caminho promissor. Dado o carácter global do setor financeiro e a crescente interdependência das cadeias de fornecimento internacionais, torna-se essencial que a plataforma seja capaz de analisar documentos em vários idiomas, como inglês, espanhol, francês ou alemão. Esta capacidade ampliará a aplicabilidade da ferramenta em grupos financeiros multinacionais, permitindo avaliar a conformidade regulatória em diferentes jurisdições e contextos organizacionais.

Do ponto de vista funcional, uma das áreas com maior potencial de evolução é a integração nativa com plataformas de Governance, Risk and Compliance (GRC). Ao permitir que os relatórios e recomendações da NIS 2 Insight sejam exportados ou diretamente integrados em *dashboards* corporativos de GRC, será possível aumentar a utilidade da solução para equipas de *compliance* e auditoria, automatizando fluxos de trabalho e reduzindo redundâncias. Esta integração contribuirá para que a plataforma deixe de ser uma ferramenta isolada e passe a desempenhar um papel ativo no ecossistema tecnológico das instituições financeiras.

Também o alargamento do âmbito funcional da ferramenta é um caminho incontornável. Embora esta dissertação tenha focado a análise de políticas de fornecedores e de controlo de acessos, é inegável que o setor financeiro exige uma cobertura muito mais vasta. Futuros desenvolvimentos deverão incluir a capacidade de avaliar políticas de gestão de incidentes e resposta a crises, planos de continuidade de negócio e de recuperação em caso de desastre, contratos de outsourcing e Service Level Agreements (SLAs), políticas de criptografia e gestão de chaves, relatórios de auditoria interna e externa e até planos de formação e sensibilização em cibersegurança. Ao abranger este conjunto mais alargado de documentos, a plataforma poderá posicionar-se como uma solução transversal de análise documental, apoiando auditorias integradas e avaliações globais de conformidade.

Mais ambiciosamente, a ferramenta poderá expandir-se para áreas complementares de grande relevância, como a deteção de fraudes financeiras, recorrendo à análise de padrões anómalos em relatórios e transações; a gestão de identidades e acessos privilegiados (IAM/PAM), verificando políticas ligadas à segregação de funções e à utilização de contas críticas; e a análise de risco comportamental de fornecedores e colaboradores, cruzando documentos contratuais com métricas de reputação, histórico de incidentes e indicadores de risco humano. Estas áreas representam pontos de vulnerabilidade reconhecidos no setor e a sua integração numa única plataforma traria ganhos significativos em termos de visibilidade, proatividade e resiliência.

Outro aspeto crítico para a evolução tecnológica da solução será a migração para modelos privados e auto-hospedados (*self-hosted*). A atual dependência de APIs públicas de

fornecedores externos de LLMs, como Groq ou OpenAI, implica riscos significativos ao nível da confidencialidade dos dados e da soberania digital. Ao adotar modelos de linguagem abertos e privados, como LLaMA, Falcon ou Mistral, executados em infraestruturas próprias ou em *clouds* soberanas, será possível garantir que os documentos sensíveis permaneçam sob total controlo da instituição. Além disso, a utilização de modelos privados permite realizar *fine-tuning,* que consiste em ajustar um modelo de Inteligência Artificial previamente treinado para que ele seja mais preciso e relevante em tarefas específicas, com base em dados do setor financeiro europeu e em normativos como a NIS 2, o DORA ou a ISO/IEC 27001, aumentando a precisão e a relevância das análises.

Finalmente, será igualmente relevante expandir o enquadramento regulatório da plataforma. Embora esta dissertação se tenha centrado na Diretiva NIS 2, é previsível que instituições financeiras necessitem de demonstrar conformidade com múltiplos quadros normativos em simultâneo. Assim, futuros trabalhos deverão considerar a integração com o Digital Operational Resilience Act (DORA), que impõe requisitos específicos de resiliência operacional digital; com o AI Act, que estabelece critérios de classificação, explicabilidade e mitigação de enviesamentos; e com regulamentos nacionais e setoriais específicos. Este alargamento permitirá que a plataforma funcione como uma solução multi-normativa, adaptável a diferentes contextos legais e organizacionais, e capaz de apoiar as instituições na sua jornada de transformação digital segura e sustentável.

