ISPGAYA
instituto superior politécnico

Cláudia Inês Borgguen Ascenção

IMPLEMENTAÇÃO DA CONFORMIDADE COM O REGIME JURÍDICO DE SEGURANÇA NO CIBERESPAÇO

Relatório de estágio no âmbito do Mestrado em Cibersegurança e Auditoria em Sistemas Informáticos orientado pelo Professor Mestre Especialista Justino Marco Ronda Lourenço e apresentada ao Instituto Superior Politécnico Gaya.

Janeiro de 2025

Dedicatória

Dedico este trabalho aos meus pais, que são o meu maior suporte e que sempre me apoiaram incondicionalmente e me incentivaram a ir atrás dos meus sonhos.

Agradecimentos

Gostaria de expressar os meus sinceros agradecimentos a todos aqueles que contribuíram para a realização deste estágio.

Primeiramente, agradeço à empresa NECHO TECHLAW por me acolher e proporcionar um ambiente de aprendizagem tão enriquecedor. Em especial, agradeço ao Engenheiro Henrique Necho, o meu supervisor, pela sua orientação e apoio durante todo o período de estágio.

Agradeço também ao Professor Mestre Especialista Justino Lourenço, o meu orientador académico, pelo seu inestimável suporte e conselhos valiosos. A sua orientação foi fundamental para o desenvolvimento deste trabalho. Também agradeço aos Professores Dr. José Morais e Dr. Mário Lousã, que de alguma forma também contribuíram para a elaboração deste relatório, com as suas dicas dadas durante a unidade curricular de Metodologias de Investigação.

Finalmente, agradeço à minha família e amigos pelo constante incentivo e compreensão ao longo deste percurso.

Resumo

O presente relatório de estágio descreve as atividades desenvolvidas na empresa NECHO TECHLAW, no âmbito do curso de Mestrado em Cibersegurança e Auditoria de Sistemas Informáticos. O objetivo principal do estágio foi a implementação de medidas técnicas e organizacionais para garantir o alinhamento das práticas de segurança da organização com as exigências do Regime Jurídico de Segurança do Ciberespaço (RJSC) e demais legislações aplicáveis, assegurando a conformidade.

No contexto do trabalho, foram realizadas diversas atividades, incluindo a análise da situação atual das infraestruturas tecnológicas (*gap analysis*), o desenvolvimento de políticas e planos de cibersegurança, a elaboração de inventário de ativos e análises de risco, bem como a implementação de programas de formação e sensibilização para *stakeholders*. No presente relatório encontram-se descritos o local de estágio, assim como as principais atividades nele desenvolvidas, destacando-se o apoio à equipa organizadora na participação da CYBER & CLOUD EXPO, onde foi realizado um ciberexercício para Operadores de Serviços Essenciais do setor das águas. Adicionalmente, foram realizadas a implementação do RJSC em duas grandes entidades, uma do setor aeroportuário e outra do setor público municipal, além da execução de um ciberexercício no SIMAS em Oeiras.

Os métodos utilizados incluíram a aplicação da metodologia de análise de processos para identificação de vulnerabilidades e necessidades de melhoria; a análise de riscos conforme a norma ISO 27005, integrada nos requisitos da ISO 27001 para gestão de segurança da informação, garantindo uma abordagem sistemática para avaliação e tratamento de ameaças; a utilização do Quadro Nacional de Referência para a Cibersegurança, que serviu de base para alinhar as ações ao Regime Jurídico de Segurança do Ciberespaço (RJSC); e a documentação robusta de políticas, procedimentos e resultados, seguindo diretrizes de governança como a ISO/IEC 27002 para controlos de segurança.

Os resultados demonstraram uma melhoria significativa na conformidade com o RJSC, com a implementação bem sucedida de diversas políticas de cibersegurança e aumento na consciencialização dos *stakeholders*. A experiência proporcionou um aprofundamento teórico e prático, refletindo a importância da cibersegurança na proteção dos ativos digitais e da informação dos clientes.

