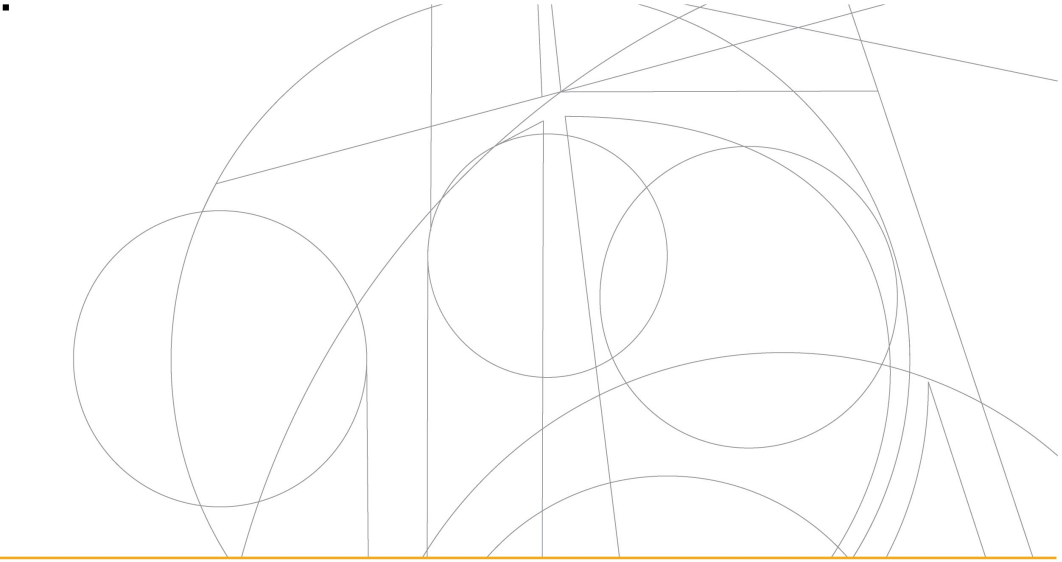

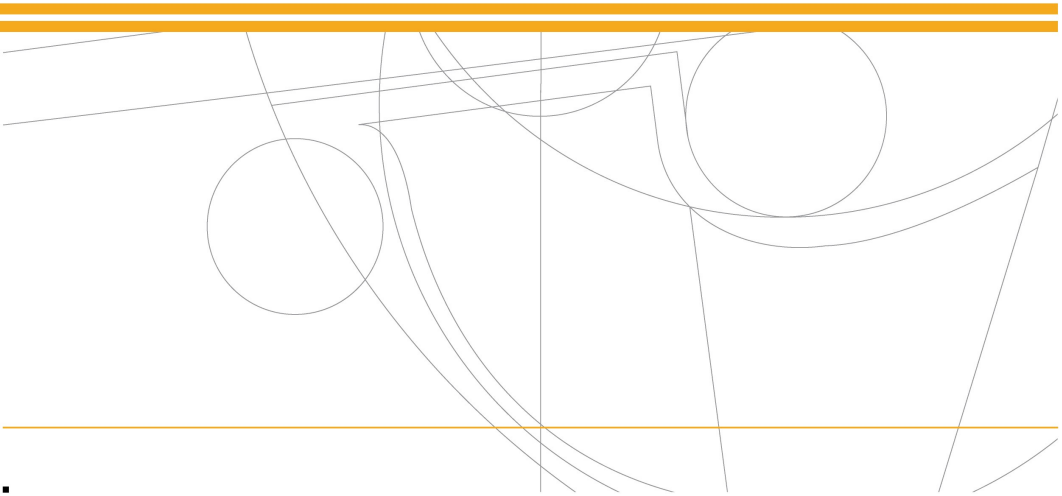

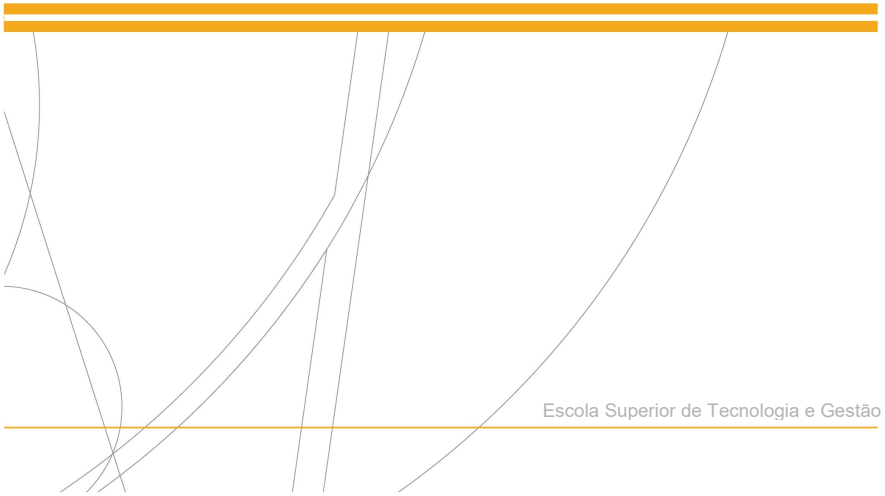

INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO

ESTG

Implementação do normativo DORA, integrado no modelo de governação em cibersegurança, numa Seguradora do Ramo Vida

Implementação do normativo DORA, integrado no modelo de governação em cibersegurança, numa Seguradora do Ramo Vida

Luis Filipe Figueiredo Lima

2025

INSTITUTO POLITÉCNICO
DE VIANA DO CASTELO

Escola Superior de Tecnologia e Gestão

Instituto Politécnico
de Viana do Castelo

Implementação do normativo DORA, integrado no modelo de governação em cibersegurança, numa Seguradora do Ramo Vida

Autor(a)

Luis Filipe Lima

Trabalho orientado por

Prof. Dr. Francisco Guimarães e Prof. Pedro Coutinho

Mestrado em Cibersegurança

30 de 05 de 2025

Mestrado em Cibersegurança
Master in Cybersecurity

Implementação do normativo DORA, integrado no modelo de governação em cibersegurança, numa Seguradora do Ramo Vida

a master's thesis authored by

Luis Filipe Lima

and supervised by

Pedro Coutinho
Professor Coordenador, IPVC

Francisco Santana Guimarães
Professor Auxiliar, ISCTE

This thesis was submitted in partial fulfilment of the requirements for the Master's degree in Cybersecurity at the Instituto Politécnico de Viana do Castelo

ipvc

31 of May, 2025

Abstract

The thesis deals with the implementation of the European standard called the Digital Operational Resilience Act (DORA), aligned with the European standard called the Network and Information Systems Directive 2 (NIS2), integrated into the information security management model in a life insurance company, as a way of managing information security risks and information and communication technology (ICT) risks.

DORA was approved by the European Union in 2022 and came into force in January 2023, with mandatory application in January 2025. This regulation is designed to increase the digital operational resilience of financial organisations, including insurance companies. To this end, it includes five main areas: ICT risk management; ICT incident management; digital operational resilience testing; third-party ICT risk management and cyber threat information sharing.

The thesis analyses the state of the art as the basis for a proposal to define a framework to relate information security risks and controls applied to ICT to asset categories, their vulnerabilities and threats. It thus addresses the challenges and opportunities in implementing DORA, so that insurers can fulfil the requirements of the regulation and thus improve their digital resilience, while taking a holistic view of information security for risk management.

The study demonstrated that the adoption of DORA not only enhances compliance and digital resilience but also promotes a strategic alignment between governance, technology, and operational risk management within the insurance sector.

Keywords: Insurance. DORA. Cybersecurity. Governance. NIS2. ISO 27002.

Resumo

A tese aborda a implementacão do normativo Europeu designado como Digital Operacional Resilience Act (DORA), alinhado com o normativo Europeu designado como Network and Information Systems Directive 2 (NIS2), integrados no modelo de gestão de segurança de informação numa seguradora do ramo vida, como forma de gerir os riscos de segurança de informação e riscos de tecnologias de informação de comunicação (TIC).

O DORA, foi aprovado pela União Europeia em 2022 e entrou em vigor em janeiro de 2023, sendo obrigatória a sua aplicação em janeiro de 2025. Este regulamento foi concebido para aumentar a resiliência operacional digital das entidades financeiras, incluindo as seguradoras. Para o efeito, inclui cinco domínios principais: gestão de riscos de TIC; gestão de incidentes de TIC; testes de resiliência operacional digital; gestão de riscos de TIC de terceiros e partilha de informação sobre ciberameaças.

A tese efetua uma análise de estado da arte como base para uma proposta de definição de uma framework que permita relacionar os riscos e controlos de segurança de informação aplicados às TIC face às categorias de ativos, suas vulnerabilidades e ameaças. Aborda-se assim os desafios e oportunidades na implementação do DORA, para que as seguradoras possam cumprir os requisitos do regulamento e como tal melhorar a sua resiliência digital, mas considerando uma visão holística de segurança de informação para gestão de risco.

O estudo realizado demonstrou que a adoção do DORA não apenas reforça a conformidade e a resiliência digital, mas também promove um alinhamento estratégico entre a governação, a tecnologia e a gestão de riscos operacionais no setor segurador.

Palavras-chave: Seguradora. DORA. Cibersegurança. Governação. NIS2. ISO 27002.

Agradecimentos

A conclusão desta tese representa não apenas o final de um ciclo académico, mas também o reflexo do apoio, incentivo e inspiração de várias pessoas que marcaram esta jornada.

Em primeiro lugar, agradeço aos meus orientadores, Professor Francisco Guimarães e Professor Pedro Coutinho, pela orientação científica rigorosa, pela disponibilidade constante e pelas valiosas contribuições que foram fundamentais para o desenvolvimento e aprofundamento deste trabalho. A vossa exigência, apoio e confiança foram decisivos ao longo de todo o percurso.

Aos meus amigos de jornadas académicas, Luís Pereira e Paulo Rocha, expresso a minha sincera gratidão pela amizade, pelo companheirismo e por todas as partilhas ao longo destes anos. O vosso apoio tornou esta caminhada mais rica e humana. Saúdo também a recente entrada de José Oliveira no grupo, cuja presença já acrescenta valor e dinamismo ao nosso trabalho.

Por fim, à minha família — Cristina, Marta e Margarida, o meu mais profundo agradecimento. São o meu alicerce, a minha fonte de motivação e o desafio constante que me impulsiona a procurar mais e melhor. O vosso amor, paciência e presença foram essenciais para que este projeto se concretizasse.

A todos, o meu muito obrigado.

Conteúdo

Lista de Figuras

Lista de Abreviaturas

API Application Programming Interface

ASF Autoridade de Supervisão de Seguros e Fundos de Pensões

CIS Center for Internet Security

CISOs Chief Information Security Officer

CNCS Centro Nacional de Cibersegurança

CRM Customer Relationship Management

CSIRT Computer Security Incident Response Team

DORA Digital Operational Resilience Act

EDR Endpoint Detection and Response

EIOPA European Insurance and Occupational Pensions Authority

ENISA European Union Agency for Cybersecurity

ESA Autoridades Europeias de Supervisão

ESTG Escola Superior de Tecnologia e Gestão

EU European Union

EU-CyCLON European Cyber Crisis Liaison Organisation Network

IAM Identity and Access Management

IPVC Instituto Politécnico de Viana do Castelo

ISO International Organization for Standardization

MCyber Master in Cybersecurity

MFA Multi-factor Authentication

NIS2 Network and Information System Directive 2

NIST National Institute of Standards and Technology

RGPD Regulamento Geral de Proteção de Dados

RMF Risk Management Framework

SaaS Software as a Service

SIEM Security Information and Event Management

SOC Security Operation Center

TI Tecnologias da Informação

TIC Tecnologias da Informação e Comunicação

TLPT Threat-led Penetration Testing

TPRM Third-Party Risk Management

VPN Virtual Private Network

WAF Web Application Firewall

Capítulo 1

Introdução

A presente tese apresenta o trabalho desenvolvido pelo autor no âmbito do mestrado em Cibersegurança, da Escola Superior de Tecnologia e Gestão (ESTG), do Instituto Politécnico de Viana do Castelo (IPVC), orientada pelo Prof. Francisco Guimarães e Prof. Pedro Coutinho. Neste Capítulo é feita a contextualização do tema a desenvolver e de seguida descritos os seus objetivos e respetiva motivação.

1.1 Motivação

A cibersegurança tornou-se um elemento crítico para as seguradoras, que lidam com volumes significativos de dados sensíveis e dependem fortemente de sistemas digitais. Qualquer falha nestes sistemas pode gerar consequências económicas, legais e reputacionais graves. Embora já existam requisitos regulamentares – como Solvência II(regime europeu de regulação para seguradoras que estabelece regras para gestão de riscos) e orientações da ASF (Autoridade de Supervisão de Seguros e Fundos de Pensões) – a ausência, até recentemente, de um normativo europeu harmonizado deixava lacunas significativas. O DORA (Digital Operational Resilience Act) surge para colmatar essas falhas, promovendo um quadro regulatório coerente para a resiliência digital no setor financeiro. Esta evolução regulatória, aliada ao curto prazo para implementação, motivou o desenvolvimento desta tese com foco numa seguradora portuguesa do Ramo Vida, particularmente exposta a riscos.

1.2 Objetivo da Investigação

O principal objetivo desta investigação é identificar um possível mapeamento dos controlos DORA no contexto de uma arquitetura de segurança e gestão de risco de uma seguradora portuguesa do Ramo Vida, propondo um plano de ação que permita atingir a conformidade regulatória e fortalecer a resiliência operacional. Pretende-se ainda compreender de que forma o DORA se distingue de regulamentos anteriores e como pode ser operacionalizado no contexto real de uma organização com sistemas legados, recursos limitados e elevada sensibilidade dos dados tratados. A tese procura, assim, desenvolver recomendações práticas alinhadas com os requisitos legais, as boas práticas internacionais e o nível de maturidade tecnológica da entidade analisada. Importa referir que o nome da companhia não será mencionado, garantindo a confidencialidade das informações internas que venham a ser utilizadas.

1.3 Impacto Esperado

A implementação das recomendações propostas neste trabalho deverá contribuir diretamente para elevar o grau de maturidade em cibersegurança da seguradora estudada, reduzir o risco de incidentes, e fortalecer a confiança junto dos reguladores, clientes e parceiros.

A nível setorial e académico, o trabalho pretende preencher uma lacuna existente na documentação prática sobre a aplicação do DORA em Portugal. Como muitas seguradoras partilham características semelhantes – como dependência de sistemas legados e desafios de gestão de fornecedores de TIC – as recomendações extraídas deste estudo poderão ser generalizadas e aplicadas a outras entidades do setor. Desta forma, a tese poderá contribuir para a difusão de conhecimento aplicado num momento-chave de transformação regulatória.

1.4 Atividades de Investigação Realizadas

Foram realizadas as seguintes atividades no âmbito desta tese:

- Revisão da literatura e de documentação oficial (DORA, orientações da EIOPA-

European Insurance and Occupational Pensions Authority, ASF, etc.);

- Levantamento dos requisitos do DORA e sua comparação com o quadro regulatório pré-existente (ex.: Solvência II, ISO 27001);
- Definição de critérios de análise de maturidade organizacional face ao DORA;
- Levantamento de práticas internas da seguradora estudada (entrevistas, documentos internos), arquitetura de segurança de informação e modelo de governo de segurança de informação;
- Identificação de lacunas e formulação de recomendações organizadas num plano de ação prático e estruturado.

1.5 Organização do Documento

Este documento encontra-se estruturado em cinco capítulos principais, organizados de forma a apresentar progressivamente o contexto, os objetivos, a metodologia e os resultados do estudo realizado sobre a implementação do Regulamento DORA numa seguradora portuguesa do Ramo Vida.

- **Capítulo 1 – Introdução:** Apresenta o contexto geral da investigação, incluindo a motivação, os objetivos, o impacto esperado, as linhas de investigação abertas e as atividades realizadas até ao momento.
- **Capítulo 2 – Estado da Arte:** Descreve o enquadramento teórico e regulamentar do setor segurador, com foco em referências normativas como o DORA, a ISO/IEC 27001, ISO 27002, ISO 27005 e a Diretiva NIS2.
- **Capítulo 3 – Proposta de Tese:** Define o problema de investigação, a hipótese de solução e a metodologia adotada, detalhando a abordagem aplicada ao estudo de caso.
- **Capítulo 4 – Estudo de Caso e Resultados:** Apresenta a análise de conformidade com o DORA na seguradora, incluindo os controlos implementados, lacunas identificadas e mapeamento com normas ISO relevantes.

- **Capítulo 5 – Conclusão:** Resume os principais resultados obtidos e recomendações futuras.

Capítulo 2

Estado da Arte

Este capítulo apresenta o enquadramento teórico e normativo que sustenta o estudo, com foco nas principais referências aplicáveis à resiliência digital e à cibersegurança no setor segurador. São analisadas as normas e diretivas europeias relevantes — incluindo o DORA, a NIS2 e as normas ISO 27x — bem como as características do setor segurador e as suas arquiteturas tecnológicas típicas. O objetivo é construir uma base sólida de conhecimento para contextualizar o estudo de caso apresentado nos capítulos seguintes.

2.1 Visão Geral e Estado da Arte

A cibersegurança no setor financeiro, em particular nas seguradoras, tem sido objeto de crescente atenção devido à digitalização intensiva dos serviços e à complexidade das ameaças atuais. Neste capítulo é apresentado o enquadramento teórico e regulamentar relevante para a investigação, incluindo uma caracterização do setor segurador, as normas e diretivas aplicáveis – como a NIS2, a família ISO 27x e o Regulamento DORA – e os seus impactos práticos. Adicionalmente, são exploradas as arquiteturas de sistemas e infraestruturas tecnológicas típicas do setor, com foco na realidade portuguesa. O objetivo é construir uma base sólida para compreender os desafios e oportunidades decorrentes da implementação do DORA no contexto de uma seguradora do ramo Vida.

2.2 Setor Segurador

As seguradoras são entidades financeiras que operam com base na assunção e gestão de riscos, oferecendo proteção contra perdas económicas a indivíduos e organizações em troca do pagamento de prémios. Para cumprir essa função, estas instituições utilizam apólices de seguro – contratos formais que estabelecem as coberturas (isto é, os riscos garantidos), os limites de indemnização, as exclusões e as obrigações de ambas as partes.

A operação de uma seguradora envolve o processamento intensivo de dados sensíveis, incluindo dados pessoais e médicos dos segurados, informações contratuais e transacionais, dados bancários, registos de sinistros (pedidos de indemnização), e registos de prémios pagos ou em dívida. Para além disso, muitas seguradoras participam em processos de co-seguro(partilha de risco entre várias companhias num mesmo contrato) e resseguro (transferência de parte do risco para um ressegurador), o que implica a troca de dados comerciais e operacionais com parceiros externos, frequentemente de natureza internacional [46].

No Ramo Vida e Saúde, a complexidade aumenta com a necessidade de integrar dados clínicos, informações biométricas, registos de beneficiários e validação de tratamentos efetuados. Este modelo de negócio pressupõe também a existência de uma rede de distribuição assente em parceiros comerciais, como corretores e mediadores, que atuam como intermediários entre o cliente final e a seguradora, tratando da angariação, renovação e acompanhamento de apólices. Estes mediadores acedem frequentemente a sistemas internos da seguradora ou a portais dedicados, onde introduzem dados, consultam coberturas, acompanham sinistros e executam atos de gestão contratual.

Com a crescente digitalização dos serviços, os sistemas de informação das seguradoras tornam-se alvos frequentes de ameaças de cibersegurança. Entre os riscos mais comuns encontram-se os ataques de *ransomware*, que podem cifrar e tornar indisponíveis sistemas críticos como os de gestão de apólices, sinistros ou pagamentos, e as violações de dados, que podem expor dados sensíveis de segurados, beneficiários, mediadores e parceiros [29].

Para além das ameaças externas, também interrupções não maliciosas – como falhas técnicas, desastres naturais ou erros humanos – podem comprometer seriamente a continuidade de um negócio que, por natureza, deve manter capacidade de resposta em qualquer cenário. O impacto da indisponibilidade ou corrupção de dados relativos a prémios,

coberturas ou sinistros pode resultar em atrasos no pagamento de indemnizações, erros contratuais, ou mesmo falhas regulatórias com consequências reputacionais e legais.

Este panorama reforça a importância da resiliência operacional digital, ou seja, a capacidade da seguradora prevenir, resistir, responder e recuperar face a eventos adversos que afetem os seus sistemas e dados. Mais do que apenas proteger ativos informáticos, trata-se de garantir a continuidade do serviço aos segurados, a integridade da relação com parceiros, e a conformidade com normas regulamentares como o DORA, que elevam o patamar exigido para a gestão de riscos tecnológicos no setor segurador [16].

2.2.1 Atividade seguradora

Vários estudos têm sido realizados sobre a governação da cibersegurança em Portugal. No entanto, ainda há uma lacuna no que diz respeito ao setor de seguros. As seguradoras são um dos alvos preferenciais de ataques informáticos porque, tal como outras indústrias, trabalham com dados de clientes, mas têm uma particularidade: mantêm nas suas bases dados financeiros e uma grande quantidade de informações pessoais dos seus segurados. A Estratégia Nacional de Segurança do Ciberespaço 2019-2023 [8] destaca a necessidade de maximizar a resiliência, promover a inovação e gerar e garantir recursos. No entanto, esta estratégia é ampla e não se concentra especificamente no setor de seguros. Alguns modelos de governação de cibersegurança já foram propostos. Por exemplo, a EY Portugal sugere a criação de um modelo de governo robusto que permita uma gestão clara e eficaz dos processos de cibersegurança da empresa [42]. No entanto, esses modelos não são específicos para o setor de seguros e podem não abordar todas as suas necessidades únicas. Em resumo, embora existam muitos trabalhos relacionados à cibersegurança e à sua governação, ainda há uma necessidade significativa de pesquisa no contexto específico do setor de seguros em Portugal.

Pylant[43] identifica como grandes desafios da cibersegurança a falta de colaboração entre diferentes partes interessadas, a complexidade das ameaças de cibersegurança, a falta de recursos e financiamento adequados, a falta de consciencialização e treino em segurança cibersegurança e a necessidade de conformidade com as normas e regulamentações.

2.2.2 Arquitetura de sistemas

As seguradoras europeias – incluindo as portuguesas – tradicionalmente operam sistemas de informação centralizados, muitas vezes assentes em mainframes ou *legacy* monolítico. Essas plataformas nucleares, embora robustas, apresentam limitações em flexibilidade e interoperabilidade, levando o setor a conviver com um elevado nível de dependência de sistemas antigos e de *outsourcing* de TIC para a sua manutenção e evolução. Observa-se uma transição gradual para arquiteturas mais modernas e híbridas, combinando infraestruturas *on-premises* com serviços em *cloud*, o que permite escalar recursos e introduzir novas funcionalidades sem abandonar por completo os sistemas legados. De acordo com a EIOPA, cerca de 80% das seguradoras europeias já utilizam serviços de *cloud* fornecidos por grandes empresas tecnológicas (*Big Tech*) [21], predominando a adoção de soluções *cloud* em modelo SaaS para funções de suporte (como CRM ou *analytics*).

Consultoras como a EY recomendam que as seguradoras "enderecem o seu défice tecnológico digitalizando processos fundamentais, migrando para a *cloud* e adotando modelos flexíveis de contratação" [41], evidenciando a necessidade de modernização contínua.

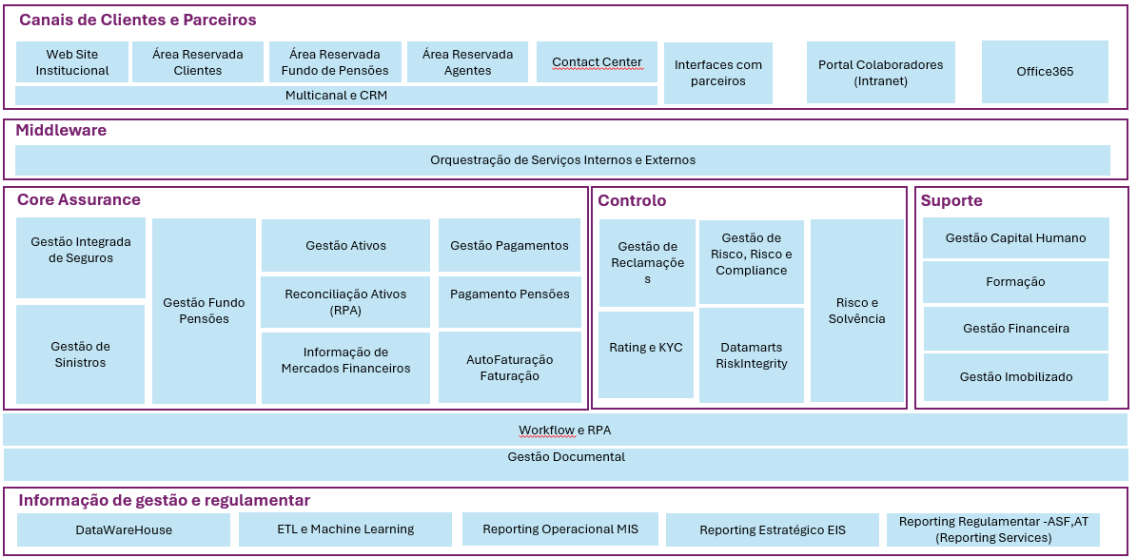

Figura 2.1: Arquitetura Aplicacional de Referência da Seguradora

A figura anterior representa a arquitetura aplicacional de referência da seguradora estudada, evidenciando a separação entre os sistemas centrais de negócio (core insurance), as aplicações de suporte e as interfaces externas. O modelo reflete uma estrutura típica do setor, combinando sistemas legados on-premises com novas plataformas baseadas em API

e serviços em nuvem, assegurando interoperabilidade e escalabilidade. Esta arquitetura serve de base para a análise de conformidade com o DORA, especialmente nos domínios da gestão de risco e continuidade operacional.