Em síntese, os trabalhos futuros apontam para a consolidação da NIS 2 Insight como uma plataforma robusta, escalável e adaptável, capaz de evoluir de protótipo académico para solução prática de referência no setor financeiro europeu. A ferramenta foi validada em contextos reais e está enriquecida com explicabilidade avançada, funcionalidades multilingues, integração com plataformas GRC e expansão para novos domínios da cibersegurança. Adicionalmente, é apoiada por modelos de linguagem privados e soberanos e está alinhada com múltiplos quadros normativos, podendo constituir um contributo duradouro para o reforço da resiliência digital e para a construção de ecossistemas financeiros mais confiáveis e preparados para os desafios do futuro.

Referências Bibliográficas

[1] O. O. Otuu and F. C. Aguboshim, “Exploring the Role of Financial Cybersecurity Risk Management in Enhancing the Performance of Banking Payment Systems in Nigeria: A Qualitative Case Study,” in *2023 IEEE International Humanitarian Technology Conference, IHTC 2023*, Institute of Electrical and Electronics Engineers Inc., 2023. doi: 10.1109/IHTC58960.2023.10508850.

[2] L. Jelovčan, A. Mihelič, and K. Prislan, “Outsource or not? An AHP Based Decision Model for Information Security Management,” *Organizacija*, vol. 55, no. 2, pp. 142–159, May 2022, doi: 10.2478/orga-2022-0010.

[3] A. Mishra, Y. I. Alzoubi, M. J. Anwar, and A. Q. Gill, “Attributes impacting cybersecurity policy development: An evidence from seven nations,” *Comput Secur*, vol. 120, Sep. 2022, doi: 10.1016/j.cose.2022.102820.

[4] E. Aghaei, E. Al-Shaer, X. Niu, and W. Shadid, “SecureBERT: A Domain-Specific Language Model for Cybersecurity.” [Online]. Available: https://github.com/ehsanaghaei/SecureBERT

[5] M. C. Ghanem, T. M. Chen, M. A. Ferrag, and M. E. Kettouche, “ESASCF: Expertise Extraction, Generalization and Reply Framework for Optimized Automation of Network Security Compliance,” *IEEE Access*, vol. 11, pp. 129840–129853, 2023, doi: 10.1109/ACCESS.2023.3332834.

[6] O. Amaral, S. Abualhaija, D. Torre, M. Sabetzadeh, and L. C. Briand, "AI-enabled automation for completeness checking of privacy policies," IEEE Transactions on Software Engineering, vol. 48, no. 11, pp. 4647–4674, 2022, doi: 10.1109/TSE.2021.3124332.

[7] S. Goodwin, “The need for a financial sector legal standard to support the NIST Cybersecurity Framework,” in *Conference Proceedings - IEEE SOUTHEASTCON*, Institute of Electrical and Electronics Engineers Inc., 2022, pp. 89–95. doi: 10.1109/SoutheastCon48659.2022.9764006.

[8] J. Angle e T. Health, “Third-Party Vendor Risk Management 2”, Cloud Security Alliance, Jul. 2022. [Online]. Available: https://cloudsecurityalliance.org/artifacts/third-party-vendor-risk-management

[9] S. Kühnel, S. Sackmann, S. Trang, I. Nastjuk, T. Matschak, L. Niedzela e L. Nake, “Towards a business process-based economic evaluation and selection of IT security measures,” in “Proc. First International Workshop on Current Compliance Issues in Information Systems Research (CIISR’21)”, co-located with “16th International Conference on Wirtschaftsinformatik (WI’21)”, Essen, Germany, Mar. 2021, pp. 7–21, CEUR Workshop Proceedings, vol. 2966. [Online]. Available: https://ceur-ws.org/Vol-2966/

[10] D. Itani, R. Itani, A. A. Eltweri, A. Faccia, and L. Wanganoo, “Enhancing Cybersecurity Through Compliance and Auditing: A Strategic Approach to Resilience,” in *2nd International Conference on Cyber Resilience, ICCR 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ICCR61006.2024.10532959.

[11] M. Khamis, J. Zaytoun, M. Mahmoud, and S. Elhoushy, “The Impact of Financial Technology on Auditing Profession: An Analytical Perspective,” *Online) International Journal of Management, Accounting and Economics*, vol. 11, no. 2, pp. 2383–2126, 2024, doi: 10.5281/zenodo.10892766.

[12] B. Ramos-Cruz, J. Andreu-Perez, and L. Martínez, “The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic

protocols and challenges for future research," May 07, 2024, *Elsevier B.V.* doi: 10.1016/j.neucom.2024.127427.