No final do documento, através das conclusões, é realizada uma reflexão crítica dividida por aprendizagens e dificuldades.

Abstract

This internship report describes the activities carried out at the company NECHO TECHLAW, as part of the Master's degree course in Cybersecurity and Computer Systems Auditing. The main objective of the internship was to implement technical and organizational measures to ensure the alignment of the organization's security practices with the requirements of the Legal Framework for Cyberspace Security (RJSC) and other applicable legislation, ensuring compliance.

In the context of the work, various activities were carried out, including the analysis of the current state of technological infrastructures (gap analysis), the development of cybersecurity policies and plans, the preparation of asset inventories and risk analyses, as well as the implementation of training and awareness programs for stakeholders. This report describes the internship location as well as the main activities developed there, including the support to the organizing team in participating in the CYBER & CLOUD EXPO, where a cyber tabletop exercise was conducted for Essential Service Operators in the water sector. Additionally, the RJSC was implemented in two major entities, one in the airport sector and the other in the municipal public sector, besides the execution of a cyber exercise at SIMAS in Oeiras.

The methods used included the application of the process analysis methodology to identify vulnerabilities and needs for improvement; risk analysis according to ISO 27005, integrated into the requirements of ISO 27001 for information security management, ensuring a systematic approach to assessing and dealing with threats; the use of the National Reference Framework for Cybersecurity, which served as the basis for aligning actions with the Legal Framework for Cyberspace Security (RJSC); and the robust documentation of policies, procedures and results, following governance guidelines such as ISO/IEC 27002 for security controls.

The results demonstrated a significant improvement in compliance with the RJSC, with the successful implementation of various cybersecurity policies and increased stakeholder awareness. The experience provided both theoretical and practical insights, reflecting the importance of cybersecurity in protecting clients' digital assets and information.

At the end of the document, through the conclusions, a critical reflection is made, divided by learnings and difficulties.

Résumé

Ce rapport de stage décrit les activités menées au sein de l'entreprise NECHO TECHLAW, dans le cadre du programme de master en cybersécurité et audit des systèmes informatiques. L'objectif principal du stage était de mettre en œuvre des mesures techniques et organisationnelles pour s'assurer que les pratiques de sécurité de l'organisation étaient alignées sur les exigences du cadre juridique pour la sécurité du cyberespace (RJSC) et d'autres législations applicables, garantissant ainsi la conformité.

Dans le contexte du travail, diverses activités ont été réalisées, notamment l'analyse de la situation actuelle des infrastructures technologiques (gap analysis), le développement de politiques et de plans de cybersécurité, la préparation d'inventaires d'actifs et d'analyses de risques, ainsi que la mise en œuvre de programmes de formation et de sensibilisation pour les parties prenantes. Ce rapport décrit le lieu de stage ainsi que les principales activités qui y ont été développées, en mettant en avant le soutien apporté à l'équipe organisatrice pour la participation à la CYBER & CLOUD EXPO, où un exercice cyber de simulation (tabletop exercise) a été réalisé pour les Opérateurs de Services Essentiels du secteur de l'eau. De plus, le RJSC a été mis en œuvre dans deux grandes entités, l'une du secteur aéroportuaire et l'autre du secteur public municipal, ainsi que l'exécution d'un exercice cyber chez SIMAS à Oeiras.

Les méthodes utilisées comprenaient l'application de la méthodologie d'analyse des processus pour identifier les vulnérabilités et les besoins d'amélioration ; l'analyse des risques selon la norme ISO 27005, intégrée aux exigences de la norme ISO 27001 pour la gestion de la sécurité de l'information, garantissant une approche systématique de l'évaluation et du traitement des menaces ; l'utilisation du cadre de référence national pour la cybersécurité, qui a servi de base pour aligner les actions sur le cadre juridique pour la sécurité du cyberespace (RJSC) ; et la documentation solide des politiques, des procédures et des résultats, suivant les lignes directrices de gouvernance telles que la norme ISO/IEC 27002 pour les contrôles de sécurité.