Em paralelo, tendências tecnológicas recentes estão a moldar a arquitetura de sistemas no setor. A implementação de arquiteturas orientadas a micro serviços e *Aplication Program Interface* (API) tem ganhado tração, permitindo modularizar funcionalidades e facilitar integrações internas e externas. Por meio de APIs abertas, algumas seguradoras expõem dados e serviços de forma controlada a parceiros e *fintech/insurtechs*, alinhando-se ao conceito emergente de *Open Insurance*[30]. Esta abordagem – análoga ao *Open Banking*– prevê a partilha segura de dados e funcionalidades de seguros com terceiros autorizados, fomentando ecossistemas de inovação. A nível europeu, discute-se a normalização do *Open Insurance* em moldes regulatórios: um documento de discussão da EIOPA concluiu que a abertura de dados no setor pode trazer benefícios a consumidores e operadores, mas também levanta riscos importantes em termos de privacidade e segurança, exigindo monitorização e possíveis ajustes regulatórios [24].

Apesar dos avanços, persistem desafios significativos na gestão deste panorama tecnológico, a coexistência de sistemas legados com aplicações modernas requer esforços de interoperabilidade, de forma a assegurar que os diversos módulos e plataformas (internos e de terceiros) comunicam de maneira eficaz e segura. O risco de concentração excessiva de fornecedores também é uma preocupação: a forte dependência de poucos prestadores de *cloud* ou de software pode comprometer a resiliência operacional, tal como alerta a própria EIOPA [26]. Neste contexto, o enquadramento normativo recente reflete essas preocupações. Em particular, o Regulamento DORA impõe requisitos reforçados de governação de TIC e de gestão de riscos de terceiros críticos no setor financeiro. O DORA obriga as seguradoras a reforçar a supervisão e resiliência dos seus sistemas e fornecedores de TI, contemplando planos de continuidade, testes regulares de segurança e a avaliação rigorosa de parceiros tecnológicos. Tais medidas ganham especial relevância no contexto português, onde estudos apontam que a transição de plataformas antigas para novas é percecionada como um dos principais constrangimentos à transformação digital das seguradoras [4]. A Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF), alinhada com orientações europeias (adotou as guidelines da EIOPA sobre *cloud outsourcing* e in-

centiva a inovação via *Open Insurance*), tem enfatizado a necessidade de melhoria contínua da resiliência operacional e da gestão de fornecedores de TIC, visando assegurar que o setor segurador nacional tira proveito da digitalização em conformidade com as exigências regulatórias atuais.

2.2.3 Arquitetura tecnológica

As exigências regulatórias mais recentes, como as introduzidas pela NIS2 e pelo Regulamento DORA, obrigam as seguradoras a reforçar significativamente a sua arquitetura tecnológica, com foco na resiliência operacional, capacidade de deteção e resposta a incidentes, e na segurança da informação. Este reforço implica a modernização de sistemas de monitorização, a introdução de ferramentas de gestão de eventos e informações de segurança (SIEM), soluções de *logging* centralizado, mecanismos de deteção de anomalias baseados em inteligência artificial, e plataformas integradas para gestão de incidentes [1].

Todavia, muitas seguradoras operam, ainda hoje, com processos informais e fragmentados de resposta a incidentes ou sem planos específicos de continuidade e recuperação focados em ciberataques. A nova regulamentação exige a formalização de procedimentos e a documentação de planos robustos de continuidade de negócios e de recuperação de negócios, com testes regulares e métricas de eficácia [19]. Para garantir conformidade e eficácia operacional, torna-se igualmente necessário investir em competências internas especializadas, incluindo ciberforense, testes de penetração, gestão de riscos de fornecedores de TIC e resposta a incidentes.

A ASF, alinhada com a EIOPA, tem salientado a importância da capacitação técnica e organizacional do setor segurador, nomeadamente através da adoção de modelos de avaliação contínua da maturidade em cibersegurança, da integração de *frameworks* internacionais (ex. NIST, ISO 27001/2) e da articulação entre departamentos técnicos, jurídicos e de compliance [3]. Em Portugal, estudos recentes indicam que a maioria das seguradoras reconhece a necessidade de atualizar os seus sistemas tecnológicos, embora nem todas tenham planos formalizados de investimento a médio prazo [5]. Este desfasamento entre a perceção de risco e a concretização de medidas é um dos fatores críticos apontados nos relatórios de estabilidade financeira do setor.

A Figura seguinte apresenta uma representação de referência da arquitetura tecnológica

atualmente utilizada na seguradora, baseada num datacenter redundante e num modelo híbrido com serviços maioritariamente *on-premises*. Esta arquitetura alinha-se com as exigências do novo enquadramento regulatório, evidenciando a articulação entre os componentes técnicos e a resiliência operacional.

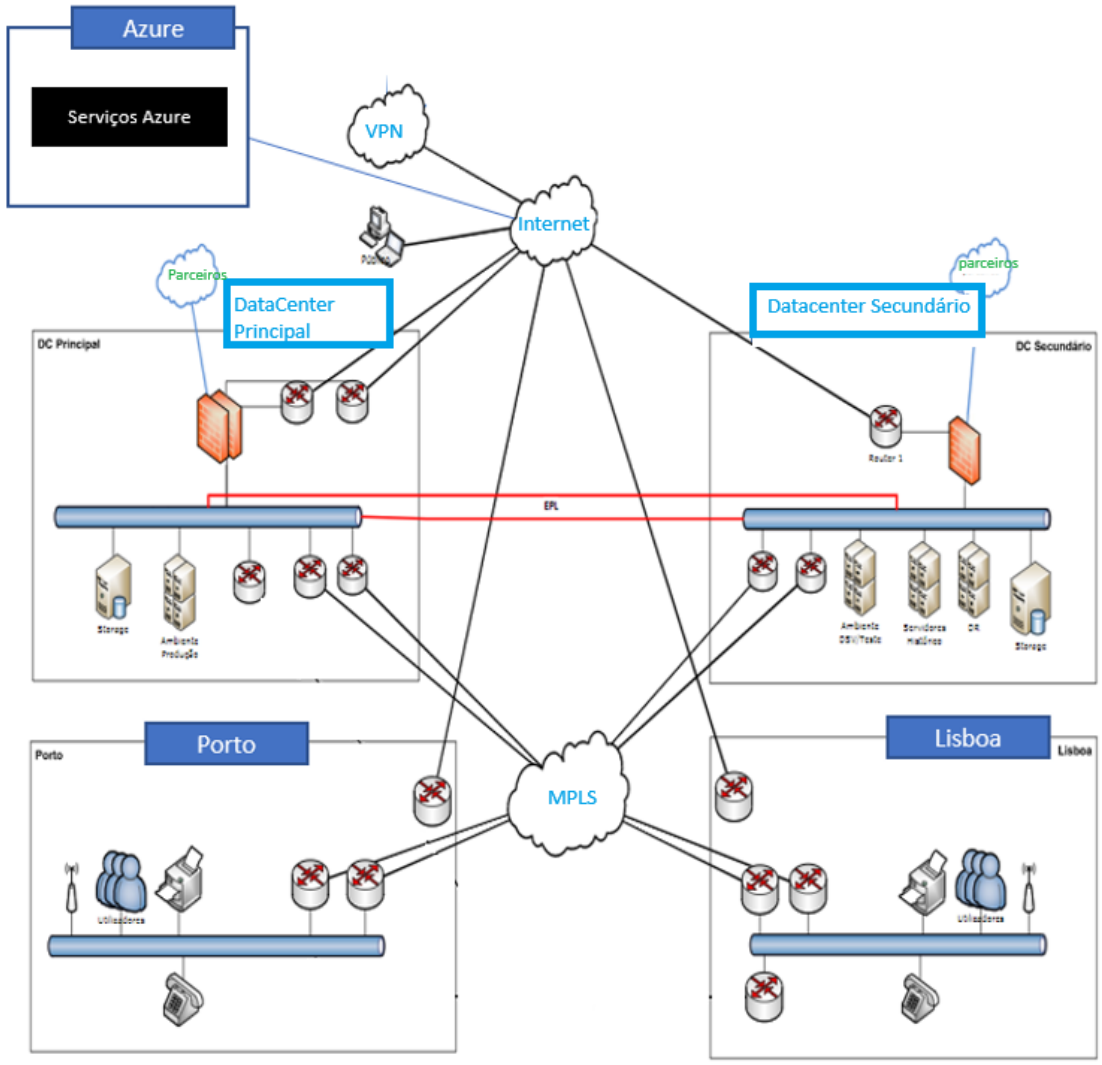

Figura 2.2: Arquitetura Tecnológica

Em síntese, a arquitetura tecnológica das seguradoras deve evoluir no sentido de suportar operações seguras, resilientes e auditáveis. Tal evolução exige não apenas tecnologia de ponta, mas também cultura organizacional orientada à prevenção, deteção e resposta coordenada, bem como forte cooperação entre as áreas de IT, gestão de risco e auditoria interna.

2.2.4 Arquitetura de Segurança

A digitalização crescente do setor segurador europeu trouxe uma maior exposição a riscos de cibersegurança, levando as seguradoras a adotarem arquiteturas de defesa em profundidade. Essa abordagem consiste em múltiplas camadas de segurança para proteger os ativos em diferentes níveis, conforme identificado na Figura 2.3.

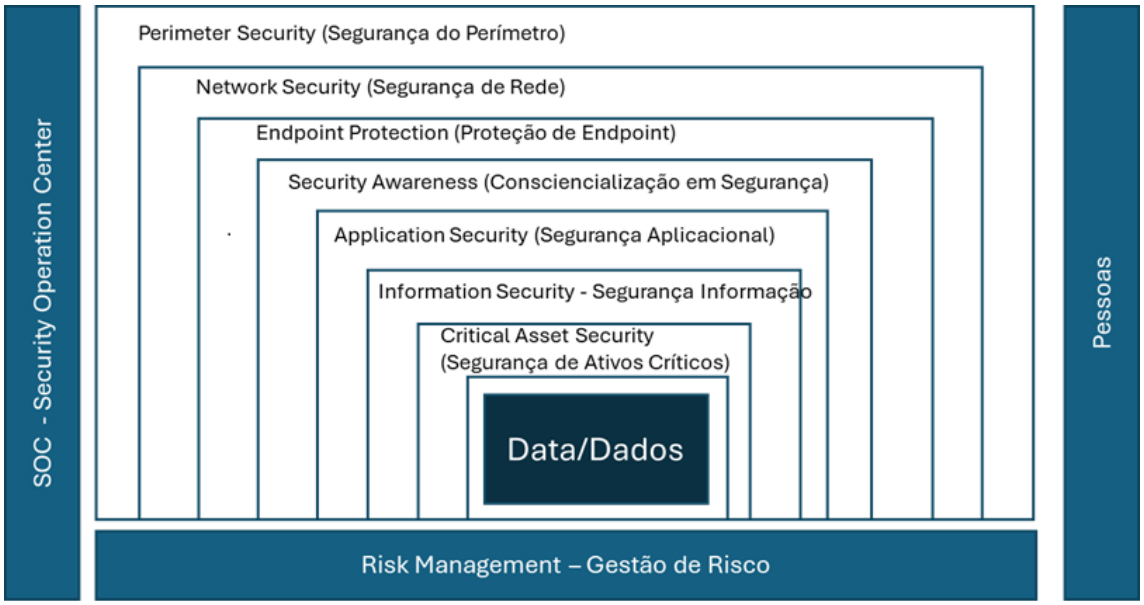

Figura 2.3: Defesa de Segurança em camadas

Reguladores europeus têm reforçado essa prática por meio de normas e orientações. Por exemplo, a EIOPA emitiu diretrizes que estabelecem capacidades mínimas de segurança esperadas ("*security baseline*") para as seguradoras. O DORA adotado em 2022, harmoniza as práticas de resiliência em cibersegurança entre todas as seguradoras europeias, levando o setor a um nível comum elevado de cibersegurança. Com base nesse quadro regulatório e nas recomendações de entidades como a ENISA, as seguradoras europeias estruturam sua segurança em camadas complementares (*defense-in-depth*). Em termos de perímetro e rede, são implementados *firewalls* avançados e segmentação de rede para controlar o tráfego e bloquear acessos não autorizados. Conexões externas (por exemplo, escritórios remotos ou *cloud*) são protegidas com VPNs seguras e, cada vez mais, com modelos *zero trust*de autenticação forte. Na camada de *endpoints*, utiliza-se antivírus/EDR de última geração para monitorizar continuamente dispositivos (estações de trabalho, servidores) e responder a comportamentos suspeitos em tempo real [17][44]. As seguradoras também

mantêm rigorosos processos de gestão de *patches*para mitigar vulnerabilidades exploráveis. Na camada aplicacional e de dados, adota-se o princípio de "*secure by design*" no desenvolvimento de software, recorrendo a testes de segurança (análise de código,*pentests*) e à proteção em tempo real de aplicações críticas (por exemplo, via WAF – *Web Application Firewall*). Os dados sensíveis são cifrados em repouso e em trânsito, com controles de acesso baseados no princípio do menor privilégio. De facto, as normas europeias enfatizam políticas robustas de controle lógico de acessos (identidade e gestão de acessos) e autenticação multi-fator, para garantir que os utilizadores acedem apenas ao necessário (*need-to-know*).

O cumprimento do RGPD é igualmente exigido,o que obriga a medidas adequadas de proteção de dados pessoais em todas as camadas de sistemas. Adicionalmente, as seguradoras investem na camada humana e organizacional, reconhecendo que a consciencialização dos colaboradores é crucial. Os programas regulares de training e *awareness* em cibersegurança são práticas comuns no setor, alinhados às diretrizes de supervisores europeus. Por exemplo, as próprias orientações da EIOPA reforçam que todos os colaboradores e prestadores de serviços sejam adequadamente informados sobre as políticas de segurança, através de formação e sessões de sensibilização. Essa educação contínua visa mitigar ameaças como *phishing*e erro humano, frequentemente responsáveis por incidentes de segurança.

Por fim, uma camada de monitorização, resposta e recuperação completa a arquitetura: seguradoras tipicamente operam centros de operações de segurança (SOC) ou serviços de monitorização de eventos (SIEM) para detetar intrusões e responder prontamente a incidentes. Planos de resposta a incidentes e de continuidade de negócio são periodicamente testados, e a recuperação de desastres é apoiada por rotinas robustas de *backup*, incluindo cópias imutáveis. A ENISA, por exemplo, recomenda manter cópias de segurança atualizadas e isoladas da rede, seguindo a regra 3-2-1 (3 cópias em 2 tipos de médias, 1 *off-site*) para assegurar a recuperação em caso de ataques (como por exemplo, *ransomware*). Está também cada vez mais em voga as componentes de *cyber vault* desconectado da rede de produção através de *airgap*(desconexão automatizada) onde se armazenam todos os dados críticos fora da rede para isolá-los de possíveis ataques.

Estas múltiplas salvaguardas garantem que, mesmo se um atacante ultrapassar uma

camada de defesa, outra camada subsequente possa conter a ameaça.

Em Portugal, a arquitetura de segurança da informação das seguradoras reflete as melhores práticas europeias acima descritas, adaptando-as à dimensão e contexto local. As seguradoras nacionais seguem as orientações da EIOPA e agora do DORA, implementadas através do regulador setorial (ASF). Historicamente, a aplicação da Diretiva NIS 1 ao setor segurador português não foi obrigatória, mas o DORA vem uniformizar os requisitos de resiliência digital também no mercado português.

No panorama nacional, destaca-se o papel do Centro Nacional de Cibersegurança (CNCS) e da Associação Portuguesa de Seguradores (APS) na promoção da segurança da informação no setor. O CNCS disponibiliza instrumentos e referenciais de boas práticas que orientam as organizações portuguesas na adoção das melhores medidas de cibersegurança.

Em paralelo, a APS tem incentivado a capacitação em cibersegurança, evidenciada por iniciativas como cursos dirigidos aos executivos sobre DORA e gestão de riscos digitais em parceria com entidades especializadas.

Essas ações reforçam a cultura de segurança nas seguradoras portuguesas, complementando os controles técnicos. Na prática, os grandes grupos seguradores em Portugal já contam com arquiteturas em camadas semelhantes às dos seus pares europeus: *firewalls* de próxima geração no perímetro, segmentação de rede interna, ferramentas EDR nos *endpoints*, políticas de IAM rigorosas (com MFA, gestão de privilégios) e proteção de dados sensíveis conforme o RGPD. Além disso, é comum a realização de auditorias de segurança e alinhamento com *frameworks* de segurança e certificações (como a ISO 27001) para atestar a maturidade dos processos de segurança da informação. Importa notar que a resiliência é uma prioridade: mecanismos de backup e recuperação de desastres são regularmente revistos, e as seguradoras colaboram com a ASF no reporte e gestão de incidentes críticos. Em suma, a arquitetura de segurança da informação das seguradoras portuguesas – em ambientes híbridos que combinam infraestruturas locais e *cloud*– apoia-se num modelo de defesa em camadas alinhado com os padrões europeus, utilizando um conjunto abrangente de controles técnicos e práticas de gestão para proteger os sistemas e os dados dos clientes em face de um cenário de ameaças em constante evolução.

2.3 Regulamentação e boas práticas

Do ponto de vista regulatório, antes do DORA, as exigências relativas à segurança de TIC no setor segurador estavam principalmente incorporadas em normas de gestão de risco e controlo interno, sem um padrão único de referência. O regime Solvência II, por exemplo, estabelece que as seguradoras devem ter sistemas de gestão de risco eficazes, abrangendo todos os tipos de risco (incluindo risco operacional e de TIC), e requer a existência de funções de controlo independentes (como gestão de riscos, compliance, auditoria interna) que supervisionem também esses domínios [27].

2.3.1 Referência DORA

O Regulamento DORA surge, assim, para uniformizar e elevar o patamar de resiliência digital em todo o setor financeiro europeu. De acordo com a EIOPA, o DORA tem o objetivo de assegurar que as entidades financeiras "se mantenham resilientes em caso de perturbação operacional severa", harmonizando as regras relativas à resiliência operacional digital em diferentes tipos de instituições e cobrindo também os prestadores de serviços de TIC que lhes fornecem serviços críticos [23]. Em síntese, o DORA explicita requisitos em cinco domínios principais:

1. Gestão de riscos de TIC – As entidades devem implementar um *framework* robusto de gestão de risco relacionado com as Tecnologias de Informação e Comunicação. Isto inclui governação interna adequada (papéis e responsabilidades bem definidos, envolvendo a gestão de topo), políticas e procedimentos para identificar, avaliar, mitigar e monitorizar riscos de TIC de forma contínua. O DORA enfatiza que a alta administração (Conselho de Administração) é responsável por aprovar e supervisionar este framework, assegurando que dispõe de recursos e competências para tal. Um elemento introduzido pelo DORA é a necessidade de existir uma função de controlo de risco de TIC dedicada, que pode ser incorporada numa função existente (por exemplo, na gestão de riscos ou segurança da informação), mas que deve ter independência face às operações de TI. Também fazem parte deste domínio requisitos para gestão de mudanças nos sistemas, desenvolvimento seguro de software, classificação de ativos de informação e proteção conforme a criticidade, entre outros.

2. Gestão de incidentes de TIC – Implementação de processos eficazes de deteção, resposta e recuperação perante incidentes que afetem a segurança ou funcionamento dos sistemas de informação. O DORA define um conceito de incidente de TIC que abrange qualquer evento inesperado com impacto negativo na integridade, disponibilidade, confidencialidade ou autenticidade dos dados ou serviços de informação da empresa. As entidades devem possuir capacidades de monitorização e *logging*, assim como procedimentos de escalonamento interno. Importa salientar que o DORA estabelece critérios para classificação de incidentes (por magnitude, número de clientes afetados, duração, etc.) e identifica quais são considerados "incidentes graves" (*major incidents*). Estes incidentes mais sérios deverão ser notificados às autoridades de supervisão competentes num prazo definido, seguindo formatos e procedimentos que estão a ser detalhados através de *standards* técnicos regulatórios (RTS/ITS) a nível europeu.

3. Testes de resiliência operacional digital – O regulamento exige que as instituições realizem testes periódicos aos seus sistemas e controlos de segurança, com uma frequência mínima anual, visando avaliar a eficácia da sua resiliência operacional digital. Esses testes devem incluir diferentes tipos de avaliações, desde análises de vulnerabilidades e testes de penetração (incluindo, para entidades mais complexas, testes avançados do tipo TLPT(*Threat -Led Penetration Testing*), conduzidos por equipas certificadas e simulando técnicas de ameaças reais [25]. O objetivo é identificar proativamente falhas ou fragilidades nos sistemas, processos ou equipas, e corrigi-las antes que sejam exploradas em ataques reais. O DORA requer que as entidades desenvolvam programas de teste proporcionais à sua dimensão e risco, e que abordem tanto sistemas internos como interdependências com terceiros. Este componente de teste regular é fundamental para assegurar uma melhoria contínua da postura de segurança.

4. Gestão de riscos de TIC de terceiros – Reconhecendo que as entidades financeiras dependem crescentemente de fornecedores externos de tecnologia (por exemplo, *cloud providers*, empresas de outsourcing de TI, fornecedores de software, etc.), o DORA introduz requisitos estritos para *due diligence*, monitorização e gestão de contratos

com esses terceiros. As empresas devem avaliar os riscos de TIC associados a cada fornecedor crítico, garantir que cláusulas contratuais específicas estejam presentes (cobrindo aspetos como direitos de auditoria, requisitos de notificações de incidentes, medidas de segurança que o fornecedor deve cumprir, planos de contingência, etc.), e monitorizar continuamente o desempenho e a conformidade dos terceiros com essas obrigações. Além disso, o DORA estabelece um regime de supervisão direta para prestadores de TIC terceiros críticos, através da designação de alguns deles para um esquema de supervisão europeia (conduzido pelas Autoridades Europeias de Supervisão(ESAs), o que implica que certas empresas tecnológicas que sirvam grande parte do setor financeiro sejam auditadas e orientadas diretamente pelos reguladores financeiros. As seguradoras, por sua vez, deverão cooperar nesse processo e considerar a resiliência dos seus fornecedores como parte integrante da sua própria resiliência operacional.

5. Partilha de informação sobre ciberameaças – O DORA encoraja as entidades a partilhar informações entre si, de forma voluntária, acerca de ameaças, vulnerabilidades, técnicas de ataque e incidentes (*cyber threat intelligence*). O intuito é promover uma inteligência coletiva no setor financeiro que ajude a antecipar riscos emergentes e a adotar medidas preventivas. As entidades que participem em grupos de partilha de informação devem informar o regulador da sua participação. Embora essa partilha não seja obrigatória, ela representa uma mudança cultural importante: sai-se de um paradigma em que incidentes eram mantidos em segredo por vergonha ou medo de repercussões, para um paradigma de colaboração setorial na resposta a ameaças comuns. A criação de repositórios ou fóruns de informação partilhada poderá, a médio prazo, beneficiar sobretudo organizações com menos recursos, que passam a ter acesso a *insights* e alertas precoces fornecidos por pares ou por entidades especializadas.

Esses cinco domínios cobrem, portanto, todo o ciclo de vida da resiliência digital: desde a prevenção e preparação (gestão de riscos e testes), passando pela gestão de incidentes e continuidade, até a cooperação inter-institucional. A amplitude do âmbito do DORA traz uma elevação do nível de exigência. Não basta que a seguradora tenha algumas políticas

genéricas é necessário comprovar que existem procedimentos e capacidades operacionais em cada um desses pilares, funcionando de forma integrada. Por exemplo, políticas de gestão de risco de TIC devem estar alinhadas com procedimentos de resposta a incidentes; os resultados dos testes de resiliência devem retroalimentar o processo de gestão de risco; a gestão de terceiros deve estar alinhada com a estratégia de continuidade de negócio, e assim por diante. Essa necessidade de coerência interna é um dos aspetos que tornam a implementação prática do DORA desafiante.

2.3.2 Referência ISO 27001, 27002 e 27005

Adicionalmente, organizações internacionais e nacionais forneceram *frameworks* de boas práticas em cibersegurança que, embora não obrigatórias por lei, serviam de orientação para as seguradoras reforçarem a sua postura de segurança. Destacam-se, entre elas, o NIST *Cybersecurity Framework*, a norma ISO/IEC 27001, os Controles CIS, bem como orientações da ENISA e do Centro Nacional de Cibersegurança (CNCS) em Portugal [28][9].

2.3.3 Referência NIS2

A Diretiva (UE) 2022/2555 (NIS2), adotada a 14 de dezembro de 2022, substitui a Diretiva NIS (2016/1148), reforçando o quadro normativo europeu em matéria de cibersegurança. O principal objetivo da NIS2 é alcançar um elevado nível comum de resiliência em cibersegurança em todos os Estados-Membros, corrigindo lacunas observadas na implementação da diretiva anterior [12]. Para tal, impõe que os países reforcem as suas capacidades nacionais, com estratégias atualizadas, e que as entidades abrangidas adotem medidas proporcionais de gestão de risco de segurança da informação [32].

A NIS2 define requisitos mínimos harmonizados para todas as entidades críticas, incluindo políticas de análise de risco, planos de continuidade de negócio, resposta a incidentes, segurança na cadeia de fornecimento, controlo de acessos, criptografia, e formação em cibersegurança [13]. O regime de notificação de incidentes foi reforçado, exigindo comunicação em três fases: alerta inicial, notificação completa e relatório final [36].