[13] A. Awadallah *et al.*, "Artificial Intelligence-Based Cybersecurity for the Metaverse: Research Challenges and Opportunities," *IEEE Communications Surveys and Tutorials*, 2024, doi: 10.1109/COMST.2024.3442475.

[14] S. Romanosky, L. Ablon, A. Kuehn, and T. Jones, "Content analysis of cyber insurance policies: How do carriers price cyber risk?," *J Cybersecur*, vol. 5, no. 1, Jan. 2019, doi: 10.1093/cybsec/tyz002.

[15] F. Cremer *et al.*, "Cyber risk and cybersecurity: a systematic review of data availability," *Geneva Papers on Risk and Insurance: Issues and Practice*, vol. 47, no. 3, pp. 698–736, Jul. 2022, doi: 10.1057/s41288-022-00266-6.

[16] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of Management Information Systems*, vol. 24, no. 3, pp. 45–77, Dec. 2007, doi: 10.2753/MIS0742-1222240302.

[17] S. Onimisi Dawodu, A. Omotosho, O. Josephine Akindote, A. Oluwatoyin Adegbite, S. Kuzankah Ewuga, and C. Author, "Cybersecurity Risk Assessment in Banking: Methodologies and Best Practices," *Computer Science & IT Research Journal*, vol. 4, no. 3, pp. 220–243, 2023, doi: 10.51594/csitrj.v659.

[18] N. Kshetri and J. Voas, "Banking on availability," *Computer (Long Beach Calif)*, vol. 50, no. 1, pp. 76–80, Jan. 2017, doi: 10.1109/MC.2017.22.

[19] Temitayo Oluwaseun Abrahams, Oluwatoyin Ajoke Farayola, Simon Kaggwa, Prisca Ugomma Uwaoma, Azeez Olanipekun Hassan, and Samuel Onimisi Dawodu, "Reviewing Third-Party Risk Management: Best Practices in Accounting and Cybersecurity for Superannuation Organizations," *Finance & Accounting Research Journal*, vol. 6, no. 1, pp. 21–39, Jan. 2024, doi: 10.51594/farj.v6i1.706.

[20] S. Jawhar, J. Miller, and Z. Bitar, "AI-Based Cybersecurity Policies and Procedures," in *2024 IEEE 3rd International Conference on AI in Cybersecurity, ICAIC 2024*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ICAIC60265.2024.10433845.

[21] M. Benyahya, A. Collen, and N. A. Nijdam, "Cybersecurity and Data Privacy Certification Gaps of Connected and Automated Vehicles," in *Transportation Research Procedia*, Elsevier B.V., 2023, pp. 783–790. doi: 10.1016/j.trpro.2023.11.468.

[22] T. West and A. Zentner, "Threats and Major Data Breaches: Securing Third-Party Vendors," *SSRN Electronic Journal*, Mar. 2020, doi: 10.2139/ssrn.3532024.

[23] D. Patil, N. L. Rane, and J. Rane, "Enhancing resilience in various business sectors with ChatGPT and generative artificial intelligence," in *The Future Impact of ChatGPT on Several Business Sectors*, Deep Science Publishing, 2024. doi: 10.70593/978-81-981367-8-7_4.

[24] D. Javaheri, M. Fahmideh, H. Chizari, P. Lalbakhsh, and J. Hur, "Cybersecurity threats in FinTech: A systematic review," May 01, 2024, *Elsevier Ltd*. doi: 10.1016/j.eswa.2023.122697.

[25] Centro Nacional de Cibersegurança, "Quadro Nacional de Referência para a Cibersegurança (QNRCS)", Versão 1.0, Jun. 2019. [Online]. Available: https://www.cncs.gov.pt/docs/cncs-qnrcs-2019.pdf

[26] J. P. A. Yaacoub, H. N. Noura, O. Salman, and A. Chehab, "Ethical hacking for IoT: Security issues, challenges, solutions and recommendations," *Internet of Things and Cyber-Physical Systems*, vol. 3, pp. 280–308, Jan. 2023, doi: 10.1016/j.iotcps.2023.04.002.