Les résultats ont démontré une amélioration significative de la conformité au RJSC, avec la mise en œuvre réussie de diverses politiques de cybersécurité et une sensibilisation accrue des parties prenantes. L'expérience a fourni des perspectives théoriques et pratiques, reflétant l'importance de la cybersécurité dans la protection des actifs numériques et des informations des clients.

À la fin du document, à travers les conclusions, une réflexion critique est réalisée, divisée par apprentissages et difficultés.

Lista de abreviaturas e siglas

RJSC	Regime Jurídico de Segurança no Ciberespaço.
CNCS	Centro Nacional de Cibersegurança.
ISO	Internacional Organization for Standardization.
TI	Tecnologias de Informação
OSE	Operadores de Serviços Essenciais
CISA	Cybersecurity & Infrasctructure Security Agency
CTEP	CISA Tabletop Exercise Package
TO	Tecnologia Operacional

Índice

Índice de figuras

Índice de tabelas

1. Introdução

Este relatório, elaborado no âmbito do Mestrado em Cibersegurança e Auditoria de Sistemas Informáticos, apresenta e analisa criticamente as atividades desenvolvidas durante o estágio na NECHO TECHLAW, com foco na implementação prática do Regime Jurídico de Segurança do Ciberespaço (RJSC) e na conformidade com legislações complementares. Através da análise de infraestruturas tecnológicas, realização de ciberexercícios e participação em eventos setoriais, o trabalho demonstra como a harmonização entre requisitos legais e medidas técnicas contribuiu para a robustez da segurança digital em contextos corporativos multissetoriais.

O relatório está estruturado de maneira a fornecer uma visão clara e detalhada de todas as etapas do estágio, incluindo o contexto teórico, as atividades realizadas, os métodos utilizados e os resultados alcançados, além de reflexões críticas sobre as aprendizagens e desafios enfrentados ao longo do período de estágio.

1.1. Objetivos

- Descrever detalhadamente o local de estágio e as atividades desenvolvidas.
- Apresentar a aplicação prática do RJSC em diferentes contextos organizacionais.
- Refletir sobre as aprendizagens e desafios enfrentados durante o estágio.
- Propor recomendações com base na experiência adquirida.

1.2. Revisão da Literatura

A revisão da literatura permite contextualizar o trabalho realizado no estágio e fornecer uma base teórica sólida. Esta secção aborda os principais conceitos na área de cibersegurança, destacando a importância da conformidade com legislações e normas de segurança no ciberespaço.

1.2.1. **Cibersegurança**

A cibersegurança é uma componente crucial na proteção de sistemas, redes e programas contra ataques digitais que que têm como alvo informações sensíveis, ganhos financeiros ou operações comerciais (Nifakos et al., 2021). A profissionalização do cibercrime levou a um aumento de ciberameaças sofisticadas e frequentes,

sublinhando a importância da cibersegurança na proteção das infraestruturas digitais (Saeed et al., 2023). O termo cibersegurança engloba a proteção de dispositivos, redes e informações digitais contra o acesso não autorizado, o roubo ou a alteração de dados (Shukur et al., 2023).

A evolução das ciberameaças, como o ransomware (Sophos, 2024) e ataques à cadeia de suprimentos (ex.: incidente CrowdStrike), exige medidas robustas e atualizadas. Estudos demonstram que a adoção de frameworks como o NIST Cybersecurity Framework reduz incidentes em 40% (Gartner, 2024), enquanto a automatização com IA generativa acelera a resposta a ameaças em 53% (SANS, 2024).