Introduz-se a responsabilidade direta dos órgãos de gestão de topo e um sistema de supervisão mais rigoroso, com sanções que podem atingir 10 milhões de euros ou 2% do vo-

lume de negócios global [14]. A NIS2 alarga significativamente a sua abrangência setorial, incluindo agora operadores de serviços financeiros, saúde, indústria, transportes, comunicações, entre outros [34]. A diretiva distingue entidades "essenciais" e "importantes", com obrigações semelhantes, mas regimes de supervisão distintos [18].

A cooperação europeia é reforçada através do Grupo de Cooperação NIS, da rede CSIRT e da nova EU-CyCLON(*European cyber crisis liaison organisation network*), promovendo uma resposta coordenada a ciberameaças de grande escala [33]. Por fim, a diretiva adota o princípio da proporcionalidade, adequando as exigências à criticidade e dimensão da entidade, visando um equilíbrio entre segurança e capacidade operacional [15].

Um estudo da IDC, datado de julho de 2024, com o patrocínio da Microsoft, revela que 47% das empresas portuguesas têm pouco ou nenhum conhecimento sobre a diretiva NIS2,evidenciando fraca preparação para os novos requisitos de cibersegurança. Apenas 14% das organizações europeias estão totalmente preparadas, e 60% das empresas nacionais não envolvem a administração no tema. Portugal apresentava uma das coberturas mais baixas sob a NIS1 (60%), demonstrando necessidade urgente de sensibilização. A NIS2 é vista como componente essencial da segurança nacional [6].

Como referenciado no estudo da *Frontier Economics*[20], a implementação da diretiva NIS2 em Portugal terá um custo estimado de 529 milhões de euros para as empresas, afetando especialmente as de menor dimensão. O setor financeiro, fortemente dependente de fornecedores tecnológicos, será impactado por maiores custos operacionais e de conformidade. Medidas discriminatórias, como a exclusão de fornecedores com base em critérios não técnicos, podem reduzir a concorrência e travar a inovação. Estima-se que estas políticas resultem numa perda de 289 milhões de euros no PIB e na eliminação de cerca de mil postos de trabalho. O estudo recomenda focar em critérios técnicos para mitigar riscos de forma proporcionada e eficiente.

A Diretiva (UE) 2022/2555 (NIS2) não foi transposta para a lei portuguesa até outubro de 2024, encontrando-se atualmente em fase de proposta legislativa, através da Proposta de Lei n.º50/XVI/1.ª, devido à dissolução do Parlamento no dia 14 de março de 2025 a votação da autorização legislativa para aprovação da proposta de lei ainda não ocorreu. Esta proposta visa estabelecer um novo Regime Jurídico da Cibersegurança, alinhado

com os requisitos europeus, reforçando a proteção das redes e dos sistemas de informação críticos para o funcionamento da economia e da sociedade portuguesa. Reforça o papel do Centro Nacional de Cibersegurança (CNCS) como autoridade competente. Introduz ainda mecanismos estruturantes como a Estratégia Nacional de Segurança do Ciberespaço, o Plano Nacional de Resposta a Incidentes de Cibersegurança e o Quadro Nacional de Referência para a Cibersegurança, bem como um novo modelo de supervisão dual, com base no risco e categoria da entidade supervisionada.

O novo regime revoga, entre outros diplomas, a Lei n.º 46/2018, de 13 de agosto, que constituía o regime jurídico anterior de segurança do ciberespaço, e o Decreto-Lei n.º 65/2021, de 30 de julho, que regulamentava essa mesma lei.

A aplicabilidade da Diretiva (UE) 2022/2555 (NIS2) às empresas de seguros suscita alguma ambiguidade regulamentar. A nível europeu, a posição da *Insurance Europe*é clara ao afirmar que, no quadro legal harmonizado da UE, o setor segurador — nomeadamente as seguradoras de vida e fundos de pensões — está prioritariamente abrangido pelo Regulamento (UE) 2022/2554 (DORA), sendo a NIS2 considerada não aplicável de forma autónoma ao setor financeiro, exceto nos casos especificamente definidos pelas autoridades competentes [31]. No entanto, em Portugal, esta leitura não é pacífica. Por um lado, a Presidente da ASF reconhece publicamente a relevância crescente da NIS2 no contexto da cibersegurança financeira e admite a sua articulação com o DORA, especialmente no que toca ao reforço da resiliência e à cooperação institucional entre entidades públicas e privadas [2]. Por outro lado, o Decreto-Lei n.º 22/2025, de 19 de março, que transpõe a Diretiva (UE) 2022/2557 relativa à resiliência de entidades críticas, designa explicitamente o setor segurador e os fundos de pensões como prestadores de serviços essenciais em território nacional[11], o que poderá implicar a sua inclusão formal no perímetro da NIS2. Esta sobreposição levanta dúvidas quanto à delimitação de obrigações, à articulação entre regimes jurídicos e ao modelo de supervisão entre CNCS e ASF, sendo necessário clarificar juridicamente o enquadramento aplicável às empresas de seguros no contexto português.

2.4 Impacto de boas práticas e referências para o setor segurador

Apesar dessas referências, a sua adoção era heterogénea e, na ausência de um mandato específico, algumas seguradoras poderiam não ter implementado todos os controles de forma abrangente ou consistente.

Vários desafios têm sido apontados por profissionais e entidades de supervisão no processo de implementação do DORA. Em primeiro lugar, a complexidade regulatória em si: o DORA é complementado por normas técnicas (RTS e ITS) e orientações que detalham os seus requisitos,o que resulta num conjunto extenso de textos técnicos a assimilar. Manter-se atualizado e entender plenamente essas especificações é exigente, especialmente para organizações de menor dimensão ou com equipas de *compliance* reduzidas.

Em segundo lugar, há desafios de governação e organização interna: possivelmente foi necessário criar funções ou comités (por exemplo, um responsável pelo controlo de risco de TIC,caso não exista), atribuir novas responsabilidades à gestão de topo e articular as várias áreas da empresa (TI, risco, segurança, operações, negócio) numa abordagem integrada de resiliência. Isso pode implicar mudanças culturais e de estrutura, nem sempre fáceis de implementar rapidamente.

Outro ponto crítico é o fator tempo e recursos disponíveis. O prazo para conformidade é curto, o que pressiona as seguradoras a executarem muitos projetos em paralelo – da avaliação de maturidade à implementação de ferramentas – em pouco tempo. Isso implica custos consideráveis e alocação de recursos dedicados. Entidades de menor porte ou com restrições orçamentais podem enfrentar dificuldades em arcar com investimentos em tecnologia e contratação/treino de especialistas. Mesmo grandes seguradoras precisam equilibrar as iniciativas do DORA com outros projetos estratégicos, evitando sobrecarga das equipas de TI e riscos de execução apressada.

Apesar desses desafios, a implementação do DORA traz benefícios significativos tanto para as organizações individualmente quanto para a robustez do sistema financeiro como um todo. Ao obrigar as empresas a olharem de forma holística para a sua resiliência digital, o DORA reduz a probabilidade de falhas catastróficas e limita efeitos em cascata de incidentes (onde o problema numa entidade pode propagar-se a outras,via interconexões

tecnológicas ou confiança do mercado).

Para a seguradora em estudo, a adoção das medidas exigidas pode resultar em melhoria substancial na proteção dos dados dos clientes e na continuidade das operações, diminuindo a frequência e impacto de interrupções. Adicionalmente, cumprir com sucesso o DORA pode se tornar um fator de vantagem competitiva: num mercado onde clientes e parceiros estão cada vez mais conscientes dos riscos de cibersegurança, demonstrar elevada resiliência e ter processos sólidos de gestão de incidentes pode elevar a confiança na marca e evitar perdas de negócio.

De facto, espera-se que o DORA contribua para um setor segurador mais resiliente e confiável, onde mesmo as empresas menores elevem seu padrão de segurança, fortalecendo a confiança dos consumidores na estabilidade do mercado. Em suma, embora a jornada de conformidade com o DORA seja trabalhosa, ela alinha-se com os interesses de longo prazo das seguradoras: proteger os seus clientes, assegurar a prestação contínua de serviços e manter a sustentabilidade e integridade do negócio frente aos desafios da era digital.

Capítulo 3

Tese e Problema de Investigação

Este capítulo descreve a abordagem seguida para o desenvolvimento do trabalho, incluindo o âmbito do estudo de caso e a metodologia que foi seguida para atingir os objetivos delineados. Em particular,é explicado como se identificou os desafios e lacunas na implementação do DORA e como foram desenvolvidas as recomendações para ultrapassar tais desafios numa seguradora modelo portuguesa do Ramo Vida (não identificada nesta tese por questões de confidencialidade),mas estruturadas para serem aplicada a qualquer seguradora.

3.1 Enquadramento do Estudo de Caso

A pesquisa foi centrada numa seguradora portuguesa do Ramo Vida de média dimensão, que opera num contexto de mercado nacional e está sujeita à regulação da ASF e às diretivas europeias aplicáveis. Esta seguradora serviu de caso de estudo para a análise de implementação do DORA. A opção por um estudo de caso permite obter uma visão aprofundada e concreta de como os requisitos do DORA se traduzem em desafios reais numa organização específica, oferecendo contexto e nuances que complementam a análise teórica. Os dados sobre a seguradora foram obtidos através de fontes documentais internas (por exemplo, políticas de segurança, relatórios de auditoria ou de risco, organogramas, etc.) e pela observação direta de processos, respeitando sempre as restrições de sigilo profissional e a autorização da empresa.

Este estudo de caso foi utilizado para validar o presente trabalho, na medida em

que permite confrontar as recomendações teóricas com a realidade prática. Os resultados específicos da seguradora (como as lacunas identificadas e as medidas teste) foram apresentados de forma agregada ou anonimizadas, de modo que as conclusões possam ser generalizáveis e úteis também para outras seguradoras que enfrentem desafios semelhantes na implementação do DORA.

3.2 Metodologia e Abordagem

Para alcançar os objetivos traçados, a metodologia da tese combinou pesquisa exploratória qualitativa (revisão de literatura e análise documental) com uma análise de caso prático (*gap analysis* na organização escolhida). Em vez de recorrer a entrevistas ou questionários junto a *stakeholders,* optou-se por privilegiar a análise de dados já disponíveis e referências consolidadas, complementada com a avaliação direta da seguradora, a fim de identificar de forma objetiva as discrepâncias em relação ao normativo DORA.

As etapas metodológicas principais foram as seguintes:

Revisão de Literatura e Referenciais: Numa fase inicial, foi realizada uma extensa pesquisa bibliográfica e documental para embasar o estudo. Esta revisão abrange:

O conteúdo detalhado do Regulamento DORA, regulamentação ASF e teses complementares (normas técnicas regulatórias, orientações das autoridades europeias, etc.), para extrair um elenco completo dos requisitos aplicáveis às seguradoras. Também foram consideradas comunicações e guias emitidos pela ASF ou EIOPA especificamente para apoiar a implementação do DORA.

Estudos, artigos e análises recentes sobre os desafios de implementação do DORA no setor financeiro e, quando possível, no setor segurador. Este subtema emergiu recentemente na literatura, dado *timing* do regulamento, e inclui artigos de consultorias, publicações especializadas em TI e gestão de risco,assim como casos já reportados. Por exemplo, pretendeu-se identificar através da literatura quais são os principais *gaps* comuns que as instituições têm encontrado (como falta de processos formais de gestão de incidentes, ausência de ferramentas de teste, etc.), bem como estratégias sugeridas para os colmatar.

Normas e boas práticas de cibersegurança relevantes para o cumprimento do DORA.

Nesta componente, foram avaliadas *frameworks* como NIST CSF, ISO 27001, COBIT, entre outras, para compreender como podem ser utilizadas como camadas de estrutura na construção de capacidades de resiliência operacional. Embora o foco do trabalho seja o DORA, essas normas oferecem orientações práticas que podem inspirar as soluções a adotar. Por exemplo, o NIST CSF poderá ser útil para estruturar o processo de gestão de riscos de TIC (identificar, proteger, detetar, responder, recuperar), enquanto a ISO 27001 fornece um catálogo de controlos de segurança que podem ser mapeados para requisitos do DORA (ex.: controle de acessos, criptografia, backups, etc.).

O contexto regulatório e ambiente atual do setor segurador português em matéria de segurança da informação. Aqui foram incluídos relatórios ou estudos do mercado português (por exemplo, da ASF, do CNCS ou de associações do setor) que indiquem o nível de preparação médio das seguradoras face a riscos de cibersegurança, incidência de incidentes, etc., para situar o caso de estudo numa perspetiva mais ampla.

Esta revisão de literatura culminou numa visão consolidada do estado da arte, identificando não só o que o DORA requer, mas também *benchmarks* de como poderia ser implementado com eficácia e quais armadilhas evitar.

Análise de Lacunas (*Gap Analysis*): Com base no quadro de requisitos do DORA levantado na etapa anterior, foi conduzida uma análise de lacunas na seguradora em estudo. Esta análise consiste em:

Mapeamento dos controlos e processos atuais da seguradora relacionados a cada um dos cinco domínios do DORA. Por exemplo, identificar que políticas de segurança de informação já existem, como é feita hoje a gestão de risco operacional e de TI, que procedimentos de resposta a incidentes estão documentados, que mecanismos de backup e recuperação existem, como são geridos os contratos com fornecedores críticos, etc.

Identificação de conformidades e deficiências: Para cada requisito específico do DORA, verificar se a seguradora já o cumpre plenamente, cumpre de forma parcial ou não cumpre de todo. Esta identificação poderá ser facilitada elaborando uma matriz de conformidade, listando os requisitos e evidenciando a situação atual. Onde possível, foram recolhidas evidências comprobatórias (por exemplo, extratos de políticas internas, relatórios de auditoria interna relacionados, etc.) para sustentar a avaliação.

Avaliação do nível de criticidade das lacunas:As lacunas não têm todas o mesmo peso,

foi avaliado o risco associado a cada *gap*, ou seja, qual o potencial impacto para a organização se aquele requisito não estiver implementado, bem como o esforço estimado para supri-lo. Isso permite priorizar as áreas de foco. Por exemplo, se se identificasse que não existe um procedimento formal de notificação de incidentes graves à autoridade de supervisão (conforme exige o DORA), essa lacuna teria alta prioridade por implicações regulatórias; se faltar uma política escrita em determinado tema, mas existir uma prática informal robusta, talvez seja menor a prioridade, embora ainda precise ser endereçada.

Benchmarking interno: Caso possível, comparar a maturidade observada na seguradora com eventuais referências do setor (por exemplo, se houver dados publicados sobre níveis médios de preparação de seguradoras para o DORA). Isso permite contextualizar se a organização está alinhada à média ou se há áreas que estão muito aquém do que seria esperado.

O resultado desta fase foi um diagnóstico estruturado indicando "onde estamos" vs. "onde precisamos chegar" em termos de conformidade DORA. Este diagnóstico inicial e objetivo é um passo fundamental recomendado por especialistas para enfrentar o DORA, pois fornece clareza sobre os *gaps* e orienta a elaboração do plano de ação.

Sugestão da Framework de Implementação (Recomendações): De posse da lista de lacunas e pontos de melhoria, a próxima etapa foi desenvolver as soluções e medidas necessárias para que a seguradora alcance a conformidade e fortaleça sua resiliência digital. Esta fase constitui a contribuição central da tese e envolverá:

Definição de ações corretivas ou de melhoria para cada lacuna identificada. Por exemplo, se há ausência de uma função formal de risco de TIC, recomendar a criação dessa função, definindo suas atribuições e posicionamento na estrutura organizacional; se existem ferramentas insuficientes de monitorização, sugerir a aquisição ou desenvolvimento de capacidades adicionais; se os planos de continuidade não contemplam cenários de ciberataques, propor a revisão dos planos incluindo tais cenários e testes periódicos.

Prioritização e *roadmap*: Organizar as recomendações numa sequência lógica e exequível, considerando *quick wins* (ações de baixo esforço e alto impacto que podem ser implementadas rapidamente) e iniciativas de longo prazo. Será elaborado um plano de implementação faseado, possivelmente distribuído em trimestres ou fases, dado que o DORA entrou em vigor em janeiro de 2025 – por exemplo, recomendar a conclusão das ações críticas até

essa data e planeamento de melhorias contínuas posteriormente.

Integração com*frameworks*existentes: Para cada recomendação, indicar como ela se relaciona com boas práticas reconhecidas. Por exemplo, se a recomendação é implementar um *Security Information and Event Management* (SIEM) para deteção de incidentes, apontar alinhamento com controles do NIST (detetar) ou ISO 27001 (monitorização); se é treinar a equipa em resposta a incidentes, relacionar com as diretrizes da CERT.PT ou ENISA. Essa integração reforça a validade das recomendações e mostra que a empresa não estará a "reinventar a roda", mas sim a aproveitar soluções testadas.

Consideração de recursos e benefícios: Cada iniciativa recomendada virá acompanhada de comentários sobre os recursos necessários (humanos, financeiros, tecnológicos) e sobre os benefícios esperados. Esta sub-etapa é importante para justificar as recomendações face à gestão da empresa,demonstrando o *business case*de investir nessas melhorias. Por exemplo, implementar testes de penetração regulares terá um custo, mas o benefício é reduzir a probabilidade de incidentes graves e evitar perdas financeiras ou multas, e esse balanço foi discutido.

Validação das recomendações: Embora o método não inclua formalmente entrevistas estruturadas, pretendeu-se validar algumas recomendações através de discussões informais com especialistas internos da seguradora (como responsáveis de TI ou de risco, caso acessíveis). Essas interações, ainda que não caracterizadas como entrevistas formais, serviram para verificar a viabilidade prática das medidas teses e ajustar detalhes conforme a realidade operacional da empresa. Alternativamente, a validação pode ser feita confrontando as recomendações com incidentes passados (reais ou simulações) para verificar se resolveriam ou mitigariam aqueles casos.

O produto final desta etapa foi uma *framework* de implementação do DORA adaptado à seguradora estudada – essencialmente um conjunto organizado de linhas de orientação, controlos e processos a adotar, acompanhados de um plano de execução. Este *framework*funcionará como um *blueprint* que a seguradora poderá seguir para atingir a conformidade e, mais do que isso, para instituir uma governação de resiliência operacional robusta e sustentável.

Avaliação dos Resultados e Benefícios: Com as recomendações delineadas, a tese procede a uma análise do impacto esperado dessas medidas na organização. Parte-se do

pressuposto de que a implementação do framework sugerido irá elevar o nível de maturidade em cibersegurança da seguradora. Para evidenciar isso é utilizada alguma forma de avaliação de maturidade antes e depois (mesmo que simulada/projetada, já que a implementação real pode extrapolar o tempo da tese). Por exemplo, recorrendo a um modelo para mostrar quais domínios passariam do nível atual para um nível superior após as mudanças.

Relacionar as melhorias com os riscos mitigados: fazer um exercício teórico de como ficaria o perfil de risco da seguradora pós-implementação. Se inicialmente havia, por exemplo, alto risco de não deteção de um incidente, mostrar que com as medidas de monitorização implementadas esse risco se reduz substancialmente.

Destacar os benefícios qualitativos e quantitativos: qualitativamente, mencionar a robustez de processos, clareza de responsabilidades, cumprimento regulatório evitando multas; quantitativamente, se possível, mencionar redução esperada de custos com indisponibilidade (estimando, por exemplo, que melhorar o tempo de recuperação de sistemas pode poupar X euros por hora de indisponibilidade evitada) ou evitar perdas financeiras por fraude informática.

Comparar a situação da seguradora com melhores práticas do setor: argumentar que as recomendações a colocam num patamar de excelência comparável ao de organizações líderes em resiliência (por exemplo, alinhada com o que bancos de topo fazem, dado que bancos tradicionalmente investem mais em cibersegurança).

Esta avaliação serve para consolidar a ideia de que cumprir o DORA não é apenas um *tick the box compliance*, mas que traz ganhos tangíveis. É também uma forma de verificar se os objetivos iniciais da tese foram atendidos – nomeadamente, identificar desafios e oportunidades, e propor soluções que efetivamente melhoram a segurança e criam valor.

Generalização das descobertas: Por fim, a tese considera em que medida as lições e o framework desenvolvido podem ser generalizados ou adaptados para outras seguradoras ou instituições financeiras. São discutidos quais aspetos são específicos daquela organização e quais são aplicáveis de forma mais ampla. Idealmente, o resultado da tese poderá servir como referência para outras seguradoras portuguesas que busquem orientação para se adequarem ao DORA, respeitando as devidas diferenças de porte e contexto. Essa discussão reforça a relevância do trabalho no panorama setorial e não apenas para o caso

singular estudado.

Em termos de abordagem metodológica, importa mencionar que o trabalho adota uma postura orientada para as soluções e prática, focada em produzir um plano/framework útil para a organização. Não se trata de uma pesquisa puramente teórica; pelo contrário, é um projeto inserido numa necessidade real e atual da empresa e do setor. Os métodos escolhidos (revisão, análise de lacunas, estudo de caso) são adequados para compreender profundamente o problema e desenvolver uma solução customizada, garantindo que a perspetiva das partes interessadas (administração, equipas técnicas, etc.) seja considerada implicitamente na análise.

3.3 Relevância da gestão de risco/controlo de cibersegurança

Em cibersegurança, gestão de risco refere-se ao processo de identificar, analisar e tratar os riscos que ameaçam os ativos de informação de uma organização. De acordo com o NIST, risco é "uma medida do nível em que uma entidade é ameaçada por uma potencial circunstância ou evento, tipicamente função dos impactos adversos que surgiriam se o evento ocorrer e da respetiva probabilidade"[40]. O CNCS no seu Guia dos Riscos em matérias de Segurança de Informação e Cibersegurança[7] define risco de forma similar, como uma circunstância ou evento com potencial efeito adverso na segurança das redes e sistemas de informação. Em outras palavras, risco é a possibilidade de uma ameaça explorar vulnerabilidades e causar impacto negativo.

Para compreender a relação entre riscos e controlos, é essencial definir formalmente alguns termos-chave. Ameaça é geralmente definida como uma potencial causa de um incidente indesejado que pode resultar em dano a um sistema ou organização. Vulnerabilidade refere-se a uma fraqueza de um ativo ou controle que pode ser explorada por uma ou mais ameaças. Por sua vez, um controlo (ou contramedida) é qualquer medida – técnica ou organizacional – destinada a modificar (reduzir) o risco. Em suma, ameaças exploram vulnerabilidades, gerando riscos; e os controlos são implementados para mitigar esses riscos, reduzindo a vulnerabilidade ou o impacto potencial [7][45].

A figura 3.1, baseada em um modelo do CNCS (Centro Nacional de Cibersegurança)

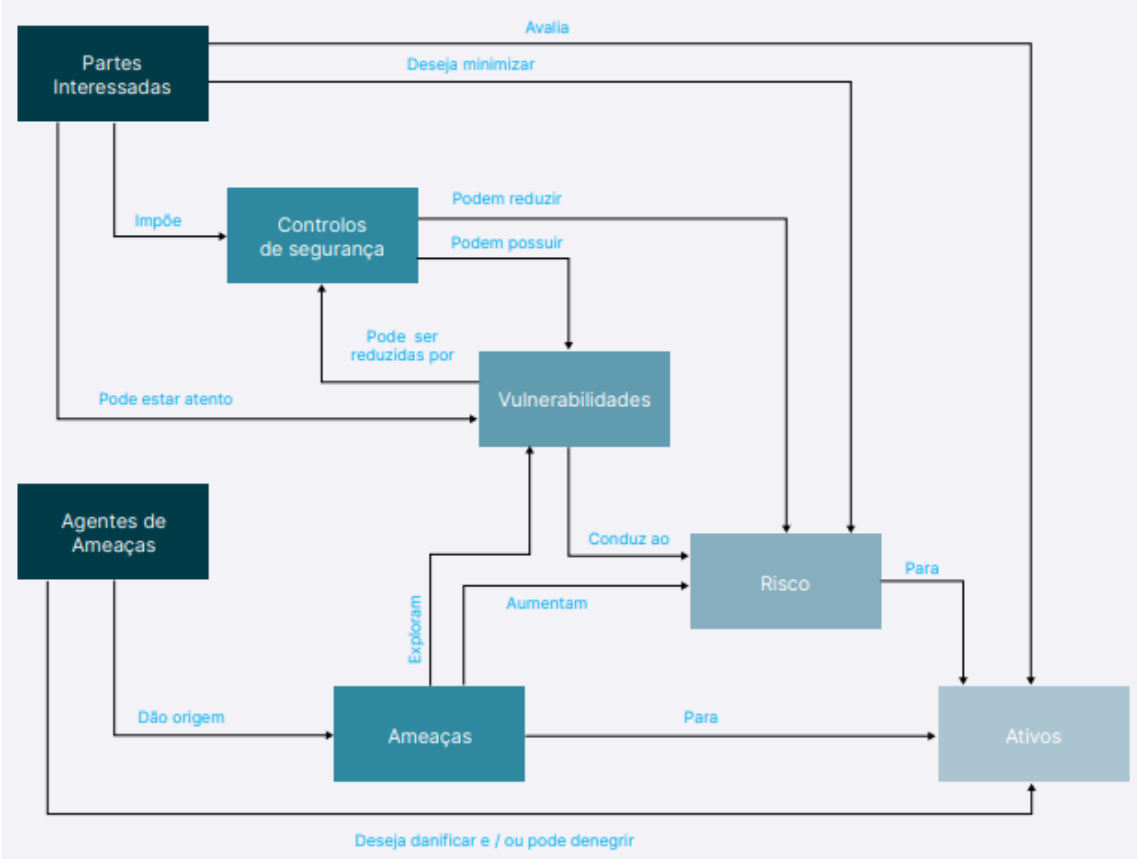

Figura 3.1: Conceitos e Relações Alto Nível CNCS - Guia de Riscos

adaptado da norma ISO/IEC 15408-1, ilustra as interações de alto nível entre os conceitos de segurança.Como representado,os Agentes de ameaça (ameaças ativas, como cibercriminosos ou *malware*) desejam abusar ou danificar os ativos da organização e, para isso, dão origem a ameaças específicas. Essas ameaças exploram vulnerabilidades nos ativos, o que conduz à materialização de riscos. Quanto maiores as vulnerabilidades, maior o risco (probabilidade e impacto de incidentes) associado. Por outro lado, as partes interessadas (ex.: gestores de segurança, proprietários dos ativos) desejam minimizar o risco e por isso impõem controlos de segurança. Os controlos, que podem ser procedimentos, políticas ou salvaguardas técnicas, reduzem as vulnerabilidades dos ativos e, consequentemente, reduzem o nível de risco a um patamar aceitável. Este equilíbrio reflete-se também no conceito de apetite de risco: as organizações definem quanta exposição a risco estão dispostas a aceitar, e implementam controlos para que o risco residual fique dentro desse apetite. Em síntese, há uma relação direta de causa e efeito: ameaças e vulnerabilidades aumentam o risco, ao passo que controlos adequadamente selecionados o diminuem, protegendo os

ativos contra danos.