[27] M. Mahabub Alam and S. Reza Anan, “The Human Element in Cybersecurity-Bridging the Gap Between Technology and Human Behaviour.” [Online]. Available: https://www.researchgate.net/publication/380270220
[28] K. Aruna Kumari and V. Naga Lakshmi, “A Survey on Third Party Auditor in Cloud Computing,” in *Proceedings - International Conference on Artificial Intelligence and Smart Systems, ICAIS 2021*, Institute of Electrical and Electronics Engineers Inc., Mar. 2021, pp. 1116–1121. doi: 10.1109/ICAIS50930.2021.9395972.
[29] S. S. Pericherla, “Cloud Computing Threats, Vulnerabilities and Countermeasures: A State-of-the-Art,” vol. 15, no. 1, pp. 1–58, 2023, doi: 10.22042/ISECURE.2022.
[30] T. Ali, M. Al-Khalidi, and R. Al-Zaidi, “Information Security Risk Assessment Methods in Cloud Computing: Comprehensive Review,” 2024, *Taylor and Francis Ltd.* doi: 10.1080/08874417.2024.2329985.
[31] S. P. Otta, S. Panda, M. Gupta, and C. Hota, “A Systematic Survey of Multi-Factor Authentication for Cloud Infrastructure,” *Future Internet*, vol. 15, no. 4, Apr. 2023, doi: 10.3390/fi15040146.
[32] M. Dawood, S. Tu, C. Xiao, H. Alasmary, M. Waqas, and S. U. Rehman, “Cyberattacks and Security of Cloud Computing: A Complete Guideline,” *Symmetry (Basel)*, vol. 15, no. 11, Nov. 2023, doi: 10.3390/sym15111981.
[33] S. Y. Mahmud, K. V. English, S. Thorn, W. Enck, A. Oest, and M. Saad, “Analysis of Payment Service Provider SDKs in Android,” in *ACM International Conference Proceeding Series*, Association for Computing Machinery, Dec. 2022, pp. 576–590. doi: 10.1145/3564625.3564641.
[34] S. A. Frimpong *et al.*, “RecGuard: An efficient privacy preservation blockchain-based system for online social network users,” *Blockchain: Research and Applications*, vol. 4, no. 1, Mar. 2023, doi: 10.1016/j.bcra.2022.100111.
[35] E. D. Canedo *et al.*, “ICT Governance and Management Macroprocesses of a Brazilian Federal Government Agency,” *Information (Switzerland)*, vol. 13, no. 5, May 2022, doi: 10.3390/info13050231.
[36] [6] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148 (NIS 2 Directive), OJ L 333, 27.12.2022, p. 80. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022L2555
[37] “IMPLEMENTING GUIDANCE.” [Online]. Available: www.enisa.europa.eu.
[38] M. D. M. Negreiro, “The NIS2 Directive: A high common level of cybersecurity in the EU,” EU Legislation in Progress, European Parliamentary Research Service (EPRS), Briefing EPRS_BRI(2021)689333, 08-Feb-2023. [Online]. Available: https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI(2021)689333
[39] M. Papaphilippou, “Good Practices for Supply Chain Cybersecurity,” ENISA, Jun. 2023. doi: 10.2824/805268.
[40] M. Veigurs, T. Lasmanis, and A. Romanovs, “IT Governance in Critical Sectors: Towards the NIS2 Implementation,” in *ITMS - International Scientific Conference on Information Technology and Management Science of Riga Technical University*, Institute of Electrical and Electronics Engineers Inc., 2024. doi: 10.1109/ITMS64072.2024.10741938.
[41] E. B. Laidlaw, C. Research Chair, and C. Law, “Privacy and Cybersecurity in Digital Trade: The Challenge of Cross border Data Flows A paper prepared for Global Affairs Canada*,” 2021. [Online]. Available: https://ssrn.com/abstract=3790936

[42] B. Ramos-Cruz, J. Andreu-Perez, and L. Martínez, “The cybersecurity mesh: A comprehensive survey of involved artificial intelligence methods, cryptographic protocols and challenges for future research,” May 07, 2024, *Elsevier B.V.* doi: 10.1016/j.neucom.2024.127427.

[43] M. Elliot, A. M. Mandalari, M. Mourby e K. O’Hara, *Dictionary of Privacy, Data Protection and Information Security*, Cheltenham, UK / Northampton, MA, USA: Edward Elgar Publishing, Jul. 2024, ISBN 978-1-03530-0921-X. doi:10.4337/9781035300921.