A integração da cibersegurança nas iniciativas de digitalização é essencial para mitigar riscos, mas os seus resultados dependem da adoção de estratégias holísticas. Por exemplo:

- **Casos de sucesso**: Em junho de 2017, a empresa de transporte marítimo Maersk enfrentou um dos maiores ciberataques da história: o ransomware NotPetya, inicialmente direcionado à Ucrânia, mas que se espalhou globalmente. O ataque, atribuído a um grupo patrocinado por um Estado-nação, encriptou os sistemas da empresa, paralisando operações em 600 unidades distribuídas por 130 países. Apesar da gravidade, a Maersk recuperou-se em apenas 10 dias, graças a práticas robustas de cibersegurança. Um dos fatores críticos para a rápida recuperação foi a política de backups regulares e redundantes. A empresa mantinha cópias offline de dados essenciais, armazenadas em locais geograficamente dispersos, o que permitiu restaurar sistemas sem ceder ao pagamento do resgate. Além disso, a segmentação de redes isolou setores críticos, como as operações portuárias, impedindo que o ransomware se espalhasse por toda a infraestrutura. A existência de um plano de resposta a incidentes pré-definido também foi decisivo. Uma equipa especializada agiu imediatamente para conter o ataque, comunicar-se com clientes e parceiros, e priorizar a reconstrução de sistemas prioritários. Paralelamente, foram feitas formações regulares de consciencialização em cibersegurança para preparar os funcionários para identificarem ameaças, como phishing (SOS Intelligence, 2024).
- **Falhas críticas**: Em abril de 2024, a rede de lojas mexicana Coppel enfrentou um grave ciberataque realizado pelo grupo de ransomware Lockbit 3.0, um dos mais perigosos do mundo. Durante três meses, o ataque comprometeu mais de 9.500 serviços comerciais, impactando 1.800 lojas físicas, plataformas online,

centros de distribuição e sistemas logísticos. A falha de segurança explorada pelos hackers revelou a falta de preparação da empresa para ameaças de grande escala. Embora os sistemas financeiros do banco da Coppel, operados numa plataforma separada, tenham escapado do comprometimento, os prejuízos financeiros e operacionais foram significativos. O tempo de recuperação, inicialmente estimado em nove meses, foi reduzido para três graças a esforços intensivos, mas o episódio danificou a reputação da empresa e a confiança dos clientes (CyberPeace, 2024).

1.2.2. **Princípios da Cibersegurança**

Os princípios de cibersegurança são fundamentais para a proteção das informações e infraestruturas tecnológicas de uma organização. A adoção de uma abordagem baseada nesses princípios garante que as ameaças e vulnerabilidades possam ser mitigadas de forma eficiente, mantendo a integridade dos sistemas e a continuidade dos negócios. Os três pilares da cibersegurança – confidencialidade, integridade e disponibilidade – formam a base da segurança da informação e são complementados por outros princípios importantes, como a autenticidade e o não-repúdio (Nieles et al., 2017).

Confidencialidade

A confidencialidade visa proteger informações contra acessos não autorizados, exigindo a combinação de tecnologias avançadas e procedimentos rigorosos (Nieles et al., 2017). Na prática, as organizações adotam soluções, como a criptografia homomórfica, que permite processar dados encriptados sem desencriptá-los, aplicada pela IBM em análises de dados de saúde para garantir privacidade em pesquisas clínicas, por exemplo (IBM, n.d.). Sistemas de Identity and Access Management (IAM) também são críticos: a autenticação multifatorial (MFA), implementada por empresas, reduziu violações ao restringir acessos a sistemas críticos (Roopesh, 2024). O controlo de acessos baseado em papéis é usado em hospitais para limitar o acesso apenas a profissionais envolvidos no tratamento (Garg et al., 2021).

A integração de normas de cifragem avançadas e de arquiteturas de segurança modernas representa uma mudança fundamental no panorama da proteção de dados, em especial em sectores sensíveis como o dos cuidados de saúde. Os algoritmos de encriptação robustos, como o AES, são conhecidos pela sua fiabilidade e resistência contra o acesso não autorizado (Al-Khafaji & Rahma, 2022). Além disso, estes avanços

enfrentam desafios de ameaças emergentes, como evidenciado pela resposta às tecnologias de IA generativa. Por exemplo, a proibição de ferramentas como o ChatGPT em Itália foi implementada devido a preocupações com a exposição de dados confidenciais (BBC, 2023).