3.3.1 Controlos Processuais vs. Técnicos

É importante notar que os controlos de segurança podem assumir natureza processual (organizacional) ou técnica. Controlos processuais são medidas administrativas, de gestão ou operacionais — por exemplo, políticas de segurança, procedimentos de *backup*, sensibilização e formação em cibersegurança, segregação de funções, auditorias e avaliações de risco periódicas. Já os controlos técnicos (ou lógicos) envolvem soluções tecnológicas implementadas em sistemas e redes — por exemplo, *firewalls*, sistemas de deteção de intrusão, mecanismos de criptografia, controle de acessos lógico, autenticação multifator, etc. Ambos os tipos são fundamentais e complementares: medidas técnicas protegem contra ataques explorando falhas tecnológicas, enquanto medidas processuais asseguram boa governação, conformidade e resposta adequada aos incidentes. As melhores práticas, como as preconizadas pela ISO/IEC 27002 e pelo NIST SP 800-53, abrangem múltiplas camadas de controlos, incluindo controlos físicos, lógicos e administrativos, que em conjunto reduzem significativamente a superfície de risco. Por exemplo, a série NIST 800-53 classifica controlos em categorias como técnicos, de gestão e operacionais, assegurando que haja políticas e procedimentos (gestão) para sustentar as defesas tecnológicas, bem como atividades de monitorização e resposta (operacionais). De forma equivalente, a ISO 27002:2022 agrupa 93 controlos de segurança em domínios que incluem controlos organizacionais, de pessoas, físicos e tecnológicos refletindo essa divisão entre medidas procedimentais e técnicas. Uma abordagem de defesa em profundidade combina todos esses tipos de controlos para cobrir lacunas que um único controlo deixaria expostas.

3.3.2 Mapeamento com Controles ISO 27x e Referenciais de Mercado

AS *frameworks* internacionais de segurança da informação adotam a gestão de risco como princípio orientador para seleção de controlos. A norma ISO/IEC 27001 exige que organizações realizem uma avaliação de riscos e então apliquem tratamento de riscos selecionando controlos apropriados do seu Anexo A (detalhados na ISO/IEC 27002) para mitigar os riscos identificados. Esses controlos ISO abrangem tanto soluções técnicas quanto práticas organizacionais, podendo-se mapear praticamente qualquer contra me-

dida de segurança adotada pela empresa a um controle específico das normas ISO 27x. Por exemplo, um risco de intrusão na rede pode ser tratado implementando controlos correspondentes como *firewall* e sistemas de prevenção de intrusões (controles técnicos) combinados com um processo de monitorização contínua e resposta a incidentes (controle processual), todos eles alinhados a controlos do Anexo A. A Declaração de Aplicabilidade (SoA), exigida pela ISO 27001, faz explicitamente essa ponte: lista os controlos aplicáveis e justifica sua inclusão como tratamento para riscos identificados.

Organizações do setor financeiro também utilizam frequentemente *frameworks* complementares, como o COBIT (ISACA), que mapeia objetivos de controlo de TI aos riscos de negócio. O COBIT 5/2019, por exemplo, possui processos dedicados à gestão de risco (APO12 –*Manage Risk*) e governação de risco (EDM03 –*Ensure Risk Optimization*), assegurando que o risco de TI não exceda o apetite e tolerância definidos pela organização. Este *framework* auxilia a integrar a gestão de riscos de TI à gestão de riscos corporativos, fornecendo uma visão holística e orientada a processos. Adicionalmente, o Risk IT (também da ISACA) e publicações como *COBIT 5 for Risk* fornecem categorias de cenários de risco e orientações de mitigação específicas, facilitando o mapeamento de riscos a controlos e garantindo cobertura dos riscos emergentes (por ex., riscos de terceiros, falhas de conformidade, ameaças internas, etc.). Em paralelo, o NIST desenvolveu um *Risk Management Framework* (RMF) que vincula as etapas de avaliação de risco à seleção de controlos de segurança (referenciados no NIST SP 800-53). Esse RMF, muito adotado nos EUA, define que as organizações devem categorizar os sistemas, selecionar controlos baseados no impacto (mapeando para um catálogo predefinido), implementar e avaliar esses controlos, autorizando o sistema somente quando o perfil de risco estiver dentro do aceitável, e monitorizando continuamente os riscos e controlos ao longo do ciclo de vida. Apesar das diferenças de abordagem e terminologia, há um alinhamento considerável entre NIST, ISO e ISACA: todos defendem que a gestão de risco deve ser contínua e integrada aos processos de negócio, e que a implementação de controlos apropriados é a chave para tratar riscos de segurança de informação.

3.3.3 Importância da Gestão de Risco no Setor de Seguros e Contexto Regulatório (DORA e NIS2)

No contexto de cibersegurança em seguradoras, a gestão de risco e controlo assume uma relevância crítica. As seguradoras lidam com dados sensíveis e financeiros, estando expostas tanto a ataques informáticos (ex.: roubo de dados de clientes, fraude, *ransomware*) quanto a exigências regulatórias rigorosas de segurança. Regulamentos recentes da UE, como o DORA e a Diretiva NIS2, reforçam explicitamente a necessidade de abordagens robustas de gestão de riscos de TIC nas instituições financeiras, incluindo seguradoras. O DORA, publicado em 2022, enfatiza que as organizações financeiras realizem avaliações regulares de risco e desenvolvam estratégias de gestão de risco abrangentes. Isso inclui identificar e avaliar ameaças emergentes, vulnerabilidades tecnológicas e riscos de terceiros, bem como mitigar esses riscos através de controlos efetivos e estabelecer uma clara apetência/tolerância ao risco operacional digital. Em outras palavras, seguradoras sob DORA devem demonstrar que possuem um sistema contínuo de gestão de riscos de cibersegurança, com controlos proporcionais aos riscos identificados e mecanismos de governação para manter o risco residual dentro de níveis aceitáveis.

De forma semelhante, a Diretiva NIS2 (que atualiza a diretiva NIS original) expande os requisitos de cibersegurança para setores críticos e importantes na Europa, possivelmente abrangendo o setor financeiro e seguradoras de grande porte como entidades "importantes". A NIS2 adota uma abordagem baseada em risco, exigindo que as organizações implementem medidas de segurança proporcionais ao risco e à escala do negócio. Além disso, impõe responsabilidade à gestão de topo pelas decisões de risco: os líderes deverão garantir a existência de políticas e controlos eficazes, e supervisão adequada dos riscos de cibersegurança. A diretiva estabelece que avaliações regulares de risco e relatórios periódicos sejam realizadas, visando melhoria contínua da postura de segurança. Entre as medidas exigidas estão planos de continuidade de negócio, resposta a incidentes, gestão de vulnerabilidades e ciber-higiene, todas baseadas na identificação prévia dos riscos e lacunas de controlo. A não observância dessas práticas de gestão de risco pode acarretar sanções significativas pelos reguladores, dado o potencial impacto sistémico de incidentes em seguradoras (que podem afetar clientes em larga escala e mesmo a estabilidade do setor

financeiro).

Em suma, a gestão de risco e controlo é um pilar central da cibersegurança moderna, fortemente respaldado por normas e *frameworks* reconhecidos (ENISA, CNCS, NIST, ISACA, ISO 27001, etc.) e agora mandatado por regulamentações setoriais. Conforme destaca a ENISA, estabelecer um processo sistemático de gestão de riscos deve ser parte fundamental do programa de cibersegurança de qualquer organização. Todos esses referenciais convergem na mensagem de que identificar riscos e implementar controlos (processuais e técnicos) adequados é essencial para proteger os ativos de informação e assegurar a resiliência operacional. No ambiente de seguradoras – onde a confiança, a proteção de dados pessoais e a continuidade dos serviços são vitais – essa relação entre riscos e controlos ganha ainda mais destaque. A adoção de uma gestão de risco proativa, comparativa (buscando alinhar-se às melhores práticas internacionais) e integrada ao negócio permite às seguradoras não só cumprir DORA e NIS2, mas também fortalecer a sua resiliência em cibersegurança, reduzindo a probabilidade de incidentes de segurança e limitando os impactos caso ocorram. Assim, a organização consegue equilibrar inovação digital com controlo de riscos, assegurando a proteção dos clientes e a estabilidade do setor financeiro em que opera.

3.4 Complexidade de definição de modelo de gestão de risco/controlo de cibersegurança

A crescente sofisticação das ciberameaças e a digitalização intensiva dos serviços tornam a gestão de risco em cibersegurança um imperativo estratégico para as seguradoras. No setor segurador europeu, a definição e operacionalização de modelos de gestão de risco/controlo de cibersegurança enfrenta uma complexidade considerável, derivada tanto do panorama regulatório em rápida evolução quanto da necessidade de integrar controlos técnicos e processuais de forma coerente. As seguradoras armazenam volumes massivos de dados sensíveis de clientes e dependem fortemente de sistemas de informação, o que as coloca entre os alvos prioritários de ataques – por exemplo, de acordo com o relatório da *Cybersecurity Ventures* indicou que em 2023 ocorria um ciberataque a cada 39 segundos,em média [38]. Nesse contexto, os reguladores europeus têm imposto requisitos mais rigorosos

de resiliência em cibersegurança, nomeadamente através do DORA e da Diretiva NIS2, enquanto normas internacionais como a família ISO/IEC 27000 oferecem *frameworks* de melhores práticas.De seguida,analisa-se comparativamente esses referenciais e os desafios específicos que surgem ao aplicá-los no setor segurador, com destaque para a integração de controlos tecnológicos e procedimentais e para limitações operacionais e organizacionais observadas em casos concretos.

Segundo o responsável de Resiliência Operacional da MAPFRE, o DORA não implicará mudança drástica de estratégia pois muitas medidas já existiam, mas exigirá maior formalização e documentação de atividades (por exemplo, o controlo sistematizado de fornecedores externos) [38]. Esta experiência sugere que seguradoras de grande porte com práticas de segurança maduras encaram o DORA como uma consolidação de boas práticas, ao passo que para outras seguradoras de menor dimensão,como é a seguradora do caso em estudo,pode obrigar a melhorias substantivas em processos e sistemas num curto espaço de tempo.

O relatório da EIOPA *Cyber Risk for Insurers Challenges and Oportunities* (2019) identifica o risco de cibersegurança como uma componente crítica do risco operacional no setor segurador, destacando a sua crescente relevância face à digitalização dos serviços financeiros. Este tipo de risco distingue-se pela sua natureza dinâmica, sistémica e de difícil quantificação, exigindo abordagens específicas de gestão. As seguradoras europeias demonstram níveis variados de maturidade na implementação de estruturas de governação para a cibersegurança, sendo que muitas já integram planos de continuidade de negócio e resposta a incidentes. Contudo, a eficácia desses planos depende da sua testagem regular, o que nem sempre ocorre. A avaliação do risco de cibersegurança é dificultada pela escassez de dados históricos e pela rápida evolução das ameaças, o que compromete a modelação precisa de cenários. A implementação de controlos técnicos, como autenticação multifator e segmentação de rede, é prática comum, mas a cultura organizacional e a formação dos colaboradores ainda carecem de reforço. A dependência de terceiros e de serviços em nuvem amplia a superfície de ataque, enquanto a subnotificação de incidentes e a ausência de métricas padronizadas dificultam a monitorização eficaz. A EIOPA recomenda, assim, o fortalecimento da resiliência em cibersegurança, a promoção da transparência e a partilha de boas práticas como pilares fundamentais para a gestão operacional deste risco.

Paralelamente às exigências legais, muitas seguradoras adotam referenciais internacionais de melhores práticas para estruturar a gestão de risco de cibersegurança. No contexto segurador – altamente intensivo em dados pessoais e financeiros – a implementação da ISO 27001 mitiga riscos de ataques e violações de dados, melhora a conformidade regulatória (por exemplo,com RGPD) e fomenta a confiança dos clientes, ao assegurar confidencialidade, integridade e disponibilidade da informação.Embora a ISO 27001 seja valiosa como base para um modelo de gestão de risco de cibersegurança consistente – e ajude na conformidade com DORA e NIS2 – as seguradoras precisam despender recursos significativos para adaptar essas boas práticas à sua realidade operacional, garantindo que o *framework* não fique apenas no papel.

Desafios na Integração de Controlos Técnicos e Processuais

Um dos pontos nevrálgicos na definição de modelos de gestão de risco de cibersegurança é a integração harmoniosa entre controlos técnicos (de natureza tecnológica) e controlos processuais (procedimentos de gestão, políticas e governação). No papel,*frameworks* como DORA e NIS2 exigem simultaneamente medidas técnicas (por exemplo,ferramentas de monitorização, encriptação, autenticação forte, testes de intrusão) e medidas organizacionais (por exemplo,planos de resposta a incidentes, auditorias de risco, formações de sensibilização, governação clara com envolvimento da gestão de topo). Na prática, contudo, muitas seguradoras defrontam-se com lacunas entre a camada tecnológica e a camada procedimental. Um exemplo comum é a gestão de acessos privilegiados: a tecnologia pode implementar controlos de acesso e registo de atividades, mas se não houver um processo bem definido de revisão periódica de privilégios e segregação de funções, as falhas humanas ou de processo podem anular a eficácia técnica. A coordenação entre equipas de TI/cibersegurança e equipas de risco/conformidade nem sempre é fluida, dado que historicamente a segurança da informação era tratada como domínio estritamente tecnológico, enquanto a gestão de riscos operacionais (sobretudo em seguradoras focadas em risco financeiro/atuarial) seguia um percurso separado. Integrar essas vertentes requer mudanças culturais e estruturais – por exemplo, estabelecer governação de cibersegurança com envolvimento da administração e modelo de "três linhas de defesa", de forma que as funções de risco e auditoria interna consigam avaliar objetivamente os controlos técnicos implementados.

Vários obstáculos específicos tornam essa integração desafiante no setor segurador eu-

ropeu. Um deles é a prevalência de sistemas legados e dívida técnica: muitas seguradoras operam há décadas, acumulando plataformas de TI obsoletas ou altamente customizadas, nas quais faltam funcionalidades modernas de segurança ou mesmo compatibilidade com padrões atuais. Esses *legacy systems* podem não suportar controlos técnicos essenciais (como criptografia forte ou registos avançados de log), deixando a empresa vulnerável apesar de políticas bem-intencionadas. Atualizar ou substituir tais sistemas é complexo e oneroso, exigindo investimento significativo e podendo gerar resistência interna por impactar operações de negócio críticas. Outro fator é a forte dependência de terceiros: serviços *cloud*, softwares de parceiros, provedores de processamento, entre outros. Estima-se que 88% das seguradoras contam com provedores externos para funções-chave, o que amplia a superfície de ataque. Mesmo que a seguradora tenha controlos internos robustos, uma falha de segurança num fornecedor pode expor dados ou interromper serviços – daí a importância de processos rigorosos de *Third-Party Risk Management*(TPRM) alinhados aos controlos técnicos (ex.: avaliação de segurança dos fornecedores, exigências contratuais de conformidade com normas, etc.) [39].

Do ponto de vista operacional e organizacional, destacam-se limitações significativas de recursos e competências que dificultam a aplicação eficaz dos modelos de controlo de cibersegurança no setor segurador. Muitas seguradoras enfrentam orçamentos restritos para áreas de TI e cibersegurança, especialmente num contexto em que precisam simultaneamente investir em inovação digital e modernização tecnológica. A escassez de talento qualificado agrava este cenário: estima-se que existam mais de 2,8 milhões de vagas não preenchidas na área de cibersegurança a nível global, sendo o setor financeiro um dos mais afetados [35]. Encontrar profissionais experientes, como *Chief Information Security Officers*-(CISOs), é apontado como um dos principais desafios iniciais para instituições que buscam elevar sua maturidade em segurança da informação.

Essa carência de especialistas pode resultar numa implementação fragmentada de *frameworks* de segurança: por exemplo, políticas de segurança podem ser formalizadas em documentos, mas não aplicadas de forma eficaz nas ferramentas operacionais; ou tecnologias avançadas podem ser adquiridas, mas subutilizadas por falta de pessoal capacitado para operá-las [10]. Além disso, dificuldades na mudança cultural interna não devem ser subestimadas. Um modelo de gestão de risco de cibersegurança eficaz requer envolvimento

e adesão de todos os níveis hierárquicos da organização. A promoção de uma cultura de segurança, por meio de programas de sensibilização e formação contínua, é essencial — tal como previsto em normas como a ISO/IEC 27001 e reforçado por regulamentos como o DORA e a diretiva NIS2. No entanto, mobilizar os colaboradores a adotarem práticas seguras no dia a dia continua a ser um desafio comportamental persistente [37].

Por fim, vale notar que organismos supervisores têm reconhecido essa complexidade e a necessidade de maior harmonização de *frameworks*. A EIOPA (European Insurance and Occupational Pensions Authority), autoridade europeia para seguros, realçou a necessidade de requisitos claros e comuns de governação de cibersegurança no setor, incluindo definições consistentes de riscos e incidentes, para evitar interpretações díspares e inconsistências nos reportes que hoje dificultam uma resposta coordenada [22].

Esta observação sugere que, antes do DORA/NIS2, as seguradoras seguiam abordagens heterogéneas – algumas baseadas em ISO, outras em guidelines nacionais – levando a lacunas de eficácia. Iniciativas recentes, como a criação de fóruns de partilha de informação de ciberameaças, também reforçam a integração entre controlos técnicos (monitorização de ameaças) e processuais (cooperação e resposta conjunta).

Em resumo, a definição de um modelo de gestão de risco de cibersegurança é uma atividade complexa e multifacetada. Ela requer navegar múltiplos referenciais regulatórios e normativos, conciliando os objetivos de cada um (resiliência operacional do DORA, segurança de redes da NIS2, boas práticas ISO) num único sistema de controlo. Além disso, impõe superar dificuldades práticas na integração entre tecnologia e processos, garantindo que ferramentas de segurança, políticas internas e estruturas de governação atuem em uníssono.

A resposta efetiva passa por investir numa combinação de soluções técnicas e capacitação humana, aliando compliance regulatória com melhoria contínua de processos, de forma a construir uma verdadeira resiliência em cibersegurança nas seguradoras.

Capítulo 4

Hipótese de solução

Antes de se avançar para a análise da aplicação prática do regulamento DORA no contexto da seguradora em estudo, é fundamental estabelecer um enquadramento conceptual claro que permita compreender a interligação entre os principais elementos da gestão de segurança da informação: ativos, ameaças, vulnerabilidades, riscos e controlos.

Este entendimento encontra-se formalizado nas normas internacionais ISO 27001 — que definem os requisitos para implementação de um Sistema de Gestão de Segurança da Informação (SGSI) — e ISO 27005, dedicada à gestão de risco de segurança da informação. A adoção destas normas como referência metodológica permite assegurar coerência, rastreabilidade e robustez analítica às práticas adotadas. Além disso, estabelece uma base sólida para a integração com os requisitos de resiliência operacional digital impostos pelo DORA.

Lógica de Interdependência

Tal como representado na Figura 4.1, os elementos mencionados estabelecem entre si uma cadeia lógica de dependência, essencial para a construção de qualquer modelo eficaz de gestão de risco:

- **Ativos**: São todos os elementos que têm valor para a organização — desde sistemas de informação, dados, aplicações críticas e infraestrutura tecnológica, até pessoas com funções sensíveis ou acesso privilegiado.

- **Ameaças**: Representam potenciais causas de incidentes, como ciberataques, erros humanos, falhas técnicas ou eventos naturais.

- **Vulnerabilidades**: Correspondem a fragilidades exploráveis nos ativos, podendo ser de natureza técnica (ex.: software desatualizado), organizacional (ex.: ausência de segregação de funções) ou humana (ex.: falta de sensibilização).

- **Riscos**: Surgem da combinação entre uma ameaça e uma vulnerabilidade que afeta um ativo, provocando um impacto adverso para a organização. A ISO/IEC 27005 sintetiza esta relação pela seguinte fórmula:

$$\text{Risco} = \text{Ameaça} \times \text{Vulnerabilidade} \times \text{Impacto no Ativo}$$

- **Controlos**: São as salvaguardas implementadas com o objetivo de mitigar riscos, reduzindo a sua probabilidade de ocorrência ou impacto. Podem ser técnicos (como firewalls ou soluções EDR), organizacionais (como segregação de funções) ou procedimentais (como políticas de backup ou de gestão de acessos).

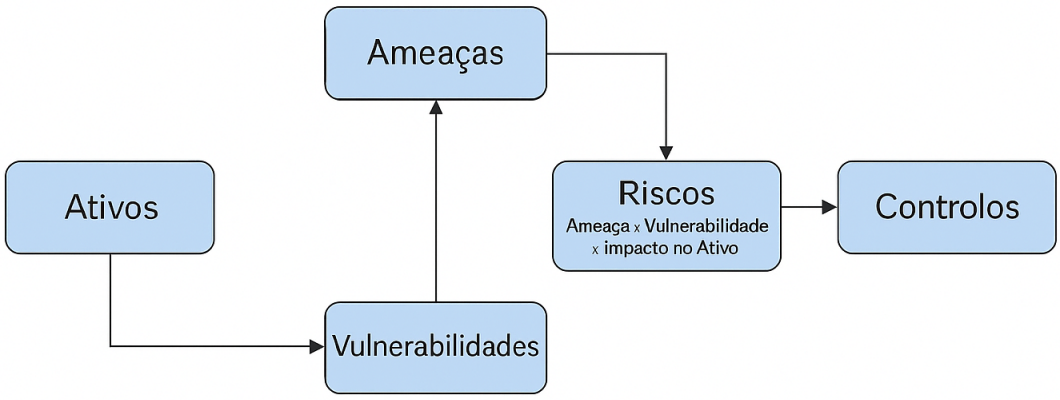

Figura 4.1: Relação entre ativos, ameaças, vulnerabilidades, riscos e controlos segundo ISO/IEC 27001, 27005 e DORA

O reconhecimento e a análise estruturada destas inter-relações é essencial para a definição de uma metodologia de gestão de risco eficaz e alinhada com os princípios do DORA. Esta abordagem orientará a análise desenvolvida nos subcapítulos seguintes

(4.1 a 4.5), permitindo mapear riscos, ativos e respetivos controlos de forma coerente com os objetivos de resiliência operacional e conformidade regulatória.

4.1 Aplicação do modelo DORA a seguradoras

A aplicação do modelo DORA nas seguradoras é um processo complexo que requer uma compreensão profunda dos requisitos regulatórios e das especificidades do setor segurador. O DORA foi concebido para aumentar a resiliência operacional digital das entidades financeiras, incluindo as seguradoras, e inclui cinco domínios principais: gestão de riscos de TIC, gestão de incidentes de TIC, testes de resiliência operacional digital, gestão de riscos de TIC de terceiros e partilha de informação sobre ciberameaças.

A sua implementação nas seguradoras deve começar com uma avaliação detalhada dos riscos de TIC. Esta avaliação deve incluir a identificação dos ativos de informação críticos, a avaliação das vulnerabilidades e ameaças associadas a esses ativos, e a definição de medidas de mitigação de riscos. A ISO 27001 e o NIST Cybersecurity Framework fornecem diretrizes úteis para a gestão de riscos de TIC, incluindo a identificação de ativos, a avaliação de riscos e a implementação de controlos de segurança.

A gestão de incidentes de TIC é outro componente crítico do DORA. As seguradoras devem implementar processos eficazes de deteção, resposta e recuperação perante incidentes que afetem a segurança ou funcionamento dos sistemas de informação. Isso inclui a implementação de capacidades de monitorização e *logging*, bem como procedimentos de escalonamento interno. A ISO 27035 fornece diretrizes para a gestão de incidentes de segurança da informação, incluindo a preparação, deteção, análise, resposta e lições aprendidas.

Os testes de resiliência operacional digital são essenciais para avaliar a eficácia dos controlos de segurança implementados. As seguradoras devem realizar testes periódicos aos seus sistemas e controlos de segurança, incluindo análises de vulnerabilidades e testes de penetração. A ISO 27001 e o NIST Cybersecurity Framework

fornecem diretrizes para a realização de testes de segurança, incluindo a definição de objetivos de teste, a seleção de métodos de teste e a avaliação dos resultados.