[44] P. H. Nguyen, T. V. Pham, L. A. T. Nguyen, H. A. T. Pham, T. H. T. Nguyen, and T. G. Vu, “Assessing cybersecurity risks and prioritizing top strategies In Vietnam’s finance and banking system using strategic decision-making models-based neutrosophic sets and Z number,” *Heliyon*, vol. 10, no. 19, Oct. 2024, doi: 10.1016/j.heliyon.2024.e37893.

[45] M. A. Hassan and Z. Shukur, “A Systematic Review of User Authentication Security in Electronic Payment System,” in *Lecture Notes in Networks and Systems*, vol. 551, Springer Science and Business Media Deutschland GmbH, 2023, pp. 121–138. doi: 10.1007/978-981-19-6631-6_10.

[46] K. Zheng *et al.*, “Blockchain technology for enterprise credit information sharing in supply chain finance,” *Journal of Innovation and Knowledge*, vol. 7, no. 4, Oct. 2022, doi: 10.1016/j.jik.2022.100256.

[47] M. Houichi, F. Jaidi, and A. Bouhoula, “A comprehensive and in-depth study of the threats faced by smart cities and the countermeasures implemented in their key areas,” *Journal of Infrastructure, Policy and Development*, vol. 8, no. 10, 2024, doi: 10.24294/jipd.v8i10.8629.

[48] A. Jahin, S. Akram Naife, A. Kumar Saha, and M. F. Mridha, “AI in Supply Chain Risk Assessment: A Systematic Literature Review and Bibliometric Analysis,” 2025.

[49] C. Cintia Coelho Dias and R. Valiatti Ferreira, “O uso da inteligência artificial na atividade de compliance: riscos e benefícios,” *Revista Científica do CPJM*, pp. 219–245, 2023, doi: 10.55689/rcpjm.2023.08.011.

[50] R. F. Olanrewaju, B. U. I. Khan, M. A. Morshidi, F. Anwar, and M. L. B. M. Kiah, “A Frictionless and Secure User Authentication in Web-Based Premium Applications,” *IEEE Access*, vol. 9, pp. 129240–129255, 2021, doi: 10.1109/ACCESS.2021.3110310.

[51] U. Narayanan, N. P. Veettil, R. T. Krishnankutty, L. E. Sunny, and V. Paul, “Mitigating Privacy and Security Risks in the Era of Big Data: A Comprehensive Framework of Best Practices and Protocols,” *Journal of Computer Science*, vol. 20, no. 9, pp. 1121–1145, 2024, doi: 10.3844/JCSSP.2024.1121.1145.

[52] R. Odarchenko, M. Iavich, G. Iashvili, S. Fedushko, and Y. Syerov, “Assessment of Security KPIs for 5G Network Slices for Special Groups of Subscribers,” *Big Data and Cognitive Computing*, vol. 7, no. 4, Dec. 2023, doi: 10.3390/bdcc7040169.

[53] F. Z. M. Irzam and H. Taherdoost, “Cybersecurity KPIs in Higher Institutions: A Systematic Review,” in *Proceedings - 2024 International Conference on Expert Clouds and Applications, ICOECA 2024*, Institute of Electrical and Electronics Engineers Inc., 2024, pp. 276–287. doi: 10.1109/ICOECA62351.2024.00058.

[54] P. Hacker, "AI Regulation in Europe: From the AI Act to Future Regulatory Challenges," preprint, arXiv:2310.04072 [cs.CY], Oct. 2023. [Online]. Available: https://doi.org/10.48550/arXiv.2310.04072

[55] A. Modi, “Data Driven Approaches to Cybersecurity Governance for Board Decision-Making-A Systematic Review.” [Online]. Available: https://www.researchgate.net/publication/371383107