A trajetória futura da cibersegurança está cada vez mais orientada para a arquitetura Zero Trust, exemplificada pela iniciativa BeyondCorp da Google, que elimina a confiança implícita ao obrigar à autenticação contínua de todos os utilizadores, tanto internos como externos (Alevizos et al., 2021).

Integridade

A integridade da informação é garantida quando os dados permanecem precisos, consistentes e inalterados ao longo de seu ciclo de vida, prevenindo alterações não autorizadas ou acidentais (Nieles et al., 2017). Esta integridade é salvaguardada principalmente através de tecnologias como assinaturas digitais e algoritmos de hashing, especificamente a função de hash SHA-256. O SHA-256, que faz parte da família SHA-2 desenvolvida pelo National Security Agency (NSA), é reconhecido pela sua capacidade de verificar com segurança a integridade dos dados e é utilizado em várias aplicações, incluindo assinaturas digitais e impressões digitais de dados (Prasanna & Premananda, 2021).

A Lei da Resiliência Operacional Digital (DORA) constitui uma medida regulamentar fundamental para as instituições financeiras, exigindo a implementação de auditorias automatizadas e medidas de redundância de dados para evitar falhas operacionais (Buttigieg & Zimmermann, 2024). A DORA estabelece uma resposta estruturada às complexas exigências da resiliência digital, colocando uma forte ênfase em práticas abrangentes de gestão do risco nas instituições financeiras (Clausmeier, 2022). Além disso, persistem desafios relacionados com a implementação da DORA, principalmente ligados à complexidade dos processos internos das empresas e ao investimento substancial necessário para o cumprimento (Maryška et al.,2024).

No domínio do combate à desinformação, o Observatório Europeu dos Meios de Comunicação Social (EDMO) desempenha um papel fundamental na identificação da desinformação através da utilização de algoritmos concebidos para detetar alterações nos conteúdos digitais (European Commission, 2024). Uma manifestação particularmente difícil de desinformação é a tecnologia deepfake, que é uma das formas mais eficazes de enganar, ao colocar, em vídeo, pessoas a exprimirem palavras que

nunca disseram, ou mesmo substituir caras, criando, assim, situações falsas (Department of Homeland Security, n.d.).

A transformação digital em Portugal, acelerada por setores público e privado, trouxe avanços tecnológicos e maior exposição a ciberameaças como ransomware e phishing, conforme destacado no Relatório de Segurança 2024 da Check Point. A integridade dos sistemas e dados tornou-se prioridade nacional, com esforços para proteger infraestruturas críticas e promover uma cultura de cibersegurança robusta. Apesar de iniciativas governamentais e colaboração intersetorial, persistem lacunas estratégicas: menos de metade das empresas possuíam políticas formais de segurança da informação em 2023, revelando fragilidades na prevenção e resposta a incidentes (Apcer, 2024).

Os desafios emergentes no panorama tecnológico atual estão cada vez mais ligados à inteligência artificial (IA) generativa e às ameaças à cibersegurança. Os sistemas de IA generativa, como o ChatGPT, embora poderosos, apresentam riscos ao gerar informações potencialmente enganosas ou falsas. Este facto levou a iniciativas centradas na verificação em tempo real do conteúdo gerado para mitigar a desinformação (Hamidu et al., 2023). A necessidade dessa verificação é fundamental num mundo em que as aplicações de IA podem influenciar a opinião pública e a tomada de decisões (Adu et al., 2024).

Disponibilidade

A disponibilidade refere-se à garantia de que os sistemas de informação e os dados estão acessíveis sempre que tal se justifique. Este princípio é crítico para operações comerciais sustentadas, particularmente no contexto de crescentes ciberameaças e falhas técnicas, onde a redundância e a resiliência são essenciais (Umam et al., 2018). Zeebaree et al. (2020) retratam especificamente o papel crítico que a disponibilidade desempenha contra ataques de negação de serviço distribuído (DDoS), enfatizando a necessidade de infraestruturas robustas que possam resistir a tais ataques. Esta afirmação é apoiada por várias normas, incluindo o NIST Cybersecurity Framework, que defende a redundância de infraestruturas e o planeamento da recuperação de desastres como meios de mitigar potenciais períodos de inatividade (Yu et al., 2024).