A gestão de riscos de TIC de terceiros é um componente crítico do DORA, dado que as seguradoras dependem crescentemente de fornecedores externos de tecnologia. As seguradoras devem avaliar os riscos de TIC associados a cada fornecedor crítico, garantir que cláusulas contratuais específicas estejam presentes e monitorizar continuamente o desempenho e a conformidade dos terceiros com essas obrigações. A ISO 27036 fornece diretrizes para a gestão de segurança da informação em relações com fornecedores, incluindo a seleção de fornecedores, a definição de requisitos de segurança e a monitorização do desempenho dos fornecedores.

A partilha de informação sobre ciberameaças é encorajada pelo DORA como uma forma de promover uma inteligência coletiva no setor financeiro. As seguradoras devem partilhar informações sobre ameaças, vulnerabilidades, técnicas de ataque e incidentes com outras entidades financeiras. A ENISA e o CNCS fornecem diretrizes para a partilha de informação sobre ciberameaças, incluindo a definição de protocolos de partilha de informação e a proteção da confidencialidade das informações partilhadas.

Em resumo, a aplicação do modelo DORA nas seguradoras requer uma abordagem integrada que abranja a gestão de riscos de TIC, a gestão de incidentes de TIC, os testes de resiliência operacional digital, a gestão de riscos de TIC de terceiros e a partilha de informação sobre ciberameaças. A adoção de normas e boas práticas internacionais, como a ISO 27001, o NIST Cybersecurity Framework, a ISO 27035, a ISO 27036 e as diretrizes da ENISA e do CNCS, pode ajudar as seguradoras a cumprir os requisitos do DORA e a fortalecer a sua resiliência operacional digital.

4.2 Controlos DORA

Os controlos DORA consistem num conjunto abrangente de medidas e procedimentos destinados a garantir a resiliência operacional digital das entidades financeiras, incluindo seguradoras. Estes controlos estão organizados em cinco domínios princi-

pais, conforme previsto no:

- Gestão de riscos de TIC: abrange a governação de riscos tecnológicos e a implementação de um enquadramento de gestão de risco robusto para os ativos de informação e sistemas de TIC. Inclui a identificação de ativos e riscos, avaliação de vulnerabilidades e impactos, implementação de controlos de mitigação, monitorização contínua e melhoria do programa de riscos. No âmbito deste domínio, o DORA especifica, por exemplo, que a instituição deve possuir um quadro de gestão de risco de TIC sólido e documentado, realizar periodicamente análises de risco abrangentes e sujeitar a gestão de risco a auditorias internas regulares para garantir a eficácia e conformidade. A formação e sensibilização em matéria de riscos de TIC também faz parte deste domínio, assegurando que membros da direção e colaboradores conhecem as políticas e assumem as suas responsabilidades no controlo de riscos.
- Gestão, classificação e comunicação de incidentes relacionados com as TIC: concentra-se em estabelecer capacidades para detetar e responder a incidentes de segurança e falhas operacionais, bem como classificar a sua gravidade e comunicar informação sobre incidentes graves. As seguradoras devem ter um processo formal de gestão de incidentes de TIC, cobrindo desde a deteção precoce (por meio de ferramentas de monitorização e alerta) até à resposta e recuperação. Incidentes são classificados por níveis de gravidade (por ex. menor, significativo, grave) de acordo com critérios de impacto previstos pelo regulador. Para incidentes considerados graves nos termos do DORA, é obrigatória a notificação às autoridades de supervisão no prazo estipulado (normalmente dentro de 24 horas após deteção) e a submissão de relatórios detalhados subsequentes. Devem também existir procedimentos para comunicar incidentes relevantes aos clientes afetados e para manter registos de todos os incidentes ocorridos. A adoção de normas como a ISO/IEC 27035 apoia este domínio, fornecendo orientações sobre preparação e resposta a incidentes, enquanto as diretrizes do regulamento estabelecem os requisitos mínimos de reporte e conteúdo dessas notificações.

– Testes de resiliência operacional digital: diz respeito a um programa de testes periódicos destinados a validar a robustez dos sistemas e dos controlos de segurança face a diferentes cenários de risco. Segundo o DORA, as entidades financeiras devem realizar, pelo menos anualmente, testes de resiliência operacional abrangentes. Estes testes incluem avaliações de vulnerabilidades, testes de penetração e simulações de interrupções significativas, cobrindo tanto infraestruturas de TIC como procedimentos de resposta. Além disso, para entidades de maior porte ou relevância sistémica, o regulamento introduz os TLPT (*Threat-Led Penetration Tests*) – testes de penetração orientados por ameaça – que simulam ataques avançados e coordenados. Esses testes avançados devem ser conduzidos por equipas qualificadas e independentes (internas ou externas), seguindo requisitos rigorosos de escopo (abrangendo funções críticas), metodologia e confidencialidade, e os resultados devem ser documentados ecomunicados à gestão de topo e às autoridades, acompanhados de planos de correção. A existência de inspetores independentes ou auditores para verificar a qualidade dos testes é outra exigência do DORA. Normas como a ISO/IEC 27001 e *frameworks* como o NIST CSF oferecem boas práticas para estruturar programas de teste, enquanto o regulamento detalha critérios específicos para sua implementação.

– Gestão do risco de terceiros nas TIC: foca-se nos riscos decorrentes da dependência de prestadores de serviços de TIC. As seguradoras devem adotar princípios de *due diligence* e gestão de risco para terceiros, garantindo que riscos de concentração ou dependência excessiva sejam considerados antes de contratar serviços externos. O DORA exige que as empresas mantenham uma lista atualizada de todos os fornecedores de TIC críticos ou importantes e que avaliem periodicamente o desempenho e riscos de cada um. Deve existir uma estratégia de riscos de terceiros integrada no quadro geral de risco da organização. Em termos contratuais, as entidades financeiras precisam assegurar que os contratos com fornecedores de TIC incluam disposições obrigatórias relativas à segurança e resiliência: por exemplo, conformidade com normas de segurança da informação, direito de acesso e auditoria às instalações e sistemas

do fornecedor, direito de rescisão dos contratos em casos de falhas graves ou incumprimentos, e requisitos para cooperação do fornecedor em caso de incidentes (incluindo notificações de incidentes que os afetem). Adicionalmente, o regulamento obriga a planos de estratégia de saída (*exit strategy*) para serviços terceirizados críticos, de modo que a empresa possa transferir ou encerrar esses serviços sem interrupção significativa caso o contrato termine inesperadamente. A monitorização contínua e a revisão periódica destes acordos fazem parte do ciclo de gestão de terceiros. As diretrizes da ISO/IEC 27036 complementam estes controlos, abordando boas práticas de gestão de segurança em relações com fornecedores.

– Acordos de partilha de informação sobre ciberameaças: cobre a cooperação entre entidades financeiras para troca de informação relevante sobre ameaças, ataques e vulnerabilidades, com vista a aumentar a consciência situacional coletiva e prevenir incidentes. O DORA autoriza e incentiva as instituições a estabelecer acordos de partilha de informação voluntária, desde que respeitados os limites legais (por exemplo, concorrência, proteção de dados) e garantida a confidencialidade das informações partilhadas. Esse intercâmbio pode ocorrer através de plataformas setoriais, centros de partilha de informação (como ISACs) ou parcerias facilitadas pelos reguladores. Embora seja voluntária, a partilha de informação é vista como uma boa prática para fortalecer a resiliência do ecossistema financeiro como um todo. Recomenda-se que as seguradoras definam protocolos internos para avaliar e disseminar informações recebidas (por exemplo, alertas de vulnerabilidades críticas ou *indicators of compromise*) e para contribuir com dados de incidentes próprios quando apropriado. Entidades como a ENISA e o CNCS fornecem recomendações sobre como estruturar essas parcerias de forma segura.

Em suma, os controlos DORA abrangem um conjunto extenso de requisitos que vão desde governação e gestão de risco de TIC, passando pela prontidão e comunicação em caso de incidentes, pela robustez da arquitetura tecnológica testada regularmente, até à gestão rigorosa de fornecedores e colaboração inter-organizacional em cibersegurança. A adoção de normas e boas práticas inter-

nacionais (ISO 27001, ISO 27002, ISO 27005, NIST CSF, entre outras) em conjunto com o cumprimento estrito dos requisitos DORA permite às seguradoras construir uma resiliência digital sólida e demonstrável, em conformidade com as exigências regulatórias.

4.3 Controlos face a riscos e ativos SI/TI

Os controlos implementados para mitigar riscos em ativos de Sistemas de Informação (SI) e Tecnologias de Informação (TI) são fundamentais para garantir a segurança e a resiliência operacional das seguradoras. Esses controlos devem ser aplicados de forma a endereçar os riscos identificados nos ativos e a proteger dados e sistemas críticos contra ameaças. A seguir, apresentam-se as principais etapas e medidas de controlo que relacionam riscos de TIC com os ativos de SI/TI, conforme a *framework* DORA e as melhores práticas de gestão de risco:

- Identificação e inventário de ativos e processos: O primeiro passo é identificar todos os ativos de informação (dados, sistemas, infraestruturas, aplicações) e os processos de negócio dependentes de TIC, bem como atribuir-lhes proprietários e classificá-los segundo a sua criticidade e sensibilidade. Segundo o DORA, as entidades devem manter um inventário atualizado desses ativos e processos, identificando quais são críticos ou importantes para as funções da organização. Por exemplo, uma seguradora deve catalogar as suas bases de dados de apólices, servidores de aplicações core, redes internas, plataformas em *cloud*, etc., indicando o nível de impacto caso cada item seja comprometido ou indisponível. A ISO/IEC 27001 e ISO/IEC27002 fornecem diretrizes para classificação de informação e gestão de ativos, o que complementa os requisitos do regulamento.
- Identificação de ameaças e vulnerabilidades: Paralelamente ao inventário de ativos, procede-se à identificação contínua das ameaças relevantes (ex.:*malware*, *phishing*, fraude interna, falhas de energia) e das vulnerabilidades nos sistemas (ex.: software desatualizado, configurações fracas). O DORA enfatiza que a

empresa deve considerar uma variedade de fontes de risco de TIC – internas e externas – ao avaliar o seu panorama de risco. Isso inclui riscos emergentes, como novas ciberameaças, e riscos de terceiros (falhas ou ataques em fornecedores críticos). A combinação de ativos, ameaças e vulnerabilidades identificados fornece a base para a próxima etapa de avaliação de riscos. Ferramentas automatizadas de varrimento de vulnerabilidades,*threat intelligence*e auditorias de segurança ajudam a cumprir este controlo de forma consistente.

- Avaliação de riscos: Com base nos dados anteriores, a seguradora deve realizar avaliações formais de risco, determinando a probabilidade e o impacto de diferentes cenários de risco sobre cada ativo ou processo. Conforme o DORA, essas avaliações devem ser documentadas e atualizadas regularmente, refletindo mudanças no ambiente de TI ou no negócio. Por exemplo, um risco avaliado pode ser"indisponibilidade do sistema de gestão de apólices devido a ataque de *ransomware*", com certa probabilidade e impacto financeiro/reputacional estimado. A ISO/IEC 27005 e a ISO 31000 fornecem metodologias para análise de riscos que podem ser aplicadas aqui. O resultado desta etapa é uma matriz de riscos ou lista de riscos priorizados – indicando quais riscos são inaceitáveis, quais requerem tratamento imediato e quais podem ser assumidos (aceites) pela organização.
- Definição de medidas de mitigação e controlos: Para cada risco identificado que exceda o apetite/tolerância definido pela organização, devem ser implementadas medidas de mitigação adequadas. Os controlos de segurança selecionados devem corresponder aos riscos – por exemplo, para mitigar o risco de acesso não autorizado a dados sensíveis, implementa-se um controlo de autenticação multifator e reforçam-se os controlos de acesso; para mitigar risco de perda de dados, estabelecem-se rotinas de backup e recuperação; contra *malware*, instalam-se soluções de antivírus e filtragem de conteúdo. O DORA exige que o quadro de gestão de riscos inclua uma variedade de controlos de segurança técnicos, organizacionais e processuais, e que estes sejam proporcionais à criticidade dos ativos. Adicionalmente, controlos preventivos como políticas de segurança da

informação documentadas e gestão de configurações - *patches* são necessários para diminuir vulnerabilidades conhecidas. Normas como a ISO/IEC 27001 e o NIST Cybersecurity Framework oferecem catálogos de controlos possíveis (controlo de acessos, criptografia, segurança física, segurança de redes, treino de utilizadores, etc.) que podem ser adotados conforme aplicável.

- Implementação e integração dos controlos: Os controlos selecionados devem ser implementados na arquitetura de segurança da empresa (detalhada no ponto 4.4) e integrados aos processos de negócio. Isso inclui configurar ferramentas de segurança (*firewalls*, sistemas de deteção de intrusão,SIEMs, etc.), atualizar procedimentos operacionais (por exemplo, processo de gestão de mudanças de TI incorporando verificações de segurança) e promover a adesão dos colaboradores às novas práticas (através de formação e consciencialização). O sucesso dessa etapa depende de uma boa gestão de projetos de segurança, apoio da gestão de topo e coordenação entre equipas de TI, segurança e unidades de negócio.
- Monitorização e revisão contínua: Após implementados, os controlos devem ser monitorizados continuamente para assegurar que estão eficazes e que os riscos permanecem dentro dos níveis aceitáveis. O DORA exige que as seguradoras realizem revisões periódicas do seu quadro de controlo de TIC, incluindo auditorias internas independentes e testes dos controlos chave. Por exemplo, podem ser conduzidos scans regulares de vulnerabilidades para verificar se as medidas de *patchmanagement* estão a funcionar, ou exercícios simulados para testar o plano de resposta a incidentes. Quando são detetadas falhas ou lacunas – como um controlo que não bloqueou um incidente ou um risco emergente não coberto – a organização deve acionar mecanismos de correção e melhoria contínua. Isso pode implicar atualizar políticas, reforçar determinados controlos, ou até reavaliar riscos com novas premissas. A cultura de aprendizagem organizacional é importante aqui: cada incidente ou teste fornecem insights para aperfeiçoar o ambiente de controlo.*Frameworks*como a ISO/IEC 27001 enfatizam o ciclo PDCA (*Plan-Do-Check-Act*) justamente para promover essa retro-alimentação

e melhoria constante no SGSI (Sistema de Gestão de Segurança da Informação). Em síntese, alinhar os controlos com os riscos e ativos SI/TI significa personalizar as medidas de segurança à realidade da seguradora, concentrando recursos de proteção onde o impacto potencial é maior. Seguindo os requisitos do DORA e as boas práticas reconhecidas, a seguradora consegue reduzir a probabilidade e impacto de incidentes, melhorar a visibilidade sobre o seu risco de cibersegurança e assegurar que, mesmo se ocorrerem eventos adversos, as consequências para os clientes e operações sejam minimizadas.

4.4 Controlos DORA na arquitetura de segurança

A implementação dos controlos DORA na arquitetura de segurança das seguradoras é essencial para garantir tanto a resiliência operacional digital quanto a proteção eficaz dos ativos de informação. A arquitetura de segurança deve ser projetada de forma a integrar os controlos exigidos pelo DORA em todos os níveis – desde a infraestrutura de TI básica, passando pelas aplicações empresariais, até aos processos de negócio e governação.

Um primeiro componente da arquitetura de segurança é a definição de políticas e princípios de segurança da informação que orientam todo o desenho arquitetural. A seguradora deve estabelecer uma Política de Segurança da Informação corporativa, aprovada pela gestão de topo, que alinhada com os requisitos do DORA e normas como a ISO/IEC 27001 defina os objetivos de segurança, as responsabilidades e as diretrizes para proteção dos ativos. Esta política serve de base para a arquitetura, garantindo que haja coerência entre os controlos técnicos implementados e as exigências de conformidade/regulamentares.

Em termos de infraestrutura tecnológica, a arquitetura de segurança deve incorporar controlos de proteção em várias camadas (segundo o princípio de defesa em profundidade). Dentre os controlos técnicos que devem ser implementados, destacam-se:

- Segurança de rede: utilização de *firewalls* para filtrar o tráfego não autorizado, sistemas de deteção e prevenção de intrusões (IDS/IPS) para identificar ati-

vidades maliciosas e segmentação de rede para isolar segmentos críticos (por exemplo, separando a rede interna da rede pública e segmentando ambientes de produção, teste e administração. Esses controlos reduzem a superfície de ataque e limitam a propagação de incidentes caso ocorram.

- Criptografia e proteção de dados: adoção de criptografia robusta para dados sensíveis, tanto em repouso (armazenados em bases de dados, discos, backups) quanto em trânsito (comunicações de rede, transações web). O uso de protocolos seguros (TLS,VPNs) e a gestão adequada de chaves de cifra são fundamentais para prevenir acessos não autorizados a informações confidenciais, em conformidade com as diretrizes do DORA de proteger a integridade e confidencialidade dos dados.
- Controlo de acessos e identidade: implementação de mecanismos de autenticação forte, como autenticação multifator (MFA) para utilizadores privilegiados e acesso remoto, e uma rigorosa gestão de identidades e acessos (IAM). Políticas de controlo de acesso baseadas em privilégio mínimo devem ser aplicadas, garantindo que cada utilizador ou sistema somente acede aos recursos necessários para as suas funções. Adicionalmente, é recomendado o uso de soluções de gestão de acessos privilegiados (PAM) para monitorizar e controlar sessões administrativas em sistemas críticos.
- Segurança de aplicações: as aplicações, sobretudo as desenvolvidas internamente, devem seguir princípios de "*security by design*". Isto envolve incorporar verificações de segurança ao longo do ciclo de desenvolvimento de software (SDLC) – por exemplo, realizar análises de código estático, testes de penetração em aplicações web/mobile antes de entrarem em produção, e assegurar a correção tempestiva de vulnerabilidades identificadas. O DORA, embora não mencione explicitamente cada medida de desenvolvimento seguro, exige que as entidades tomem medidas para prevenir e detetar falhas nos seus sistemas TIC. A norma ISO/IEC 27034 traz linhas de orientação para segurança em desenvolvimento de software, complementando os controlos DORA neste aspeto.
- Gestão de configurações e mudanças: estabelecer processos rigorosos de gestão

de mudanças de TI que incluam avaliação de risco e testes antes de alterações em sistemas críticos. Controlos como gestão de*patches*e atualizações de software regulares são cruciais – o DORA requer que as entidades tenham políticas documentadas para assegurar que softwares e sistemas sejam mantidos atualizados e livre de falhas conhecidas. Ferramentas de automação de *patch management* e configuração segura (por exemplo, aplicação de*baseline security hardening*) devem fazer parte da arquitetura para reduzir a incidência de configurações inseguras.

Além dos controlos preventivos e de proteção, a arquitetura de segurança deve incluir capacidades de deteção e resposta bem integradas. Isso significa implementar monitorização contínua dos sistemas e redes – tipicamente através de um *Security Operations Center*(SOC) ou função equivalente – utilizando soluções de correlação de eventos (SIEM) para detetar rapidamente padrões de ataque ou anomalias. Quando um incidente é detetado, devem existir controles de contenção e resposta (como sistemas de isolamento de *hosts* comprometidos,procedimentos de emergência pré-definidos) para limitar o dano. Conforme salientado pelo DORA, a capacidade de deteção e resposta a incidentes é tão importante quanto a prevenção, devendo ser testada regularmente (por meio de simulacros e testes de cenário) para garantir sua eficácia.

Ao nível dos processos de negócio, a arquitetura de segurança deve garantir a continuidade das operações mesmo em face de incidentes graves. Assim, integra-se na arquitetura planos e procedimentos de continuidade de negócio e recuperação de desastres (BCP/DRP) específicos para cenários de falhas de TIC. O DORA obriga as instituições a estabelecer planos de continuidade das atividades de TIC e de recuperação que sejam adequados e testados periodicamente. Tais planos incluem arranjos de redundância (sites alternativos, backups *off-site*), procedimentos manuais de contingência, prioridades de recuperação e estratégias de comunicação de crise. A norma ISO 22301 (Gestão da Continuidade de Negócio) e a ISO/IEC 27031 fornecem padrões para desenvolver e integrar estes planos na organização, em consonância com os controlos DORA.

Finalmente, é imprescindível instituir a monitorização e revisão contínua da arquitetura de segurança. As seguradoras devem avaliar regularmente se os controlos arquiteturais permanecem eficazes face à evolução das ameaças e mudanças no ambiente de TI. Isso envolve auditorias periódicas de segurança, testes de intrusão independentes e revisões pós-incidente que alimentam melhorias na arquitetura. O DORA espera que as entidades financeiras adotem um ciclo de melhoria contínua, revendo políticas, procedimentos e controlos à luz dos resultados de testes e incidentes (por exemplo, atualizando a arquitetura para cobrir uma nova ameaça que se materializou).*Frameworks* como o NIST CSF destacam a importância dessa função de feedback, garantindo que a arquitetura de segurança não seja estática, mas sim adaptativa e resiliente.

Em resumo, a incorporação dos controlos DORA na arquitetura de segurança assegura que os requisitos regulatórios não fiquem apenas no plano teórico, mas sim materializados em medidas técnicas e organizacionais concretas dentro do ambiente de TI da seguradora. Ao seguir uma abordagem estruturada – políticas claras, infraestrutura protegida em camadas, aplicações seguras, processos robustos de mudança, deteção e resposta eficientes, e planos de continuidade – a organização fortalece a sua postura de segurança e cumpre simultaneamente as obrigações de resiliência digital impostas pelo regulador.

No anexo 'Controlos de Implementação DORA', o estudo foi convertido num *roadmap* prático composto por 108 controlos, que servirão como guia para a jornada de implementação do regulamento. Este conjunto de controlos permitirá monitorizar e avaliar de forma estruturada a maturidade alcançada ao longo do processo.

4.5 Metodologia de gestão de risco com DORA

A metodologia de gestão de risco com alinhamento ao DORA é um processo estruturado que visa identificar, avaliar, mitigar e monitorizar os riscos de Tecnologias de Informação e Comunicação (TIC) nas seguradoras, integrando-se na gestão de risco global da organização. Essa metodologia apoia-se nos princípios tradicionais

de gestão de risco (como os da ISO 31000 e ISO/IEC 27005), mas incorpora explicitamente os controlos e exigências do DORA para assegurar resiliência operacional. Podemos delinear a metodologia em quatro etapas principais, em consonância com o ciclo de vida do risco de TIC:

1. Identificação dos riscos de TIC: Nesta fase, compila-se um inventário de riscos potenciais que possam afetar os ativos e processos de TIC da seguradora. Conforme descrito no ponto 4.3, identifica-se os ativos críticos e respetivos pontos fracos, bem como ameaças relevantes (internas ou externas). O DORA reforça a necessidade de incluir todos os riscos significativos de TIC, abrangendo não só falhas tecnológicas e ataques informáticos, mas também riscos oriundos de terceiros (ex.: falhas de fornecedores) e riscos emergentes. Ferramentas de análise de risco, como listas de verificação e bases de dados de cenários de risco (por ex. catálogos de riscos de TIC conhecidos), podem ser usadas para não omitir fatores importantes. O resultado é uma listagem abrangente de eventos de risco possíveis – por exemplo,*ransomware* em sistemas core, indisponibilidade de *datacenter*, violação de dados pessoais, indisponibilidade de fornecedor *cloud*, erro humano em configuração crítica, entre outros.
2. Avaliação e análise dos riscos de TIC: Cada risco identificado é então avaliado em termos de probabilidade de ocorrência e impacto potencial. Esta análise pode ser qualitativa (atribuição de níveis como Alto/Médio/Baixo) ou quantitativa, consoante a maturidade da organização, mas deve seguir critérios coerentes aprovados pela gestão (por exemplo, definição do que constitui um impacto alto em termos financeiros,reputacionais, legais). O DORA espera que as entidades conheçam o seu apetite e tolerância ao risco de TIC, isto é, o nível de risco que estão dispostas aaceitar, e utilizem essa referência para priorizar as ações. Riscos com probabilidade/impacto acima do tolerável serão marcados para tratamento. A avaliação também considera interdependências – por exemplo, um risco de falha de um fornecedor de TI pode ter impacto multiplicado se esse fornecedor suportar vários processos críticos (risco de concentração). Devem ser atribuídas classificações de risco inerente e residual, de modo a distinguir

o nível de risco antes e depois dos controlos existentes. Técnicas da ISO/IEC 27005 podem ser aplicadas aqui, incluindo fórmulas de cálculo de risco ou matrizes de probabilidade vs. impacto. É importante documentar os resultados – muitas vezes sob a forma de um relatório de avaliação de riscos de TIC – e submeter à apreciação do órgão de gestão de riscos ou comité de risco da seguradora.

3. Tratamento (mitigação) dos riscos de TIC: Para os riscos inaceitáveis identificados, define-se um plano de tratamento de risco, que especifica as ações de mitigação a serem implementadas, responsáveis e prazos. As opções de tratamento alinhadas ao DORA incluem: implementar ou reforçar controlos de segurança (tecnológicos ou processuais), transferir o risco (por exemplo, contratando seguros que cobrem riscos de cibersegurança ou terceirizando serviços sob acordos rigorosos), eliminar o risco (por exemplo, descontinuando um sistema vulnerável) ou aceitar formalmente o risco (somente se dentro do apetite e após avaliação). O foco principal, contudo, recai na implementação de controlos compensatórios eficazes para reduzir a probabilidade e/ou impacto.

Como descrito no ponto 4.3, esses controlos podem variar desde melhorias na arquitetura de segurança (*firewalls*, *backups*, redundâncias) até iniciativas de fortalecimento de processos (treinamentos, revisão de procedimentos).