[56] J. C. Westland, “Predicting credit card fraud with Sarbanes-Oxley assessments and Fama-French risk factors,” *Intelligent Systems in Accounting, Finance and Management*, vol. 27, no. 2, pp. 95–107, Apr. 2020, doi: 10.1002/isaf.1472.
[57] J. R. Gudeme, S. Pasupuleti, and R. Kandukuri, “Certificateless privacy preserving public auditing for dynamic shared data with group user revocation in cloud storage,” *J Parallel Distrib Comput*, vol. 156, pp. 163–175, Oct. 2021, doi: 10.1016/j.jpdc.2021.06.001.
[58] J. Kokina and T. H. Davenport, “The emergence of artificial intelligence: How automation is changing auditing,” *Journal of Emerging Technologies in Accounting*, vol. 14, no. 1, pp. 115–122, Mar. 2017, doi: 10.2308/jeta-51730.
[59] S. Dambe, “The Role of Artificial Intelligence in Enhancing Cybersecurity and Internal Audit,” in *2023 3rd International Conference on Advancement in Electronics and Communication Engineering, AECE 2023*, Institute of Electrical and Electronics Engineers Inc., 2023, pp. 88–93. doi: 10.1109/AECE59614.2023.10428353.
[60] M. Tetaly and P. Kulkarni, “Artificial intelligence in cyber security - A threat or a solution,” in *AIP Conference Proceedings*, American Institute of Physics Inc., Oct. 2022. doi: 10.1063/5.0109664.
[61] M. F. Ansari, B. Dash, P. Sharma, and N. Yathiraju, “The Impact and Limitations of Artificial Intelligence in Cybersecurity: A Literature Review,” *IJARCCE*, vol. 11, no. 9, Sep. 2022, doi: 10.17148/ijarcce.2022.11912.
[62] J. Brás, R. Pereira, and S. Moro, “Intelligent Process Automation and Business Continuity: Areas for Future Research,” Feb. 01, 2023, *MDPI*. doi: 10.3390/info14020122.

Anexos

Anexo A - Relatório de análise à Política de Gestão de Acessos" do Banco Económico

Relatório de Conformidade NIS 2

Data: 15/09/2025
Tipo de Política: Política de Controlo de Acessos
Conformidade: 60%

Critérios NIS2:

✔ Conforme — Política de controlo de acessos (Severidade: Baixa)
Justificação: O documento descreve uma política de gestão de acessos que inclui o controlo de acessos a redes e sistemas de informação.
Evidência: "Política de Gestão de Acessos"
Ações imediatas:
- Verificar se a política de controlo de acessos está implementada e atualizada. Garantir que os colaboradores e partes interessadas estejam cientes da política e procedimentos de controlo de acessos.

Próximos passos:
- Monitorar a conformidade com a política de controlo de acessos.

Informação insuficiente — Referência ao uso de MFA

✔ Conforme — Revisão periódica de privilégios (Severidade: Baixa)
Justificação: O documento menciona a revisão periódica de privilégios como um princípio geral para a gestão de acessos.
Evidência: "Rever periodicamente quais os utilizadores existentes, as suas permissões e os privilégios atribuídos"
Ações imediatas:
- Verificar se a revisão periódica de privilégios está implementada e atualizada. Garantir que os colaboradores e partes interessadas estejam cientes da política e procedimentos de revisão de privilégios.

Próximos passos:
- Monitorar a conformidade com a política de revisão de privilégios.

✔ Conforme — Conformidade com ISO 27001 (Severidade: Baixa)
Justificação: O documento menciona a conformidade com a norma ISO 27001 como um dos objetivos da política de gestão de acessos.
Evidência: "ISO/IEC 27001:2022 – Sistemas de Gestão de Segurança da Informação (Requisitos)"
Ações imediatas:
- Verificar se a conformidade com a norma ISO 27001 está implementada e atualizada. Garantir que os colaboradores e partes interessadas estejam cientes da política e

procedimentos de conformidade com a norma ISO 27001.

Próximos passos:

- Monitorar a conformidade com a norma ISO 27001.

Não conforme — Conformidade com RGPD (Severidade: Alta)
Justificação: O documento não menciona explicitamente a conformidade com o Regulamento Geral de Proteção de Dados (RGPD).
Evidência: "Não há evidência de uma referência à conformidade com o RGPD no documento."
Ações imediatas:

- Desenvolver uma política de proteção de dados que inclua procedimentos para a conformidade com o RGPD. Implementar a política de proteção de dados.

Próximos passos:

- Monitorar a implementação e conformidade com a política de proteção de dados.
  Recomendações: Desenvolver uma política de avaliação de fornecedores que inclua critérios de segurança e conformidade. Implementar a autenticação MFA para os acessos a sistemas e redes. Desenvolver uma política de notificação de incidentes que inclua procedimentos para a notificação e resposta a incidentes de segurança. Desenvolver uma política de proteção de dados que inclua procedimentos para a conformidade com o RGPD. Monitorar a implementação e conformidade com as políticas e procedimentos de segurança e proteção de dados.