Na Europa, a Diretiva SRI obriga operadores de serviços essenciais (ex.: transportes, energia) a implementar redundância e testes de *stress* regulares, de forma a prevenir a indisponibilidade dos dados, garantido a continuidade dos serviços e

prevenindo e minimizando o impacto de incidentes (Markopoulou et al., 2019). Tecnologicamente, ferramentas como o AWS Shield Advanced protegem empresas globais contra ataques DDoS, garantindo disponibilidade contínua.

1.2.3. **Ataques**

Tabela 1. *Tipos de Ciberataques*

Tipo de Ataque	Descrição	Autores
Ransomware	Criptografa dados e exige resgate para libertação. Evoluiu para "dupla extorsão": roubo de dados antes da criptografia.	O'Kane et al., 2018
Phishing	Mensagens falsas (e-mails, SMS) para roubo de dados ou instalação de malware. Usa IA para personalização.	Gupta et al., 2016
Ataques DDoS	Sobrecarrega servidores com tráfego malicioso para derrubar serviços. Alvo comum: setores críticos como educação e saúde.	Jaafar et al., 2019
SQL Injection	Insere código malicioso em bases de dados para roubo ou manipulação de dados.	Abdullayev & Chauhan, 2023
Man-in-the-Middle (MitM)	Interceta comunicações entre cliente e servidor para roubar dados. Comum em redes Wi-Fi públicas.	Mallik et al., 2019
Ameaça Persistente Avançada (APT)	Ataques prolongados para infiltrar sistemas e roubar dados sensíveis. Frequentemente ligados a grupos patrocinados por Estados.	Khalid et al., 2021
Cryptojacking	Usa recursos de dispositivos para minerar criptomoedas sem autorização. Reduz desempenho e aumenta custos energéticos.	Tekiner et al., 2021
Exploração de IoT	Ataques a dispositivos conectados (câmaras, sensores) com segurança precária. Causa interrupções operacionais.	Butun et al., 2020
Deepfakes e Engenharia Social	Uso de áudios/vídeos falsos para fraudes executivas. Exemplo: falsas autorizações de transferências bancárias.	Almars, 2021

Fonte: própria

Exemplos empresariais e Soluções

Em 2024, a operadora espanhola Orange sofreu um ataque de hijacking BGP, onde cibercriminosos redirecionaram parte do tráfego de internet para servidores não autorizados, causando interrupções generalizadas. A empresa adotou protocolos de verificação de rotas BGP (RPKI) e segmentação de redes críticas, mitigando riscos futuros. Este ataque destacou a fragilidade de

infraestruturas de telecomunicações europeias frente a técnicas avançadas de redireccionamento (Bleeping Computer, 2024).

Também em 2024, o banco Santander foi alvo de um ataque informático à sua base de dados. Houve um acesso não autorizado a uma base de dados alojada num fornecedor e dados de alguns clientes, empregados e antigos empregados foram acedidos. O banco implementou, de imediato, medidas para lidar com o incidente, incluindo o bloqueio do acesso à base de dados e o reforço da prevenção de fraudes para proteger os clientes (Jornal de Negócios, 2024).

Em setembro de 2024, a Transport for London teve dados de 5.000 utilizadores expostos, incluindo informações bancárias, após um ciberataque que afetou sistemas de pagamento *contactless*. O prejuízo atingiu 5 milhões de libras. A empresa reforçou a criptografia de dados em trânsito e adotou monitorização contínua com ferramentas SIEM (Transport for London, 2024).

Ainda nesse ano, um caso emblemático envolveu mensagens fraudulentas enviadas em nome de empresas como a EDP, CTT ou DPD, que simulavam cobranças urgentes para induzir pagamentos. Um exemplo recorrente é o SMS falsificado da "EDP" com erros grosseiros, como a palavra *PENTENTE* (no lugar de *pendente*), alertando sobre supostas faturas em atraso e ameaçando corte de serviço caso o pagamento não fosse feito até uma data específica. Essas mensagens, sem número de telefone associado e com valores discrepantes das faturas reais, incluíam links ou entidades de pagamento falsas, explorando a pressa psicológica e a falta de atenção a detalhes como erros ortográficos (Visão, 2024).