O DORA exige que o órgão de direção esteja envolvido na aprovação das medidas de mitigação mais importantes, assegurando alocação de recursos suficiente para implementá-las. Uma vez implementadas as medidas, reavalia-se o risco residual para verificar se foi reduzido a um nível aceitável. Toda a fase de tratamento deve estar bem documentada, incluindo as justificativas para medidas adotadas ou para eventuais aceitações de risco, de forma a demonstrar conformidade regulatória.

Monitorização e revisão dos riscos de TIC: A última etapa da metodologia é contínua: envolve monitorizar a exposição aos riscos ao longo do tempo e rever periodicamente tanto os riscos identificados quanto a eficácia dos controlos implementados. O DORA enfatiza a necessidade de monitorização contínua – por exemplo, através de indicadores de risco-chave (KRIs) que sinalizam aumento de risco, como número de incidentes

de determinado tipo, grau de cumprimento dos níveis de serviço (SLA)de fornecedores, etc. – e de auditorias regulares para avaliar se o processo de gestão de risco de TIC permanece adequado. Além disso, requer-se que as empresas realizem um reexame global anual do seu quadro de gestão de risco de TIC, incorporando quaisquer mudanças (novos projetos, novas ameaças, alterações regulatórias). Incidentes ocorridos servem de lições aprendidas: por exemplo, um ataque bem-sucedido pode indicar que certos riscos estavam subestimados ou que os controlos eram insuficientes, exigindo revisão dos documentos de avaliação e adoção de controlos adicionais. A melhoria contínua é, portanto, inerente à metodologia – o processo de gestão de risco deve evoluir e amadurecer com o tempo.

A governação também faz parte desta etapa: os resultados da monitorização (relatórios de estado de risco, falhas de controlo identificadas, planos de ação pendentes) devem ser reportados à gestão de topo e discutidos em fóruns de risco, garantindo *accountability* e apoio para manter a resiliência alinhada ao DORA.

Em conclusão, a metodologia de gestão de risco com DORA integra-se ao sistema de gestão da seguradora como um ciclo dinâmico de identificação, avaliação, mitigação e monitorização de riscos de TIC. A adoção dessa metodologia, alinhada às normas internacionais (ISO 31000, ISO 27005, etc.) e reforçada pelos requisitos específicos do DORA, assegura que a organização não só cumpra o regulamento, mas também que desenvolva uma capacidade resiliente frente aos desafios tecnológicos atuais. Essa gestão proativa e sistemática dos riscos de TIC permite antecipar ameaças, minimizar perdas em caso de incidente e criar uma cultura organizacional onde a resiliência operacional digital é parte integrante do negócio.

Capítulo 5

Conclusões

Neste capítulo são apresentadas as conclusões finais do estudo, com base na análise desenvolvida e nos resultados obtidos. São sintetizados os principais contributos da investigação, as implicações práticas da implementação do DORA numa seguradora do ramo Vida e as oportunidades de evolução futura, tanto a nível académico como organizacional.

5.1 Trabalho realizado

Esta tese dedicou-se a redefinir o âmbito de um trabalho originalmente voltado para a governação de cibersegurança em seguradoras, orientando-o para os desafios e oportunidades da implementação do Regulamento DORA numa seguradora portuguesa do Ramo Vida. Mantendo a estrutura da proposta inicial, foi possível integrar este novo foco através de:

- introdução contextualizando o tema e a problemática da conformidade com o DORA;
- uma revisão do estado da arte, com análise técnica dos requisitos regulatórios e dos principais desafios identificados em estudos e relatórios setoriais;
- a formulação de uma proposta metodológica adequada à realidade da organização em estudo, com um plano de trabalho faseado;

– a realização de um diagnóstico de maturidade, que permitiu identificar lacunas e definir recomendações práticas.

Todo o trabalho enfatizou não apenas os obstáculos operacionais e tecnológicos, mas também os benefícios de uma implementação eficaz, como a continuidade de negócio, a mitigação de riscos e o aumento da confiança institucional.

5.2 Relevância do tema e principais conclusões

Relevância do tema

A crescente digitalização do setor segurador, associada ao aumento da exposição a ameaças de cibersegurança, tornou a resiliência operacional uma prioridade inadiável. O DORA não representa apenas uma nova obrigação regulatória, mas sim um instrumento transformador da governação tecnológica nas instituições financeiras europeias. No setor segurador português, onde subsistem sistemas legados, dependência de fornecedores críticos e processos ainda parcialmente informais, o cumprimento do DORA assume especial complexidade. Esta tese responde à ausência de estudos práticos e contextualizados sobre a sua implementação, procurando não só contribuir para o avanço académico, mas também fornecer uma referência aplicada para outras seguradoras com desafios semelhantes. Ao abordar de forma integrada os domínios de tecnologia, risco e conformidade, o trabalho destaca-se pela sua utilidade transversal.

Principais Conclusões

Esta tese demonstrou que o DORA opera numa lógica de ciclo de vida completo da resiliência digital — incluindo desde a prevenção (gestão de riscos e arquitetura de segurança), à deteção e resposta (gestão de incidentes), até à recuperação (continuidade de negócio e testes) — impondo um alinhamento estruturado e coerente entre processos, pessoas e tecnologia. Tal abrangência revela a necessidade de uma abordagem transversal por parte das seguradoras, onde a segurança é incorporada nos processos de negócio e não tratada de forma isolada.

O estudo de caso revelou ainda que, apesar de algumas seguradoras já possuírem medidas técnicas razoáveis, existe frequentemente uma lacuna na formalização dos processos, na definição clara de responsabilidades, e na documentação das práticas exigidas pelo regulamento. Isso confirma que o DORA não é apenas mais um regulamento, mas um motor de transformação organizacional profunda — obrigando a rever práticas enraizadas, a investir na maturidade processual e a adotar uma cultura de segurança baseada na melhoria contínua.

5.3 Solução face ao problema de investigação

A implementação do DORA representa um desafio multidisciplinar que abrange tecnologia, processos e pessoas, mas também uma oportunidade única de modernização e robustecimento da gestão de risco digital nas seguradoras. Ao focar nos desafios e propor soluções concretas, esta tese foi de encontro ao duplo propósito de auxiliar a seguradora em estudo a navegar pelas exigências do DORA e de gerar conhecimento aplicado que possa orientar o setor rumo a uma maior resiliência operacional. Assim, o trabalho ambiciona não só cumprir um objetivo acadêmico, mas também deixar um legado prático num momento crucial de transformação da regulação de cibersegurança financeira.

Para responder ao problema identificado — ou seja, como operacionalizar os requisitos do DORA numa seguradora com limitações tecnológicas e organizacionais — foi proposta uma solução prática baseada em um estudo de caso detalhado.

Importa destacar que, conforme o plano proposto no anexo “Controlos de implementação DORA”, a larga maioria dos controlos identificados são de natureza processual. Este aspeto revela uma realidade crítica: o cumprimento do DORA não depende apenas de soluções tecnológicas, mas exige uma mudança profunda na forma de atuar das seguradoras, centrada na criação, formalização e gestão ativa de políticas, processos e mecanismos de governação. Trata-se de uma transformação que envolve toda a organização, desde a administração até aos operadores técnicos, e que impõe uma cultura de segurança contínua e transversal.

Os princípios estruturantes do DORA — nomeadamente a gestão integrada do risco de TIC, a resposta coordenada a incidentes, os testes regulares de resiliência e a supervisão rigorosa dos prestadores de serviços críticos — reforçam a necessidade de uma abordagem proativa e preventiva. Esta exigência é ainda mais premente quando confrontada com a realidade atual, onde eventos recentes, como o apagão que afetou toda a Península Ibérica em abril de 2025, evidenciaram que os planos de continuidade e resposta a incidentes severos ainda não se encontram totalmente preparados para cenários prolongados e de larga escala. Este tipo de ocorrência mostra que a coordenação entre entidades públicas e privadas, bem como a robustez dos mecanismos internos de resposta, são fatores determinantes para a estabilidade e segurança do setor financeiro.

5.4 Linhas de Investigação Abertas

Embora o DORA seja já aplicável, muitos dos seus efeitos ainda estão por materializar. Esta tese abre caminho a várias linhas de investigação futuras, como:

•Avaliação comparativa da implementação do DORA entre diferentes tipos de entidades financeiras (ex.: bancos versus seguradoras);

•Análise do papel das autoridades supervisoras nacionais na harmonização da supervisão em contexto europeu;

•Investigação sobre o impacto do DORA na contratação e supervisão de prestadores críticos de TIC fora da UE.

•Avaliação específica de enquadramento do DORA face a ISO 27001, NIST, CIS Controls e outras referências de Cibersegurança, e de segurança de informação de forma mais abrangente.

Assim, a proposta apresentada nesta tese não constitui apenas uma resposta regulamentar, mas sim um modelo de evolução organizacional, orientado por princípios de maturidade, melhoria contínua e alinhamento com os riscos emergentes. Ao promover esta transformação, a *framework* proposta poderá servir como referência para outras seguradoras e contribuir para uma resiliência operacional efetiva, sustentável

e alinhada com os objetivos do DORA.

Referências

[1] Accenture. "Cyber Resilience in Insurance: Operating Models and Technology Trends". Em: *Accenture*. Accenture, jun. de 2023.

[2] M. Corrêa de Aguiar. "Intervenção no Fórum Nacional de Seguros 2023". Em: *ASF*. ASF, jul. de 2023.

[3] ASF. "Boletim de Supervisão Comportamental". Em: *Lisboa*. ASF, jun. de 2023.

[4] ASF. "Relatório de Estabilidade Financeira do Setor Segurador". Em: *Lisboa*. ASF, jun. de 2023.

[5] ASF. "Relatório de Estabilidade Financeira do Setor Segurador". Em: *Lisboa*. ASF, jun. de 2023.

[6] M. Child, R. Helkenberg e D. Bindels. "NIS2 Readiness: A Guide for Organizations in Europe". Em: *InfoBrief patrocinado pela Microsoft, IDC EUR252440224*. IDC, jul. de 2024. URL: `https://www.idc.com`.

[7] Centro Nacional de Cibersegurança (CNCS). "Guia de Riscos em Matéria de Segurança da Informação e Cibersegurança". Em: 2021. URL: `https://www.cncs.gov.pt`.

[8] Conselho Nacional de Cibersegurança (CNCS). "Estratégia Nacional de Segurança do Ciberespaço 2019-2023". Em: *Lisboa, Portugal*. CNCS, jun. de 2019.

[9] CNCS. "Guia de Boas Práticas para a Cibersegurança no Setor Financeiro". Em: *Lisboa, Portugal*. Acesso em: 17-Set-2024. CNCS, jun. de 2023. URL: `https://www.cncs.gov.pt`.

[10] McKinsey Company. “The unsolved opportunities for cybersecurity providers”. Em: 2024. URL: https://www.mckinsey.com.

[11] Parlamento Europeu e Conselho da UE. “Decreto-Lei n.º 22/2025, de 19 de março — Transpõe a Diretiva (UE) 2022/2557”. Em: *Parlamento Europeu e Conselho da UE*. Parlamento Europeu e Conselho da UE, mar. de 2025.

[12] Parlamento Europeu e Conselho da UE. “Diretiva (UE) 2022/2555”. Em: *JO L 333*. Parlamento Europeu e Conselho da UE, dez. de 2022.

[13] Parlamento Europeu e Conselho da UE. “Diretiva (UE) 2022/2555”. Em: *Art. 21.º, n.º 2*. Parlamento Europeu e Conselho da UE, dez. de 2022.

[14] Parlamento Europeu e Conselho da UE. “Diretiva (UE) 2022/2555”. Em: *Art. 34.º*. Parlamento Europeu e Conselho da UE, dez. de 2022.

[15] Parlamento Europeu e Conselho da UE. “Diretiva (UE) 2022/2555”. Em: *Considerando 82*. Parlamento Europeu e Conselho da UE, dez. de 2022.

[16] Parlamento Europeu e Conselho da UE. “Regulamento (UE) 2022/2554 (DORA)”. Em: *JO L333*. Parlamento Europeu e Conselho da UE, dez. de 2022.

[17] IBM Corporation. “Layered defense approach to security”. Em: *IBM Documentation*. URL: https://www.ibm.com/docs/pt-br/i/7.5.0.

[18] Industrial Cyber. “EU Commission adopts initial cybersecurity rules to enhance critical digital infrastructure resilience”. Em: *Industrial Cyber*. Industrial Cyber, out. de 2024.

[19] EIOPA EBA ESMA. “Joint Guidelines on ICT and security risk management”. Em: *EBA, ESMA, EIOPA*. EBA, ESMA, EIOPA, jun. de 2020.

[20] Frontier Economics. “Implications of New Cyber Security Measures in Portugal”. Em: *Estudo encomendado pela Huawei*. Frontier Economics, abr. de 2024. URL: https://www.frontier-economics.com.

[21] EIOPA. “Big Data Analytics in Motor and Health Insurance”. Em: *Frankfurt*. EIOPA, jun. de 2023.

[22] EIOPA. “Cyber Risk for Insurers – Challenges and Opportunities”. Em: *Publications Office of the EU*. 2019. URL: https://www.eiopa.europa.eu.

[23] EIOPA. “Digital Operational Resilience Act (DORA): Regulatory Framework for the Financial Sector”. Em: *EIOPA*. Acesso em: 15-Jan-2025. EIOPA, jun. de 2024. URL: https://www.eiopa.europa.eu.

[24] EIOPA. “Discussion Paper on Open Insurance”. Em: *EIOPA-BoS-21/400*. EIOPA, jan. de 2021.

[25] EIOPA. “ESAs publish second batch of policy products under DORA”. Em: *EIOPA*. Acesso em: 19-Fev-2025. EIOPA, jul. de 2024. URL: https://www.eiopa.europa.eu/esas-publish-second-batch-policy-products-under-dora-2024-07-17_en.

[26] EIOPA. “Guidelines on outsourcing to cloud service providers”. Em: *EIOPA-BoS-20/002*. EIOPA, fev. de 2020.

[27] EIOPA. “Solvency II Guidelines on System of Governance”. Em: *Frankfurt, Alemanha*. Acesso em: 06-Ago-2024. EIOPA, jun. de 2021. URL: https://www.eiopa.europa.eu.

[28] ENISA. “Cybersecurity Frameworks for Financial Sector”. Em: *European Union Agency for Cybersecurity (ENISA)*. Acesso em: 15-Mar-2025. ENISA, jun. de 2024. URL: https://www.enisa.europa.eu.

[29] ENISA. “Threat Landscape 2023 – Ransomware and Data Breaches”. Em: *European Union Agency for Cybersecurity (ENISA)*. Acesso em: 08-Jul-2024. ENISA, jun. de 2023. URL: https://www.enisa.europa.eu.

[30] Insurance Europe. “Harnessing the power of digitalisation in insurance”. Em: 2022. URL: https://www.insuranceeurope.eu/digitalisation/.

[31] Insurance Europe. “Strengthening the industry’s cyber resilience – Insights into the implementation of the Digital Operational Resilience Act (DORA)”. Em: *Insurance Europe*. Insurance Europe, jun. de 2024. URL: https://insuranceeurope.eu/news/3275.

[32] Comissão Europeia. “Cibersegurança das redes e dos sistemas de informação (2022)”. Em: *EUR-Lex Summaries of EU Legislation*. Dez. de 2022, pp. 221–227.

[33] Comissão Europeia. "Rede EU-CyCLONe – Digital Strategy". Em: *Comissão Europeia*. Comissão Europeia, jun. de 2023.

[34] Comissão Europeia. "Shaping Europe's Digital Future – NIS2 Directive". Em: *Comissão Europeia*. Comissão Europeia, jun. de 2023.

[35] Fortinet. "2024 Cybersecurity Skills Gap Global Research Report". Em: jan. de 2024. URL: https://www.fortinet.com.

[36] Infoblox. "NIS2 "for Dummies": Demystifying Directive (EU) 2022/2555". Em: *Infoblox*. Infoblox, jun. de 2023.

[37] ISACA. "Resilience and Security in Critical Sectors: Navigating NIS2 and DORA Requirements". Em: 2025. URL: https://www.isaca.org.

[38] MAPFRE. "Here's what the mandatory DORA regulation for insurance companies and fund managers entails". Em: *MAPFRE Insights*. Abr. de 2024. URL: https://www.mapfre.com.

[39] Alvarez Marsal. "Cyber Threats: The Challenges of Digital Transformation in the Insurance Industry". Em: set. de 2024. URL: https://www.alvarezandmarsal.com.

[40] NIST. "Glossary of Key Information Security Terms". Em: *NIST IR 7298 Rev. 3*. NIST, jul. de 2019. URL: https://csrc.nist.gov/glossary.

[41] EY Portugal. "Insurance Outlook 2023 – Digitalizar para competir". Em: *Lisboa*. EY, jun. de 2023.

[42] EY Portugal. "Modelo de Governo para a Cibersegurança". Em: *Lisboa, Portugal*. EY, jun. de 2024. URL: https://www.ey.com.

[43] A. C. Pylant. "Initiating a Collaborative Cybersecurity Governance Framework at the State Level". Em: *West Chester University*. West Chester University, jun. de 2020.

[44] Amazon Web Services. "Operational Best Practices for ENISA Cybersecurity Guide for SMEs". Em: URL: https://docs.aws.amazon.com.

[45] National Institute of Standards e Technology (NIST). "Glossary of Key Information Security Terms". Em: *NIST Interagency/Internal Report (IR) 7298 Revision 3*. Jul. de 2019. URL: https://csrc.nist.gov/glossary.

[46] Autoridade de Supervisão de Seguros e Fundos de Pensões (ASF). "Relatório de Estabilidade Financeira do Setor Segurador 2024". Em: *Lisboa, Portugal*. Acesso em: 15-Mar-2025. ASF, jun. de 2024. URL: https://www.asf.com.pt.

Apêndice A

Controlos DORA por Dominio

Domínio	Âmbito	Tipo de Controlo	Controlo
Gestão de Risco TIC			
	Organização e Governação		
		Processual	Quadro de governo e controlo
		Processual	Implementação da gestão de riscos e razoabilidade da gestão
		Processual	Considerações e aplicação da CIAA
		Processual	Funções e responsabilidades
		Processual	Estratégia de Resiliência Operacional Digital (DOR)
		Processual	Planos de Continuidade das Atividades TIC e Planos de Resposta e Recuperação
		Processual	Planeamento Auditoria Interna
		Processual	Orçamento
		Processual	TIC Revisão de terceiros
		Processual	Canais de comunicação
		Processual	TIC Função de gestão de riscos por terceiros
		Processual	Formação em matéria de riscos
		Processual	Recursos de gestão do risco das TIC
		Processual	Auditoria das autoridades - Pedidos relacionados com os riscos
		Processual	Independência do gestor de riscos
		Processual	Análise e relatório da gestão do risco das TIC
		Processual	Melhoria contínua
		Processual	Auditoria Interna
		Processual	Verificação e correção
		Processual	Estratégia DOR: conteúdo
		Processual	TIC Estratégia multifornecedor
		Processual	Externalização da conformidade
		Ambos	Requisitos de sistemas, protocolos e ferramentas TIC
	Identificação		
		Ambos	Inventário das operações TIC
		Processual	Fontes de riscos das TIC
		Processual	Avaliação dos Riscos
		Processual	Inventário dos activos de informação e TIC(CMDB)
		Processual	Inventário dos processos TIC
		Ambos	Revisão de modificação de inventário
		Ambos	Revisão anual da avaliação de risco específica das TIC
	Proteção e Prevenção		
		Processual	Sistemas TIC: monitorizar e controlar
		Processual	Políticas de segurança das TIC
		Ambos	Adequação das TIC
		Processual	Política de Segurança da Informação
		Ambos	Gestão de redes e infraestruturas
		Ambos	Controlo de Acesso
		Ambos	Política de Autenticação
		Ambos	Controlo das Alterações das TIC
		Processual	Gestão de Patches
	Deteção		
		Tecnico	Deteção de incidentes TIC
		Tecnico	Mecanismos de deteção de incidentes
		Ambos	Monitorização de incidentes
		Tecnico	Deteção de incidentes DRSP
	Resposta e Recuperação		
		Processual	Política de Continuidade das Atividades das TIC
		Processual	Política de Continuidade das Atividades de TIC: conteúdo mínimo
		Processual	Plano de resposta e recuperação das TIC
		Ambos	Política de continuidade das atividades de TIC: manutenção e testes
		Processual	Processo de Análise do Impacto nas Empresas (BIA)
		Ambos	Teste do PCN Continuidade e resposta
		Ambos	Teste de PCN: Cenários
		Ambos	Teste de PCN: Comunicação em caso de crise
		Processual	Revisão dos planos de continuidade das atividades e de resposta e recuperação
		Processual	Papel da Gestão de Crises

Domínio	Âmbito	Tipo de Controlo	Controlo
Gestão de Risco TIC			
	Resposta e Recuperação		
		Processual	Manutenção de Registos
		Processual	Requisitos das centrais de depósito de títulos
		Processual	Comunicação dos custos e perdas de incidentes relacionados com as TIC
	Políticas e procedimentos de cópia de segurança, procedimentos e métodos de restauro e recuperação		
		Processual	Sistemas TIC e restauro da informação
		Tecnico	Ativação de sistemas de reserva
		Tecnico	Requisitos dos sistemas de cópia de segurança
		Ambos	Planos de recuperação para contrapartes centrais
		Tecnico	Instalações de reserva e de restauro(Disaster Recovery e processamento secundário)
		Tecnico	Capacidades redundantes de TIC
		Tecnico	Local de processamento secundário(Datacenter Secundário)
		Processual	RTO e RPO
		Ambos	Recuperação de incidentes relacionados com as TIC
	Aprendizagem e evolução		
		Ambos	Conhecimentos de segurança da informação: capacidades e pessoal
		Processual	Análise Pós-Incidente
		Processual	Comunicação de alterações Pós-Incidente
		Processual	Repositório de lições aprendidas no processo de avaliação do risco das TIC
		Processual	Acompanhamento da Estratégia de Resiliência Operacional Digital
		Processual	Relatórios sobre lições de incidentes relacionados com as TIC
		Processual	Sensibilização para a segurança e formação DOR
		Processual	Acompanhamento dos desenvolvimentos tecnológicos relevantes
	Comunicação		
		Processual	Processo de comunicação de crise e Politica de Comunicação
Gestão, classificação e comunicação de incidentes relacionados com as TIC			
	Processo de gestão de incidentes TIC		
		Processual	Processo de gestão de incidentes relacionados com as TIC
	Classificação dos incidentes e das ciberameaças relacionados com as TIC		
		Processual	Classificação de Incidentes
		Processual	Classificação das ciberameaças
	Relatórios		
			Comunicação de incidentes graves relacionados com as TIC
			Relatórios Voluntários
			Comunicação com os clientes
			Comunicação de conteúdos mínimos
			Externalização de Relatórios
Teste de Resiliência Operacional Digital			
	Requisitos gerais para a realização dos testes DOR		
		Processual	Teste de Resiliência Operacional Digital
		Processual	Considerações sobre os riscos dos testes DOR
		Processual	Inspetor Independente
		Processual	Prioridade, classificação e correção dos resultados dos testes
		Processual	Testes Anuais
	Teste de ferramentas e sistemas TIC		
		Processual	Especificações dos Testes
	Testes avançados de ferramentas, sistemas e processos TIC baseados em TLPT		
		Processual	Testes avançados TLPT
		Processual	Áreas de teste TLPT
		Processual	Âmbito de aplicação do TLPT: Prestador de serviços de TIC a terceiros
		Processual	Envolvimento de terceiros nas TIC em TLPT
		Processual	Cooperação na Gestão dos Riscos e na aplicação dos controlos
		Processual	Relatório de constatações, correcções e documentação
		Processual	Comunicação de atestado TLPT
		Processual	Requisitos dos inspetores
	Requisitos para os técnicos de controlo para a realização de TLPT		
		Processual	Requisitos do TLPT

Domínio	Âmbito	Tipo de Controlo	Controlo
Teste de Resiliência Operacional Digital			
	Requisitos para os técnicos de controlo para a realização de TLPT		
		Processual	Requisitos internos de TLPT
		Processual	Requisitos do contrato TLPT
Gestão do risco de terceiros nas TIC			
	Risco de terceiros nas TIC: princípios		
		Processual	Base de riscos de terceiros em TIC
		Processual	Estratégia de riscos para terceiros nas TIC
		Processual	Acordos contratuais com terceiros nas TIC: registo de informações
		Processual	Avaliação por terceiros das TIC
		Processual	Requisitos de InfoSec de terceiros para TIC
		Processual	Direito de acesso, inspeção e auditoria de terceiros nas TIC
		Processual	Direitos de rescisão de terceiros nas TIC
		Processual	Estratégia de saída apoio aos serviços TIC
	Avaliação preliminar do risco de concentração das TIC		
		Processual	Antecedentes e considerações contratuais de terceiros nas TIC
	Principais disposições contratuais		
		Processual	Principais disposições contratuais relativas a terceiros nas TIC
		Processual	TIC de terceiros (funções críticas ou importantes) disposições contratuais adicionais
Acordos de partilha de informação			
	Acordos de partilha de informação		
		Processual	Acordos de partilha de informações sobre ameaças cibernéticas e informações