Recomendações:

- Desenvolver uma política de avaliação de fornecedores que inclua critérios de segurança e conformidade.
- Implementar a autenticação MFA para os acessos a sistemas e redes.
- Desenvolver uma política de notificação de incidentes que inclua procedimentos para a notificação e resposta a incidentes de segurança.
- Desenvolver uma política de proteção de dados que inclua procedimentos para a conformidade com o RGPD.
- Monitorar a implementação e conformidade com as políticas e procedimentos de segurança e proteção de dados.

Anexo B - Política de Fornecedores do Banco BPI

Relatório de Conformidade NIS 2

Data: 22/10/2025
Tipo de Política: Política de Fornecedores
Conformidade: 80%

Critérios NIS2:

✔ Conforme — Política de avaliação de fornecedores (Severidade: Alta)
Justificação: O documento apresenta um Código de Conduta de Fornecedores que estabelece princípios e orientações específicas para a avaliação e seleção de fornecedores.
Evidência: "O BPI considera os seus Fornecedores uma peça essencial para a concretização dos seus objetivos de crescimento e de melhoria da qualidade de serviço, estabelecendo relações de confiança e alinhadas com os seus valores."
Ações imediatas:

- Revisar o Código de Conduta de Fornecedores para garantir que ele esteja alinhado com as necessidades do BPI. Estabelecer processos claros para a avaliação e seleção de fornecedores.

Próximos passos:

- Desenvolver um plano de ação para implementar o Código de Conduta de Fornecedores. Treinar os funcionários do BPI sobre o Código de Conduta de Fornecedores.

✔ Conforme — Cláusulas de confidencialidade e responsabilidade (Severidade: Alta)
Justificação: O documento menciona a importância da confidencialidade e da responsabilidade na relação entre o BPI e os seus fornecedores.
Evidência: "Os Fornecedores devem respeitar os direitos de propriedade intelectual e industrial pertencentes ao BPI."
Ações imediatas:

- Revisar os contratos com os fornecedores para garantir que eles incluam cláusulas de confidencialidade e responsabilidade. Estabelecer processos claros para a gestão de informações confidenciais.

Próximos passos:

- Desenvolver um plano de ação para implementar as cláusulas de confidencialidade e responsabilidade. Treinar os funcionários do BPI sobre a importância da confidencialidade e da responsabilidade.

✔ Conforme — Cláusulas sobre notificação de incidentes (Severidade: Alta)
Justificação: O documento menciona a importância da notificação de incidentes na relação entre o BPI e os seus fornecedores.
Evidência: "Os Fornecedores devem notificar o BPI de qualquer incidente que possa afetar a

segurança ou a confidencialidade das informações do BPI."
Ações imediatas:

- Revisar os contratos com os fornecedores para garantir que eles incluam cláusulas sobre notificação de incidentes. Estabelecer processos claros para a gestão de incidentes.

Próximos passos:

- Desenvolver um plano de ação para implementar as cláusulas sobre notificação de incidentes. Treinar os funcionários do BPI sobre a importância da notificação de incidentes.

Não conforme — Conformidade com ISO 27001 (Severidade: Média)
Justificação: O documento não menciona explicitamente a conformidade com a ISO 27001.
Evidência: "None"
Ações imediatas:

- Considerar a implementação de um sistema de gestão de segurança da informação conforme a ISO 27001. Estabelecer processos claros para a gestão de segurança da informação.

Próximos passos:

- Desenvolver um plano de ação para implementar a ISO 27001. Treinar os funcionários do BPI sobre a importância da conformidade com a ISO 27001.

✔ Conforme — Conformidade com RGPD (Severidade: Alta)
Justificação: O documento menciona a importância da proteção de dados pessoais e da conformidade com a regulamentação aplicável, incluindo o RGPD.
Evidência: "Os Fornecedores devem garantir a proteção dos dados pessoais e cumprir com a regulamentação aplicável, incluindo o RGPD."
Ações imediatas:

- Revisar os contratos com os fornecedores para garantir que eles incluam cláusulas sobre proteção de dados pessoais e conformidade com o RGPD. Estabelecer processos claros para a gestão de dados pessoais.