1.2.4. **Medidas Preventivas**

Tabela 2. *Medidas Preventivas*

Categoria	Medida Preventiva	Controlo ISO	Exemplo de Aplicação
Gestão de Acessos	Implementar autenticação multifator (MFA) e controlo baseado em papéis.	ISO 27002:2022 8.1; 8.5; 8.18	Bancos utilizam MFA para transações online, reduzindo fraudes.
Proteção de Dados	Utilizar criptografia (AES-256) e tokens para dados sensíveis.	ISO 27002:2022 8.24; 8.11	Plataformas de pagamento utilizam tokens para evitar fugas.
Segurança Física	Restringir acesso físico a servidores e adotar monitorização por vídeo	ISO 27002:2022 7.1; 7.4	Data centers utilizam biometria e logs de acesso.
Resposta a Incidentes	Criar planos de contingência e realizar simulações de ransomware.	ISO 27001:2022 A.5.24; A.5.26	Empresas europeias testam recuperação de backups após ataques.

Treino	Programas de consciencialização em phishing e engenharia social para colaboradores.	ISO 27002:2022 6.3	PMEs portuguesas reduziram cliques maliciosos em 60% com treinos simulados.
Gestão de Vulnerabilidades	Realizar varreduras regulares e aplicar patches de segurança.	ISO 27002:2022 8.8	Empresas de energia atualizam sistemas SCADA para mitigar riscos em IoT.
Proteção de Redes	Implementar firewalls de última geração e segmentação de redes.	ISO 27002:2022 8.20; 8.22	Hospitais isolam redes médicas de sistemas administrativos para evitar invasões.
Conformidade Legal	Alinhar políticas à LGPD e RGPD, com cláusulas contratuais para fornecedores.	ISO 27002:2022 5.34	Empresas brasileiras usam a ISO 27002 para mapear requisitos da LGPD.
Monitorização Contínua	Usar SIEM (Security Information and Event Management) para deteção de anomalias.	ISO 27002:2022 8.16	Companhias aéreas monitorizam acessos suspeitos em tempo real.

Fonte: própria

As medidas preventivas não se limitam a tipos específicos de ataques, mas envolvem uma abordagem holística, como propõem as normas ISO 27001 e 27002. A combinação de controlos técnicos (ex.: criptografia), processos (ex.: gestão de riscos) e fatores humanos (ex.: treino) cria uma estrutura resiliente.

1.2.5. **Ciberespaço**

Definição e Âmbito

O ciberespaço é um ambiente global composto por redes digitais, sistemas de informação e interações virtuais, que engloba desde infraestruturas críticas (energia, saúde, finanças) até plataformas de comunicação e dispositivos IoT (Zhang et al., 2015). É conhecido como a "quinta fronteira" e a sua relevância estratégica decorre da dependência de sociedades e economias em tecnologias digitais e da exposição a ameaças transnacionais, como ciberataques e desinformação (Institute for Defense Analyses, 2011).

Quinta Fronteira

A designação de "quinta fronteira" surge da necessidade de proteger um domínio operacional distinto dos tradicionais, mas igualmente crítico para a soberania e segurança nacional. Assim como as fronteiras físicas exigem defesa militar, o

ciberespaço requer mecanismos específicos para combater ameaças como ransomware, espionagem e sabotagem de infraestruturas (Institute for Defense Analyses, 2011). Esta visão foi formalizada pela NATO em 2016, no Summit de Varsóvia, que integrou o ciberespaço como área de operações, igualando as outras quatro fronteiras: terra, água, ar e espaço (NATO, 2016).