Apêndice B

Descritivo de controlos - DORA

Controlo	Descrição Resumida
Quadro de governo e controlo	A seguradora deve ter um quadro de governo e de controlo interno que garanta uma gestão eficaz e prudente do risco TI, a fim de alcançar um elevado nível de resiliência operacional digital.
Implementação da gestão de riscos e razoabilidade da gestão	A Administração da Seguradora define, aprova, supervisiona e é responsável pela aplicação de todas as disposições relacionadas com o quadro de gestão do risco das TIC. A Administração da seguradora dever ser a responsável pela aprovação da gestão de risco TIC da Seguradora
Considerações e aplicação da CIAA	Deverá ser definido políticas que visem garantir a manutenção de elevados padrões de disponibilidade, autenticidade, integridade e confidencialidade dos dados.
Funções e responsabilidades	A Administração deve definir claramente os funções e as responsabilidades de todas as funções relacionadas com as TIC e estabelecer mecanismos de governação adequados para garantir uma comunicação, cooperação e coordenação eficazes e atempadas entre essas funções.
Estratégia de Resiliência Operacional Digital (DOR)	A Administração é globalmente responsável pela definição e aprovação da estratégia de resiliência operacional digital referida no (estratégia DOR), incluindo a determinação do nível adequado de tolerância ao risco de TIC da Seguradora, tal como referido na estratégia DOR.
Planos de Continuidade das Atividades TIC e Planos de Resposta e Recuperação	A Adminsração deve aprovar, supervisionar e rever periodicamente a aplicação da política de continuidade das atividades das TIC da Seguradora e dos planos de resposta e recuperação das TIC, referidos, respetivamente, política de continuidade das atividades das TIC) e plano de resposta e recuperação das TIC, que podem ser adotados como uma política específica que faça parte integrante da política global de continuidade das atividades e do plano de resposta e recuperação da Seguradora.
Planeamento Auditoria Interna	A Administração aprova e revê periodicamente os planos de auditoria interna das TIC da Seguradora, as auditorias das TIC e as alterações materiais que lhes sejam introduzidas.
Orçamento	A Administração atribui e revê periodicamente o orçamento adequado para satisfazer as necessidades de resiliência operacional digital da Seguradora no que diz respeito a todos os tipos de recursos, incluindo os programas relevantes de sensibilização para a segurança das TIC e a formação em resiliência operacional digital referida no (Sensibilização para a segurança e formação em DOR) e as competências em TIC para todo o pessoal.
TIC Revisão de terceiros	A Administração aprova e revê periodicamente a política da Seguradora em matéria de acordos relativos à utilização de serviços TIC fornecidos por terceiros prestadores de serviços TIC.
Canais de comunicação	A Administração da seguradora deve assegurar a existência de canais de informação formais, estruturados e contínuos que lhe permitam ser devidamente informada e exercer supervisão eficaz sobre a gestão de riscos decorrentes da contratação de prestadores de serviços terceiros de TIC. Esses canais devem garantir o reporte claro, tempestivo e completo sobre: (i) Os acordos celebrados com terceiros para a utilização de serviços de TIC, incluindo contratos com prestadores externos ou entidades subcontratadas; (ii) Quaisquer alterações materiais relevantes planeadas nesses acordos, como substituição de fornecedores, mudanças de infraestrutura, migrações para ambientes cloud, ou modificações contratuais com impacto em níveis de serviço; (iii) O impacto potencial dessas alterações sobre as funções críticas ou importantes da seguradora abrangidas pelos acordos, devendo incluir-se uma síntese da análise de risco realizada para avaliar tais impactos; (iv) Os principais incidentes relacionados com as TIC, o seu impacto operacional, reputacional ou regulatório, bem como as medidas corretivas, de recuperação e mitigação adotadas.
TIC Função de gestão de riscos por terceiros	As a seguradora estabelecem uma função para controlar os acordos celebrados com os prestadores de serviços terceiros de TIC sobre a utilização de serviços de TIC, ou designam um membro da direção como responsável pela supervisão da exposição ao risco e da documentação relevante.
Formação em matéria de riscos	Os membros da direção da Seguradora devem manter-se ativamente atualizados com conhecimentos e competências suficientes para compreender e avaliar o risco associado às TIC e o seu impacto nas operações da Seguradora, nomeadamente através de uma formação específica regular, proporcional ao risco associado às TIC que está a ser gerido.
Recursos de gestão do risco das TIC	O quadro de gestão dos riscos em matéria de TIC deve incluir, pelo menos, estratégias, políticas, procedimentos, protocolos e ferramentas em matéria de TIC que sejam necessários para proteger devida e adequadamente todos os activos de informação e activos de TIC, incluindo software informático, hardware e servidores, bem como para proteger todos os componentes físicos e infraestruturas relevantes, tais como instalações, centros de dados e áreas sensíveis designadas, a fim de garantir que todos os activos de informação e activos de TIC estejam adequadamente protegidos contra riscos, incluindo danos e acesso ou utilização não autorizados.
Auditoria das autoridades - Pedidos relacionados com os riscos	As a seguradora fornecerão às autoridades competentes, a pedido destas, informações completas e atualizadas sobre o risco associado às TIC e sobre o seu quadro de gestão do risco associado às TIC.
Independência do gestor de riscos	As a seguradora asseguram uma separação e independência adequadas das funções de gestão do risco das TIC, das funções de controlo e das funções de auditoria interna, de acordo com o modelo das três linhas de defesa ou com um modelo de gestão e controlo interno do risco.
Análise e relatório da gestão do risco das TIC	O quadro de gestão do risco das TIC deve ser documentado e revisto pelo menos uma vez por ano, bem como aquando da ocorrência de incidentes graves relacionados com as TIC, e na sequência de instruções de supervisão ou de conclusões derivadas de testes de resiliência operacional digital ou de processos de auditoria relevantes. Deve ser apresentado à autoridade competente, a pedido desta, um relatório sobre a revisão do quadro de gestão do risco das TIC.
Melhoria contínua	A gestão do risco das TIC deve ser continuamente melhorada com base nos ensinamentos retirados da execução e do controlo.
Auditoria Interna	A gestão do risco das TIC é objeto de uma auditoria interna efetuada regularmente por auditores, em conformidade com o plano de auditoria das a seguradora. Esses auditores devem possuir conhecimentos, competências e experiência suficientes no domínio do risco das TIC, bem como uma independência adequada.
Verificação e correção	Com base nas conclusões da análise da auditoria interna, as a seguradora estabelecem um processo formal de acompanhamento, incluindo regras para a verificação e correção atempadas das constatações críticas de auditoria das TIC.

Estratégia DOR: conteúdo	O quadro de gestão do risco das TIC deve incluir uma estratégia de resiliência operacional digital que estabeleça o modo como o quadro deve ser aplicado. Deve incluir métodos para fazer face aos riscos em matéria de TIC e atingir objetivos específicos neste domínio: a) O quadro de gestão do risco das TIC apoia a estratégia e os objetivos comerciais da Seguradora b) Apetência pelo risco, tolerância ao risco e impacto da tolerância nas perturbações das TIC c) Objetivos de segurança, KPI e KRM d) Arquitetura de referência das TIC e eventuais alterações necessárias para atingir objetivos comerciais específicos e) Mecanismo para detetar incidentes de TIC, prevenir o impacto e fornecer proteção f) Estado da DOR, tendo em conta o número de incidentes graves de TIC comunicados e a sua eficácia g) Teste da DOR h) Estratégia de comunicação em conformidade com Processo de comunicação de crises, Políticas de comunicação e Funções de comunicação.
TIC Estratégia multifornecedor	No contexto da estratégia de resiliência operacional digital, a empresa pode implementar uma estratégia de múltiplos fornecedores de TIC, a nível do grupo ou da entidade, mostrando as principais dependências de fornecedores de serviços terceiros de TIC e explicando a lógica subjacente à combinação de aquisições de fornecedores de serviços terceiros de TIC.
Externalização da conformidade	A Seguradora podem, em conformidade com a legislação setorial da União e nacional, subcontratar as tarefas de verificação do cumprimento dos requisitos de gestão do risco das TIC a empresas intragrupo ou externas. No caso de tal subcontratação, a Seguradora continua a ser plenamente responsável pela verificação do cumprimento dos requisitos de gestão do risco das TIC.
Requisitos de sistemas, protocolos e ferramentas TIC	Os requisitos aplicáveis aos sistemas, protocolos e instrumentos de TIC adotados pelas seguradoras devem estar em conformidade com o princípio da proporcionalidade, ou seja, ajustados à dimensão, complexidade e criticidade das operações que suportam. Nesse sentido, os sistemas devem ser: (a) Fiáveis, assegurando a exatidão, consistência e disponibilidade dos dados em todas as fases do processamento; (b) Dotados de capacidade técnica suficiente para: processar com precisão os dados necessários à execução das atividades operacionais e regulatórias; assegurar a prestação contínua e atempada dos serviços aos clientes e parceiros; acomodar picos de carga, como aumentos súbitos de transações, mensagens ou encomendas, inclusive durante a introdução de novas tecnologias ou atualizações sistémicas; (c) Tecnologicamente resilientes, permitindo à seguradora manter a continuidade e desempenho dos serviços mesmo sob condições adversas, como situações de tensão de mercado, falhas de infraestrutura, ciberincidentes ou eventos disruptivos.
Inventário das operações TIC	Identificação, classificação e documentação de todas as: funções empresariais apoiadas pelas TIC e activos TIC que apoiam essas funções, papéis e responsabilidades, activos de informação e respetivos papéis e dependências em relação aos riscos TIC.
Fontes de riscos das TIC	Deve ser identificado, numa base contínua, todas as fontes de risco das TIC, a exposição ao risco de e para outras a seguradora, e avaliar as ciberameaças e vulnerabilidades das TIC relevantes para as suas funções comerciais, activos de informação e activos de TIC apoiados pelas TIC.
Avaliação dos Riscos	A seguradora procede a uma avaliação dos riscos aquando de cada alteração importante da infraestrutura da rede e do sistema de informação, dos processos ou dos procedimentos que afetam as suas funções empresariais apoiadas pelas TIC, os seus activos de informação ou os seus activos de TIC.
Inventário dos activos de informação e TIC(CMDB)	A seguradora deve proceder à identificação e inventariação sistemática de todos os ativos de informação e ativos de Tecnologias de Informação e Comunicação (TIC), abrangendo não só os que se encontram nas instalações centrais, mas também os localizados em sítios remotos ou em ambientes híbridos (on-premises e cloud). Este levantamento deve incluir: Equipamentos informáticos, recursos de rede e dispositivos móveis; Sistemas de armazenamento, plataformas de virtualização e aplicações críticas; Configuração técnica de cada ativo, com detalhes sobre versões, dependências e funções de negócio suportadas; Mapeamento das ligações e interdependências entre ativos, de modo a identificar pontos de falha comuns, relações críticas e potenciais impactos cruzados em caso de incidente. Adicionalmente, a seguradora deve classificar os ativos com base na sua criticidade para a continuidade das funções essenciais e na sensibilidade da informação que tratam ou armazenam. Essa classificação é fundamental para definir prioridades de proteção, medidas de mitigação e estratégias de recuperação.
Inventário dos processos TIC	A seguradora identifica e documenta todos os processos que dependem de prestadores de serviços terceiros de TIC e identificam as interconexões com prestadores de serviços terceiros de TIC que prestam serviços de apoio a funções críticas ou importantes.
Revisão de modificação de inventário	Para efeitos do (Inventário das operações TIC), do (Inventário dos activos de informação e TIC) e do (Inventário dos processos TIC), as a seguradora devem manter os inventários pertinentes e atualizá-los periodicamente e sempre que ocorra uma alteração importante, tal como referido no (Avaliação dos riscos).
Revisão anual da avaliação de risco específica das TIC	A seguradora efetuam regularmente, e pelo menos uma vez por ano, uma avaliação específica dos riscos em matéria de TIC relativamente a todos os sistemas de TIC antigos e, em qualquer caso, antes e depois da ligação de tecnologias, aplicações ou sistemas.
Sistemas TIC: monitorizar e controlar	A seguradora acompanha e controla continuamente a segurança e o funcionamento dos sistemas e instrumentos de TIC e minimizam o impacto do risco associado aos sistemas de TIC através da utilização de instrumentos, políticas e procedimentos adequados de segurança das TIC.
Políticas de segurança das TIC	As seguradoras devem conceber, adquirir e aplicar políticas, procedimentos, protocolos e ferramentas de segurança das TIC com o objetivo de garantir a resiliência, continuidade e disponibilidade dos sistemas de informação, especialmente daqueles que suportam funções críticas ou importantes. Estas medidas devem assegurar elevados padrões de disponibilidade, autenticidade, integridade e confidencialidade dos dados, independentemente do seu estado: em repouso, em utilização ou em trânsito.

Adequação das TIC	As soluções e processos TIC devem ser adequados de acordo com o princípio da proporcionalidade: (a) segurança dos meios de transferência de dados; (b) minimizar o risco de corrupção ou perda de dados, de acesso não autorizado e de falhas técnicas que possam prejudicar a atividade comercial (c) prevenir a falta de disponibilidade, o comprometimento da autenticidade e integridade, a quebra de confidencialidade e a perda de dados; (d) Assegurar a proteção dos dados contra os riscos decorrentes da gestão dos dados, incluindo a má administração, os riscos relacionados com o tratamento e os erros humanos.
Política de Segurança da Informação	Desenvolver e documentar uma política de segurança da informação que defina regras para proteger a disponibilidade, autenticidade, integridade e confidencialidade dos dados, dos activos de informação e dos activos de TIC, incluindo os dos seus clientes, quando aplicável.
Gestão de redes e infraestruturas	Seguindo uma abordagem baseada no risco, estabelecer uma estrutura sólida de gestão das redes e infraestruturas, utilizando técnicas, métodos e protocolos adequados que podem incluir a implementação de mecanismos automatizados para isolar os activos de informação afetados afetados em caso de ciberataques. As a seguradora devem conceber a infraestrutura de ligação em rede para permitir a sua separação ou segmentação instantânea, a fim de minimizar e evitar o contágio, especialmente no caso de processos financeiros interligados.
Controlo de Acesso	Aplicar políticas que limitem o acesso físico ou lógico aos activos de informação e aos activos de TIC apenas ao necessário para funções e atividades legítimas e aprovadas, e estabelecer para esse efeito um conjunto de políticas, procedimentos e controlos que abordem os direitos de acesso e assegurem uma boa gestão dos mesmos;
Controlo das Alterações das TIC	Aplicar políticas, procedimentos e controlos documentados para a gestão das alterações das TIC, incluindo alterações de software, hardware, componentes de firmware, sistemas ou parâmetros de segurança, que se baseiem numa abordagem de avaliação dos riscos e sejam parte integrante do processo global de gestão das alterações da Seguradora, a fim de garantir que todas as alterações dos sistemas TIC sejam registadas, testadas, avaliadas, aprovadas, aplicadas e verificadas de forma controlada. A política de controlo das alterações das TIC deve ser aprovada pelas instâncias de gestão adequadas e deve ter protocolos específicos.
Política de Autenticação	Aplicar políticas e protocolos para mecanismos de autenticação forte, com base em normas relevantes e sistemas de controlo específicos, e medidas de proteção de chaves criptográficas através das quais os dados são cifrados com base nos resultados de processos aprovados de classificação de dados e de avaliação de riscos das TIC.
Gestão de Patches	Políticas documentadas adequadas e abrangentes para correcções e actualizações.
Deteção de incidentes TIC	A seguradora deve ter mecanismos para detetar atividades anómalas, em conformidade com o (Processo de gestão de incidentes relacionados com as TIC), incluindo problemas de desempenho da rede de TIC e incidentes relacionados com as TIC, e para identificar potenciais pontos únicos de falha importantes. O mecanismo deve ser regularmente testado em conformidade com o definido em Especificações de teste.
Mecanismos de deteção de incidentes	Os mecanismos de deteção referidos em Mecanismos de deteção de incidentes devem permitir múltiplos níveis de controlo, definir limiares de alerta e critérios para desencadear e iniciar processos de resposta a incidentes relacionados com as TIC, incluindo mecanismos de alerta automático para o pessoal competente responsável pela resposta a incidentes relacionados com as TIC.
Monitorização de incidentes	A seguradora consagra recursos e capacidades suficientes para controlar a atividade dos utilizadores, a ocorrência de anomalias nas TIC e os incidentes relacionados com as TIC, em especial os ciberataques.
Deteção de incidentes DRSP	Os prestadores de serviços de comunicação de dados devem, além disso, dispor de sistemas que permitam verificar eficazmente se as comunicações comerciais estão completas, identificar omissões e erros óbvios e solicitar a retransmissão dessas comunicações.
Política de Continuidade das Atividades das TIC	A política de continuidade das atividades das TIC pode ser adotada como uma política específica, fazendo parte integrante da política global de continuidade das atividades da Seguradora.
Política de Continuidade das Atividades de TIC: conteúdo mínimo	A política de continuidade das atividades da seguradora visa garantir a resiliência operacional digital, através de um conjunto estruturado de objetivos e medidas que asseguram a continuidade e recuperação das funções críticas ou importantes perante incidentes disruptivos, nomeadamente os relacionados com as TIC. Os objetivos centrais desta política incluem: (a) Assegurar a continuidade das funções críticas ou importantes da organização, mesmo em cenários de disrupção tecnológica; (b) Permitir uma resposta rápida, adequada e eficaz a incidentes relacionados com as TIC, limitando os danos operacionais, reputacionais e financeiros, e promovendo a retoma eficiente das atividades; (c) Garantir a ativação imediata de planos de contenção e recuperação, adaptados a cada tipo de incidente, com base em processos, ferramentas e tecnologias previamente definidos. Estes planos devem estar articulados com os procedimentos de backup, restauração e recuperação de dados, assegurando medidas preventivas e corretivas eficazes; (d) Realizar uma estimativa preliminar dos impactos, perdas e danos, com base em métricas definidas, para apoiar a decisão e priorização de resposta; (e) Estabelecer ações de comunicação e gestão de crise, garantindo a transmissão clara e atualizada de informação: a todo o pessoal interno relevante, às partes interessadas externas (clientes, parceiros, reguladores),e às autoridades competentes, de acordo com os mecanismos definidos no plano de reporte e notificação regulamentar.
Plano de resposta e recuperação das TIC	No âmbito do (quadro de gestão dos riscos em matéria de TIC), a seguradora devem aplicar planos associados de resposta e recuperação em matéria de TIC, que devem ser objeto de análises por auditorias internas independentes.
Política de continuidade das atividades de TIC: manutenção e testes	A seguradora estabelece, mantêm e testa periodicamente planos adequados de continuidade das atividades de TIC, nomeadamente no que diz respeito a funções críticas ou importantes externalizadas ou contratadas através de acordos com prestadores de serviços de TIC terceiros.
Processo de Análise do Impacto nas Empresas (BIA)	O BIA serve para avaliar o impacto potencial de perturbações graves da atividade através de critérios quantitativos e qualitativos, utilizando dados internos e externos e análises de cenários, conforme adequado. A BIA deve ter em conta o carácter crítico das funções empresariais identificadas e identificadas, dos processos de apoio, das dependências de terceiros e dos activos de informação, bem como as suas interdependências.

Teste do PCN Continuidade e resposta	São efetuados testes referente à Política de continuidade das atividades de TIC e Plano de resposta e recuperação de TIC em relação aos sistemas de TIC que suportam todas as funções, pelo menos uma vez por ano, bem como em caso de alterações substanciais aos sistemas de TIC que suportam funções críticas ou importantes.
Teste de PCN: Cenários	A seguradora deve incluir nos planos de ensaio cenários de ciberataques e de comutação entre a infraestrutura primária de TIC e a capacidade redundante, as cópias de segurança e os recursos redundantes necessários para cumprir as obrigações estabelecidas em políticas e procedimentos de cópia de segurança, procedimentos e métodos de restabelecimento e recuperação
Teste de PCN: Comunicação em caso de crise	Testar os planos de comunicação de crise estabelecidos em conformidade com referidos na comunicação
Revisão dos planos de continuidade das atividades e de resposta e recuperação	Rever a política de continuidade das atividades das TIC e os planos de resposta e recuperação das TIC, tendo em conta os resultados dos testes realizados em conformidade com o (Testes do PCN: cenários) e as recomendações decorrentes de verificações de auditoria ou de análises de supervisão.
Papel da Gestão de Crises	A seguradora deve ter uma função de gestão de crises que, em caso de ativação dos seus planos de continuidade das atividades TIC ou dos seus planos de resposta e recuperação TIC, deve, nomeadamente, estabelecer procedimentos claros para gerir as comunicações internas e externas em caso de crise, em conformidade com o plano de Comunicação
Manutenção de Registos	A seguradora conserva registos facilmente acessíveis das atividades realizadas antes e durante os eventos de perturbação, quando são ativados os seus planos de continuidade das atividades TIC e os seus planos de resposta e recuperação TIC.
Requisitos das centrais de depósito de títulos	Os depositários centrais de valores mobiliários devem fornecer às autoridades competentes cópias dos resultados dos testes de continuidade das atividades no domínio das TIC ou de exercícios semelhantes.
Comunicação dos custos e perdas de incidentes relacionados com as TIC	A seguradora comunicará às autoridades competentes, a pedido destas, uma estimativa dos custos e perdas anuais agregados causados por incidentes graves relacionados com as TIC.
Sistemas TIC e restauro da informação	Para assegurar um tempo de inatividade mínimo e reduzir ao máximo as perturbações e perdas operacionais(artigo 11º), a seguradora deve desenvolver e manter os seguintes mecanismos: (a) Políticas e procedimentos de cópia de segurança (backup), que definam claramente: o âmbito da informação sujeita a backup, com base na sua criticidade e no nível de confidencialidade dos dados; a frequência mínima dos backups, ajustada ao impacto potencial da perda de dados (ex. backups diários para sistemas críticos, mensais para arquivos históricos); (b) Procedimentos e métodos robustos de restauração e recuperação de dados, garantindo que, em caso de incidente, os sistemas e informações podem ser restaurados num prazo compatível com os objetivos de recuperação (RTO/RPO) definidos pela organização.
Ativação de sistemas de reserva	A seguradora deve dispor de sistemas de salvaguarda (backup)(Artigo 11.º, n.º 2 e n.º 3) devidamente configurados e testados, que possam ser ativados em conformidade com as suas políticas internas de salvaguarda e recuperação, bem como com os procedimentos operacionais de restauro de dados e sistemas. A ativação destes sistemas de cópia de segurança deve respeitar rigorosamente os princípios de segurança da informação, não podendo comprometer a disponibilidade, autenticidade, integridade ou confidencialidade dos dados, nem a segurança global da rede e dos sistemas de informação.
Requisitos dos sistemas de cópia de segurança	Para o restabelecimento dos dados de segurança através dos seus próprios sistemas, as a seguradora utilizam sistemas TIC física e logicamente separados do sistema TIC de origem. Os sistemas TIC devem ser protegidos de forma segura contra qualquer acesso não autorizado ou corrupção das TIC e permitir o restabelecimento atempado dos serviços, recorrendo, se necessário, a cópias de segurança dos dados e dos sistemas.
Planos de recuperação para contrapartes centrais	Relativamente às contrapartes centrais, os planos de recuperação devem permitir a recuperação de todas as transações no momento da perturbação, de modo a que a contraparte central possa continuar a operar com segurança e concluir a liquidação na data prevista.
Instalações de reserva e de restauro(Disaster Recovery e processamento secundário)	Os prestadores de serviços de transmissão de dados devem também manter recursos adequados e dispor de meios de reserva e de restabelecimento para poderem oferecer e manter os seus serviços em permanência.
Capacidades redundantes de TIC	A seguradora devem manter capacidades TIC redundantes, equipadas com recursos, capacidades e funções adequadas para assegurar as necessidades da atividade.
Local de processamento secundário(Datacenter Secundário)	A seguradora deve manter um local de processamento secundário (Esta exigência encontra-se em conformidade com o artigo 11.º)com recursos, capacidades técnicas e operacionais, e disposições adequadas em matéria de pessoal, de modo a garantir a continuidade das suas funções críticas ou importantes em caso de indisponibilidade do local principal. Este local secundário deve obedecer aos seguintes requisitos: (a) Estar situado a uma distância geográfica adequada do local de processamento primário, garantindo um perfil de risco distinto, de forma a evitar ser afetado simultaneamente pelo mesmo evento disruptivo que comprometa o centro principal; (b) Possuir capacidade para assegurar a continuidade operacional dos serviços essenciais, com níveis de desempenho equivalentes aos do centro principal ou compatíveis com os objetivos de recuperação (RTO e RPO) definidos no plano de continuidade de negócio da seguradora; (c) Ser imediatamente acessível ao pessoal relevante da organização, permitindo a ativação célere do plano de contingência e assegurando a execução das funções críticas ou importantes sem interrupções significativas.
RTO e RPO	Ao determinar o tempo de recuperação e os objetivos do ponto de recuperação para cada função, a seguradora deve ter em conta se se trata de uma função crítica ou importante e o potencial impacto global na eficiência do mercado. Esses objetivos de tempo deve garantir que, em cenários extremos, os níveis de serviço acordados sejam cumpridos.
Recuperação de incidentes relacionados com as TIC	Ao recuperar de um incidente relacionado com as TIC, as a seguradora devem efetuar as verificações necessárias, incluindo quaisquer verificações e reconciliações múltiplas, a fim de garantir a manutenção do mais elevado nível de integridade dos dados. Estas verificações devem igualmente ser efetuadas aquando da reconstrução de dados provenientes de partes interessadas externas, a fim de garantir a coerência de todos os dados entre sistemas.
Conhecimentos de segurança da informação: capacidades e pessoal	A seguradora deve ter capacidades técnicas e de pessoal para recolher informações sobre vulnerabilidades e ciberameaças, incidentes relacionados com as TIC, em especial ciberataques, e analisar o impacto que estes podem ter na sua resiliência operacional digital.