Próximos passos:

- Desenvolver um plano de ação para implementar as cláusulas sobre proteção de dados pessoais e conformidade com o RGPD. Treinar os funcionários do BPI sobre a importância da proteção de dados pessoais e da conformidade com o RGPD. Recomendações: Desenvolver uma política de segurança da informação que inclua a implementação de MFA e a revisão periódica de privilégios. Estabelecer processos claros para a gestão de incidentes e a notificação de incidentes. Considerar a implementação de um sistema de gestão de segurança da informação conforme a ISO 27001. Treinar os funcionários do BPI sobre a importância da proteção de dados pessoais, da conformidade com o RGPD e da segurança da informação.

Recomendações:

- Desenvolver uma política de segurança da informação que inclua a implementação de MFA e a revisão periódica de privilégios.
- Estabelecer processos claros para a gestão de incidentes e a notificação de incidentes.
- Considerar a implementação de um sistema de gestão de segurança da informação conforme a ISO 27001.
- Treinar os funcionários do BPI sobre a importância da proteção de dados pessoais, da conformidade com o RGPD e da segurança da informação.

Anexo C - Política de Fornecedores da Adea Information Intelligence

Relatório de Conformidade NIS 2

Data: 15/09/2025
Tipo de Política: Política de Fornecedores
Conformidade: 20%

Critérios NIS2:

✔ Conforme — Política de avaliação de fornecedores (Severidade: Baixa)
Justificação: O documento apresenta uma política de gestão de fornecedores que inclui a seleção, avaliação e acompanhamento dos fornecedores.
Evidência: "A Ade a realiza uma avaliação contínua dos fornecedores, estabelecendo um índice de qualidade que indica o grau de satisfação com cada fornecedor."
Ações imediatas:

- Implementar a política de avaliação de fornecedores Estabelecer critérios de avaliação claros e objetivos

Próximos passos:

- Monitorar e avaliar o desempenho dos fornecedores Ajustar a política de avaliação de fornecedores conforme necessário

Não conforme — Cláusulas de confidencialidade e responsabilidade (Severidade: Alta)
Justificação: O documento não apresenta cláusulas de confidencialidade e responsabilidade explícitas.
Evidência: "Nenhuma"
Ações imediatas:

- Incluir cláusulas de confidencialidade e responsabilidade nos contratos com fornecedores Estabelecer procedimentos para lidar com violações de confidencialidade e responsabilidade

Próximos passos:

- Revisar e atualizar os contratos com fornecedores para incluir as cláusulas de confidencialidade e responsabilidade

Não conforme — Cláusulas sobre notificação de incidentes (Severidade: Alta)
Justificação: O documento não apresenta cláusulas sobre notificação de incidentes explícitas.
Evidência: "Nenhuma"
Ações imediatas:

- Incluir cláusulas sobre notificação de incidentes nos contratos com fornecedores Estabelecer procedimentos para lidar com incidentes e notificações

Próximos passos:

- Revisar e atualizar os contratos com fornecedores para incluir as cláusulas sobre notificação de incidentes

Informação insuficiente — Conformidade com ISO 27001 (Severidade: Média)
Justificação: O documento não apresenta informações suficientes sobre a conformidade com ISO 27001.
Evidência: "Nenhuma"
Ações imediatas:

- Verificar a conformidade com ISO 27001 Implementar procedimentos para garantir a conformidade com ISO 27001

Próximos passos:

- Monitorar e avaliar o desempenho da conformidade com ISO 27001

Não conforme — Conformidade com RGPD (Severidade: Alta)
Justificação: O documento não apresenta informações suficientes sobre a conformidade com RGPD.
Evidência: "Nenhuma"
Ações imediatas:

- Verificar a conformidade com RGPD Implementar procedimentos para garantir a conformidade com RGPD

Próximos passos:

- Monitorar e avaliar o desempenho da conformidade com RGPD Recomendações: Incluir cláusulas de confidencialidade e responsabilidade nos contratos com fornecedores Implementar uma política de controlo de acessos Implementar o uso de MFA para acessos sensíveis Incluir cláusulas sobre notificação de incidentes nos contratos com fornecedores Verificar a conformidade com ISO 27001 e RGPD Implementar procedimentos para garantir a conformidade com ISO 27001 e RGPD

Recomendações:

- Incluir cláusulas de confidencialidade e responsabilidade nos contratos com fornecedores
- Implementar uma política de controlo de acessos
- Implementar o uso de MFA para acessos sensíveis
- Incluir cláusulas sobre notificação de incidentes nos contratos com fornecedores
- Verificar a conformidade com ISO 27001 e RGPD
- Implementar procedimentos para garantir a conformidade com ISO 27001 e RGPD