Análise Pós-Incidente	A seguradora procede a revisões após um incidente grave relacionado com as TIC que perturbe as suas atividades principais, analisando as causas da perturbação e identificando as melhorias necessárias para as operações de TIC ou no âmbito a política de continuidade das atividades das TIC referida no (política de continuidade das atividades das TIC)
Comunicação de alterações Pós-Incidente	A seguradora comunicará às autoridades competentes, a pedido destas, as alterações efetuadas na sequência da análise de incidentes relacionados com as TIC, tal como referido no . As análises pós-incidentes relacionados com as TIC referidas no determinam se os procedimentos estabelecidos foram seguidos e se as medidas tomadas foram eficazes, nomeadamente em relação aos seguintes aspetos (a) a rapidez de resposta aos alertas de segurança e a determinação do impacto dos incidentes relacionados com as TIC e a sua gravidade; (b) a qualidade e a rapidez da realização de uma análise forense, quando considerada adequada; (c) a eficácia da escalada de incidentes no seio da Seguradora; (d) A eficácia da comunicação interna e externa.
Repositório de lições aprendidas no processo de avaliação do risco das TIC	Os ensinamentos retirados dos testes de resiliência operacional digital realizados em Testes avançados de ferramentas, sistemas e processos TIC baseados em TLPT e requisitos para os testadores que realizam TLPT e de incidentes reais relacionados com as TIC, em particular ciberataques, juntamente com os desafios enfrentados aquando da ativação dos planos de continuidade das atividades TIC e dos planos de resposta e recuperação das TIC, juntamente com as informações relevantes trocadas com as contrapartes e avaliadas durante as análises de supervisão, devem ser devidamente incorporados de forma contínua no processo de avaliação do risco das TIC. Essas conclusões devem constituir a base para revisões adequadas das componentes relevantes do quadro de gestão do risco das TIC.
Acompanhamento da Estratégia de Resiliência Operacional Digital	A seguradora deve monitorizar a eficácia da aplicação da sua estratégia de resiliência operacional digital definida no . (Estratégia DOR: conteúdo).
Relatórios sobre lições de incidentes relacionados com as TIC	Os quadros superiores do pessoal das TIC devem apresentar aa direção, pelo menos uma vez por ano, um relatório sobre as conclusões referidas no (repositório dos ensinamentos obtidos no processo de avaliação dos riscos das TIC) e formular recomendações.
Sensibilização para a segurança e formação DOR	A seguradora desenvolvem programas de sensibilização para a segurança das TIC e formação em matéria de resiliência operacional digital como módulos obrigatórios dos seus programas de formação do pessoal. Esses programas e ações de formação são aplicáveis a todos os trabalhadores e ao pessoal de direção, e devem ter um nível de complexidade proporcional ao âmbito das suas funções.
Acompanhamento dos desenvolvimentos tecnológicos relevantes	A seguradora deve acompanhar continuamente os desenvolvimentos tecnológicos relevantes, também com o objetivo de compreender o possível impacto da implantação dessas novas tecnologias nos requisitos de segurança das TIC e na resiliência operacional digital. Mantêm-se atualizadas em relação aos mais recentes processos de gestão dos riscos das TIC, a fim de combater eficazmente as formas atuais ou novas de ciberataques.
Processo de comunicação de crise e Politica de Comunicação	No âmbito da gestão do risco das TIC, a seguradora deve ter planos de comunicação de crises que permitam a divulgação responsável, pelo menos, dos principais incidentes ou vulnerabilidades relacionados com as TIC aos clientes e contrapartes, bem como ao público, se for caso disso. A política de comunicação devem ser aplicadas para o pessoal interno e para as partes interessadas externas. As políticas de comunicação para o pessoal devem ter em conta a necessidade de diferenciar entre o pessoal envolvido na gestão do risco das TIC, em especial o pessoal responsável pela resposta e recuperação, e o pessoal que necessita de ser informado. Pelo menos uma pessoa da Seguradora deve ser encarregada de aplicar a estratégia de comunicação para os incidentes relacionados com as TIC e desempenhar a função pública e mediática para esse efeito.
Processo de gestão de incidentes relacionados com as TIC	
Classificação de Incidentes	A seguradora classifica os incidentes relacionados com as TIC e avalia o seu impacto com base nos seguintes critérios: (a) o número e/ou a relevância dos clientes ou contrapartes afetados, incluindo o volume de transações e eventual impacto reputacional; (b) a duração do incidente, nomeadamente o tempo de inatividade dos serviços afetados; (c) a distribuição geográfica das zonas impactadas, especialmente se envolver mais de dois Estados-Membros; (d) as perdas de dados, considerando os efeitos sobre a disponibilidade, integridade, autenticidade e confidencialidade da informação; (e) o grau de criticidade dos serviços afetados, abrangendo transações e operações essenciais da seguradora; (f) o impacto económico, incluindo custos e perdas diretas ou indiretas, tanto em termos absolutos como proporcionais
Classificação das ciberameaças	As ciberameaças são classificadas como significativas com base no carácter crítico dos serviços em risco, incluindo as transações e operações da Seguradora, o número e/ou a relevância dos clientes ou contrapartes financeiras visados e a distribuição geográfica das áreas em risco.
Comunicação de incidentes graves relacionados com as TIC	A seguradora deve comunicar os incidentes graves relacionados com as TIC à autoridade competente, em conformidade com o Artigo 46.º do Regulamento (UE) 2022/2554 (DORA). Essa comunicação deve respeitar os requisitos formais definidos na Norma Regulamentar n.º 9/2023-R da ASF, que estabelece o conteúdo mínimo obrigatório das notificações e a utilização dos modelos normalizados definidos pelas normas técnicas de regulamentação europeia (RTS). O processo compreende a elaboração da notificação inicial, seguida dos relatórios intercalares e do relatório final, após a recolha e análise de todas as informações relevantes sobre o incidente. A comunicação deve ser efetuada através da plataforma eletrónica disponibilizada para o efeito. Em situações excecionais em que uma impossibilidade técnica impeça a utilização do modelo normalizado, a seguradora deve informar a ASF de imediato, utilizando meios alternativos, nomeadamente através do endereço eletrónico dedicado: dora@asf.com.pt.
Relatórios Voluntários	A seguradora pode, numa base voluntária, notificar as ciberameaças consideradas significativas à ASF sempre que considerem que a ameaça é relevante para o sistema financeiro, os utilizadores dos serviços ou os clientes. A autoridade competente relevante pode fornecer essas informações a outras autoridades relevantes.

Comunicação com os clientes	Caso ocorra um incidente grave relacionado com as TIC que tenha impacto nos interesses financeiros dos clientes, a seguradora informará os seus clientes, sem demora injustificada e logo que tenham conhecimento do mesmo, sobre o incidente grave relacionado com as TIC e sobre as medidas adotadas para atenuar os efeitos adversos desse incidente.
Comunicação de conteúdos mínimos	A seguradora deve apresentar à ASF, no âmbito da gestão de incidentes graves relacionados com as TIC, os seguintes elementos de comunicação formal: (a) Uma notificação inicial, a remeter logo que o incidente seja detetado; (b) Um relatório intercalar, subsequente à notificação inicial, sempre que haja uma alteração significativa no estado do incidente ou na resposta adotada, com base em nova informação disponível. Este pode ser complementado por atualizações adicionais, sempre que pertinente ou mediante solicitação da autoridade competente; (c) Um relatório final, a submeter após a conclusão da análise da causa raiz do incidente, independentemente da implementação de medidas de mitigação, e com substituição das estimativas iniciais pelos valores reais do impacto verificado. Esta obrigação encontra-se prevista no artigo 20.º do Regulamento (UE) 2022/2554 (DORA)
Externalização de Relatórios	A seguradora pode subcontratar a terceiros, de acordo com a legislação nacional e da União aplicável, as obrigações de comunicação de incidentes previstas no regulamento. Contudo, essa subcontratação não isenta a seguradora da sua responsabilidade: a entidade permanece integralmente responsável pelo cumprimento dos requisitos de reporte e comunicação de incidentes relacionados com as TIC, devendo assegurar que o prestador de serviços cumpre os mesmos níveis de qualidade, segurança e tempestividade exigidos pelo quadro regulamentar, nomeadamente pelo Regulamento (UE) 2022/2554 (DORA), artigo 19.º, n.º 4.
Teste de Resiliência Operacional Digital	Para avaliar o grau de preparação para lidar com incidentes relacionados com as TIC, identificar pontos fracos, deficiências e lacunas na resiliência operacional digital e aplicar prontamente medidas corretivas, a seguradora deve, tendo em conta os critérios de proporcionalidade, estabelecer, manter e rever um programa sólido e abrangente de testes de resiliência operacional digital como parte integrante do quadro de gestão do risco das TIC.
Considerações sobre os riscos dos testes DOR	Ao realizar o programa de testes de resiliência operacional digital, a seguradora deve seguir uma abordagem baseada no risco, tendo em conta os critérios de proporcionalidade, considerando devidamente o panorama evolutivo do risco das TIC, quaisquer riscos específicos a que a Seguradora em causa esteja ou possa estar exposta, o carácter crítico dos activos de informação e dos serviços prestados, bem como qualquer outro fator que a Seguradora considere adequado.
Inspetor Independente	A seguradora assegurará que os testes sejam efetuados por entidades independentes, quer internas quer externas. Quando os testes forem efetuados por um inspetor interno, a seguradora devem afetar recursos suficientes e assegurar que os conflitos de interesses sejam evitados durante as fases de conceção e execução do teste.
Prioridade, classificação e correção dos resultados dos testes	A seguradora deve definir procedimentos e políticas para dar prioridade, classificar e solucionar todas as questões reveladas durante a realização dos testes e deve definir metodologias de validação interna para verificar se todas as insuficiências, deficiências ou lacunas identificadas são plenamente resolvidas.
Testes Anuais	A seguradora assegurará, pelo menos uma vez por ano, a realização de testes adequados a todos os sistemas e aplicações TIC que servem de suporte a funções críticas ou importantes.
Especificações dos Testes	O programa deve incluir uma série de avaliações, tais como avaliações e análises de vulnerabilidades, análises de fontes abertas, avaliações de segurança da rede, análises de lacunas, análises de segurança física, questionários e soluções de software de análise, análises de código-fonte, sempre que possível, testes baseados em cenários, testes de compatibilidade, testes de desempenho, testes de extremo a extremo e testes de penetração. As microempresas realizam os testes combinando uma abordagem baseada no risco com um planeamento estratégico dos testes de TIC, tendo devidamente em conta a necessidade de manter uma abordagem equilibrada entre, por um lado, a escala de recursos e o tempo a atribuir aos testes de TIC previstos no presente artigo e, por outro lado, a urgência, o tipo de risco, a importância crítica dos activos de informação e dos serviços prestados, bem como qualquer outro fator relevante, incluindo a capacidade da Seguradora para assumir riscos calculados.
Testes avançados TLPT	A seguradora deve efetuar, pelo menos de 3 em 3 anos, testes avançados por meio de TLPT. Com base no perfil de risco da Seguradora e tendo em conta as circunstâncias operacionais, a autoridade competente pode, se necessário, solicitar à Seguradora que reduza ou aumente esta frequência.
Áreas de teste TLPT	Cada teste de penetração baseado em ameaças deve abranger várias ou todas as funções críticas ou importantes de uma Seguradora e deve realizar em sistemas de produção em funcionamento que sirvam de suporte a essas funções. As a seguradora identificam todos os sistemas, processos e tecnologias TIC subjacentes relevantes que apoiam as funções críticas ou importantes e os serviços TIC, incluindo os que apoiam as funções críticas ou importantes que tenham sido que tenham sido externalizados ou contratados a prestadores de serviços de TIC terceiros.
Âmbito de aplicação do TLPT: Prestador de serviços de TIC a terceiros	Sempre que os prestadores de serviços terceiros de TIC estejam incluídos no âmbito do TLPT, a Seguradora toma as medidas e salvaguardas necessárias para assegurar a participação desses prestadores de serviços terceiros de TIC no TLPT e mantém a todo o momento a plena responsabilidade pelo cumprimento do presente regulamento.
Envolvimento de terceiros nas TIC em TLPT	Quando a participação de um prestador de serviços terceiros de TIC no TLPT, referida no Âmbito do TLPT: Prestador de serviços terceiros de TIC for razoavelmente suscetível de ter um impacto adverso na qualidade ou na segurança dos serviços prestados pelo prestador de serviços terceiros de TIC a clientes que sejam entidades não abrangidas pelo âmbito de aplicação do presente regulamento, ou na confidencialidade dos dados relacionados com esses serviços, a Seguradora e o prestador de serviços terceiros de TIC podem acordar por escrito que o prestador de serviços terceiros de TIC celebre diretamente acordos contratuais com um testador externo, com o objetivo de realizar, sob a direção de uma Seguradora designada, um TLPT agrupado que envolva várias a seguradora (testes agrupados) às quais o prestador de serviços terceiros de TIC presta serviços de TIC.

Cooperação na Gestão dos Riscos e na aplicação dos controlos	A seguradora aplica, com a cooperação dos prestadores de serviços terceiros de TIC e de outras partes envolvidas, incluindo os inspetores, mas excluindo as autoridades competentes, controlos eficazes da gestão do risco para atenuar os riscos de qualquer impacto potencial nos dados, danos nos activos e perturbação de funções, serviços ou operações críticos ou importantes da própria Seguradora, das suas contrapartes ou do sector financeiro.
Relatório de constatações, correcções e documentação	No final dos testes, após a aprovação dos relatórios e dos planos de correção, a Seguradora e, quando aplicável, os inspetores externos devem fornecer à autoridade, designada em conformidade com os n.ºs 9 ou 10 do artigo 26.º da DORA, um resumo das conclusões relevantes, dos planos de correção e da documentação que demonstra que a PTF foi realizada em conformidade com os requisitos.
Comunicação de atestado TLPT	As autoridades fornecerão às a seguradora um atestado que confirme que o teste foi efectuado em conformidade com os requisitos evidenciados na documentação, a fim de permitir o reconhecimento mútuo dos testes de penetração baseados em ameaças entre as autoridades competentes. A Seguradora notifica a autoridade competente relevante do atestado, do resumo das conclusões relevantes e dos planos de correção.
Requisitos dos inspetores	A seguradora devem contratar inspetores para efeitos da realização de TLPT em conformidade com o . (Requisitos TLPT) Quando as a seguradora utilizam inspetores internos para a realização de TLPT, devem contratar inspetores externos a cada três testes.
Requisitos do TLPT	A seguradora só deve utilizar para a realização dos TLPT testadores que (a) Sejam da mais elevada idoneidade e reputação; (b) Possuam capacidades técnicas e organizativas e demonstrem conhecimentos específicos em matéria de informações sobre ameaças, testes de penetração e testes de equipas vermelhas penetração e testes de equipas vermelhas; (c) Sejam certificadas por um organismo de acreditação num Estado-Membro ou adiram a códigos de conduta formais ou a quadros éticos; (d) Forneçam uma garantia independente, ou um relatório de auditoria, relativamente à boa gestão dos riscos associados à d) Fornecer uma garantia independente ou um relatório de auditoria relativamente à boa gestão dos riscos associados à execução dos PTF, incluindo a devida proteção das informações confidenciais da Seguradora e a reparação dos riscos de negócio da Seguradora; (e) estão devida e integralmente cobertos por seguros de responsabilidade civil profissional relevantes, incluindo contra riscos de má conduta e negligência.
Requisitos internos de TLPT	Ao utilizarem testadores internos, as a seguradora deve garantir que, para além dos requisitos constantes do (Requisitos TLTP) as seguintes condições são cumpridas: (a) Essa utilização foi aprovada pela autoridade competente relevante ou pela autoridade pública única designada em conformidade com os n.ºs 9 e 10 do artigo 26; (b) A autoridade competente relevante verificou que a Seguradora dispõe de recursos dedicados suficientes e assegurou que os conflitos de interesses são evitados durante as fases de conceção e execução do teste; e (c) O fornecedor de informações sobre ameaças é externo à Seguradora.
Requisitos do contrato TLPT	A seguradora asseguram-se de que os contratos celebrados com os examinadores externos exigem uma boa gestão dos resultados dos testes TLPT e de que qualquer tratamento dos dados, incluindo a sua geração, armazenamento, agregação, redação, relatório, comunicação ou destruição, não cria riscos para a Seguradora.
Base de riscos de terceiros em TIC	A Seguradora deve considerar o risco de terceiros como parte integrante do seu risco global de TIC, garantindo: (a) Responsabilidade plena: mesmo quando contrata serviços TIC a terceiros, a Seguradora continua inteiramente responsável pelo cumprimento das obrigações previstas no DORA e na legislação financeira aplicável. (b) Gestão proporcional do risco: a abordagem ao risco de terceiros deve respeitar o princípio da proporcionalidade, considerando: (i) A natureza, escala, complexidade e importância das dependências relacionadas com os serviços TIC; (ii) Os riscos decorrentes dos contratos com terceiros, especialmente quando envolvem funções críticas ou importantes, e o seu impacto na continuidade e disponibilidade das atividades da Seguradora, tanto individualmente como em contexto de grupo.
Estratégia de riscos para terceiros nas TIC	A Seguradora deve definir e rever regularmente uma estratégia para a gestão do risco de terceiros nas TIC, integrada no seu enquadramento de gestão do risco das TIC. Essa estratégia deve: Ter em conta, quando aplicável, a estratégia de multifornecedores; Incluir uma política específica para a utilização de serviços TIC de suporte a funções críticas ou importantes, prestados por terceiros; Ser aplicada a nível individual, e, quando aplicável, também subconsolidado e consolidado
Acordos contratuais com terceiros nas TIC: registo de informações	A Seguradora deve manter e atualizar, tanto a nível da entidade como a nível subconsolidado e consolidado, um registo completo das disposições contratuais relativas à utilização de serviços TIC prestados por terceiros. Esse registo deve: Ser adequadamente documentado; Distinguir claramente entre contratos que envolvem funções críticas ou importantes e os que não as envolvem.
Avaliação por terceiros das TIC	A Seguradora deve, antes de celebrar contratos com prestadores de serviços terceiros de TIC: (a) Avaliar se o serviço prestado apoia funções críticas ou importantes; (b) Verificar se estão reunidas as condições de supervisão para a celebração do contrato; (c) Identificar e avaliar os riscos associados, incluindo potenciais riscos de concentração de TIC, conforme o artigo 29 do DORA; (d) Realizar as diligências devidas (due diligence) para garantir que o prestador é adequado; (e) Identificar e avaliar possíveis conflitos de interesse decorrentes do contrato.
Requisitos de InfoSec de terceiros para TIC	A seguradora só pode celebrar acordos contratuais com prestadores de serviços terceiros de TIC que cumpram as normas de segurança da informação adequadas. Sempre que esses acordos contratuais digam respeito a funções críticas ou importantes, as a seguradora devem, antes de os concluírem, ter devidamente em conta a utilização, pelos prestadores de serviços terceiros de TIC, das normas de segurança da informação mais atualizadas e de maior qualidade.

Direito de acesso, inspeção e auditoria de terceiros nas TIC	A Seguradora, ao exercer os seus direitos de acesso, inspeção e auditoria sobre prestadores de serviços terceiros de TIC, deve: Adotar uma abordagem baseada no risco para definir previamente a frequência das auditorias e as áreas a auditar, respeitando as normas de auditoria reconhecidas e as instruções de supervisão aplicáveis; Quando os contratos envolverem elevada complexidade técnica, assegurar que os auditores (internos, externos ou grupos de auditoria) possuem competências e conhecimentos adequados para realizar as auditorias de forma eficaz.
Direitos de rescisão de terceiros nas TIC	A Seguradora pode rescindir um contrato com um prestador de serviços terceiros de TIC nas seguintes situações: (a) Violação grave de leis, regulamentos ou cláusulas contratuais por parte do prestador; (b) Fatores identificados na monitorização de risco que possam comprometer o desempenho do serviço, incluindo alterações materiais ao contrato ou à situação do prestador; (c) Deficiências comprovadas na gestão do risco das TIC por parte do prestador, especialmente se afetarem a disponibilidade, autenticidade, integridade ou confidencialidade dos dados (pessoais ou não); (d) Impossibilidade de a autoridade competente exercer supervisão eficaz sobre a Seguradora, devido a restrições ou condições decorrentes do contrato.
Estratégia de saída apoio aos serviços TIC	A Seguradora deve definir estratégias de saída para contratos com prestadores de serviços TIC, considerando riscos como: Falha do prestador; Degradação da qualidade dos serviços; Perturbações na atividade devido a prestação deficiente; Riscos associados à rescisão contratual. Essas estratégias devem garantir que a rescisão de contratos pode ocorrer sem: (a) Interromper as atividades comerciais; (b) Comprometer o cumprimento dos requisitos regulamentares; (c) Prejudicar a continuidade ou qualidade dos serviços prestados aos clientes. Os planos de saída devem ser completos, documentados, testados regularmente e revistos periodicamente, respeitando o princípio da proporcionalidade.
Antecedentes e considerações contratuais de terceiros nas TIC	No âmbito da avaliação de terceiros em TIC, a Seguradora deve analisar se o novo contrato poderá gerar: (a) Dependência de um prestador de serviços TIC não facilmente substituível; (b) Concentração de contratos com o mesmo prestador ou com prestadores estreitamente ligados, quando estejam em causa funções críticas ou importantes. Nesses casos, a Seguradora deve ponderar os custos e benefícios de soluções alternativas, como diversificar fornecedores, avaliando se estas opções estão alinhadas com os seus objetivos de resiliência digital. Quando os contratos de serviços TIC relacionados com funções críticas ou importantes prevejam a possibilidade de subcontratação, a Seguradora deve: (a) Avaliar os benefícios e riscos dessa subcontratação, especialmente quando envolver subcontratantes sediados fora da UE; (b) Ter em conta as leis de insolvência aplicáveis em caso de falência do prestador principal e quaisquer limitações legais ou práticas à recuperação urgente dos dados da Seguradora.
Principais disposições contratuais relativas a terceiros nas TIC	O contrato entre a Seguradora e o prestador de serviços terceiros de TIC deve: Estabelecer por escrito todos os direitos e obrigações, incluindo os acordos de nível de serviço, num formato duradouro e acessível. Inclui obrigatoriamente: (a) Descrição completa das funções e serviços TIC prestados, indicando se é permitida a subcontratação de funções críticas ou importantes, e em que condições. (b) Identificação dos locais (regiões ou países) onde os serviços TIC são prestados e os dados tratados, incluindo obrigação de notificação prévia em caso de alteração desses locais. (c) Regras claras sobre a proteção da disponibilidade, autenticidade, integridade e confidencialidade dos dados, incluindo dados pessoais. (d) Garantias de acesso, recuperação e devolução dos dados (pessoais e não pessoais) em caso de insolvência, cessação de atividade ou rescisão do contrato. (e) Detalhes dos níveis de serviço contratados, bem como as respetivas atualizações e revisões. (f) Obrigação do prestador de prestar assistência à Seguradora, sem custos adicionais ou a um custo pré-definido, em caso de incidente de TIC. (g) Dever de cooperação com as autoridades competentes e autoridades de resolução de crises, incluindo representantes nomeados. (h) Definição dos direitos de rescisão contratual e dos prazos mínimos de pré-aviso, em conformidade com as expectativas regulatórias. (i) Participação do prestador nos programas de sensibilização de segurança das TIC e formação em resiliência operacional digital da Seguradora, conforme aplicável.

TIC de terceiros (funções críticas ou importantes) disposições contratuais adicionais	
	O contrato com prestadores de serviços terceiros de TIC deve incluir: (a) Níveis de serviço claros: Descrições completas, atualizações e revisões com objetivos quantitativos e qualitativos, permitindo um acompanhamento eficaz e medidas corretivas quando necessário. (b) Obrigações de notificação: Comunicação prévia de eventos com impacto na prestação de serviços críticos ou importantes. (c) Requisitos de segurança: Implementação de planos de contingência, medidas, ferramentas e políticas de segurança que garantam um nível de proteção adequado, em conformidade com o enquadramento regulatório da seguradora. (d) Participação na TLPT: Obrigatoriedade de cooperação plena com os testes de penetração baseados em ameaças (PTF), conforme o artigo 26 da DORA. (e) Monitorização contínua: (i) Direito de acesso, inspeção e auditoria pela seguradora, terceiros nomeados ou autoridades competentes, incluindo direito a cópias de documentação relevante. (ii) Possibilidade de definir garantias alternativas se os direitos de outros clientes forem afetados. (iii) Obrigação de cooperação durante auditorias e inspeções realizadas por qualquer entidade autorizada. (iv) Prestação de informações sobre o âmbito, frequência e procedimentos de auditoria. (f) Estratégias de saída: (i) Período de transição obrigatório para assegurar continuidade e mitigar perturbações. (ii) Permitir migração segura para outro prestador ou para soluções internas. As microempresas podem acordar que os direitos de acesso, inspeção e auditoria da Seguradora podem ser delegados a um terceiro independente, nomeado pelo prestador de serviços terceiros de TIC, e que a Seguradora pode solicitar a esse terceiro, a qualquer momento, informações e garantias sobre o desempenho do prestador de serviços terceiros de TIC. informações e garantias a qualquer momento.
Acordos de partilha de informações sobre ameaças cibernéticas e informações	A seguradora pode partilhar informações sobre ciberameaças, como indicadores de comprometimento e alertas de segurança, para reforçar a resiliência operacional digital. Esta partilha deve ocorrer em comunidades de confiança, com base em acordos que garantam a proteção da informação, respeitando a confidencialidade, o RGPD e as normas de concorrência.