Exemplos de Implementação Estratégica

NATO e a Adaptação Militar:

A Aliança Atlântica adotou a metodologia DOTMLPFI (Doutrina, Organização, Treino, Material, Liderança, Pessoal, Instalações e Interoperabilidade) para sistematizar operações no ciberespaço. Isso inclui a criação de comandos especializados e exercícios conjuntos para simular ataques a redes críticas (Instituto da Defesa Nacional).

Soberania cibernética e Controlo Estadual:

Países como Portugal e membros da UE estão a estabelecer "fronteiras digitais" para regular fluxos de dados e combater interferências externas. Isso inclui a criação de leis como o RGPD e mecanismos de resposta rápida a incidentes, como o CERT.PT.

Vulnerabilidades

Tabela 3. *Vulnerabilidades*

Vulnerabilidade	Exemplo
Ataques a Infraestruturas	Ataques DDoS a redes elétricas na Europa
Espionagem Estratégica	Grupos APT (Ameaças Persistentes Avançadas) ligados a Estados.
Desinformação	Campanhas de manipulação em redes sociais durante eleições.
Ameaças Físicas	Acesso não autorizado a infraestruturas críticas (data centers, redes elétricas).
Novas Ameaças	Uso de IA generativa para criar phishing personalizado ou deepfakes.
Complexidade e Escala	Ataques à cadeia de suprimentos que afetam múltiplas organizações simultaneamente.

Fonte: própria

1.2.6. Visão Geral dos Regimes de Segurança Jurídica no Ciberespaço

O panorama jurídico da cibersegurança não segue um modelo único, mas é marcado por abordagens regionais e setoriais. A União Europeia (UE) destaca-se como

líder regulatória com instrumentos como a Diretiva NIS2 (2022/2555), que estabelece padrões rigorosos para infraestruturas críticas e serviços essenciais, incluindo saúde, energia e transportes. A UE serve como referência para países como Portugal, que adaptaram as suas leis para transpor diretivas europeias, criando um regime jurídico alinhado à cooperação transnacional e à resiliência digital (Diário de Notícias, 2024).

A falta de um tratado global vinculativo torna o cenário fragmentado e desafiador. Manuel da Costa Cabral (2024) aponta que a "soft law" (normas não obrigatórias) e a divergência geopolítica impedem a criação de uma convenção única, como uma Convenção Internacional para a Cibersegurança.

Exemplos práticos incluem:

- Fragmentação Regulatória: Empresas multinacionais enfrentam requisitos conflituantes, como a Diretiva NIS2 na UE versus leis locais na Ásia ou EUA.
- Sobrecarga de Conformidade: os CISOs europeus relatam que é muito complexo o cumprimento de múltiplas normas.
- Falta de Padronização: Enquanto a UE exige notificação de incidentes em 24 horas, outros países têm prazos mais flexíveis, gerando inconsistências.

Ciberterrorismo

- Ciberataques à Rede Energética Ucraniana: Em 2016 e 2022, a Rússia usou malware (Industroyer One e Two) para desligar circuitos elétricos em Kiev e outras regiões. O malware automatizado atacou sistemas de controlo de subestações, causando apagões localizados (UC Santa Cruz, 2024).
- Vulnerabilidades nas energias Renováveis: A transição para energias renováveis na Europa aumentou riscos, já que painéis solares e redes digitais são alvos potenciais. Ataques aos mesmos podem causar desequilíbrios na rede (NewsRoom, 2024).
- Ataques à Cadeia de Suprimentos: Em 2020, o ataque ao software SolarWinds Orion comprometeu governos e empresas globais. Cibercriminosos inseriram malware em atualizações legítimas, espiando dados estratégicos por meses. Este caso ilustra como ataques a fornecedores podem ter alcance transnacional (Zscaler, n.d.).

- Destruição Total de Dados em Portugal: Em 2022, dois dos oito grandes ciberataques em Portugal resultaram na destruição completa de dados, incluindo backups. Organizações como o Hospital Garcia de Orta e empresas de energia tiveram as suas operações paralisadas por semanas, com impactos económicos e sociais graves (CNN Portugal, 2022).

As medidas jurídicas regionais são cruciais para proteger a informação e garantir a segurança dos sistemas informáticos. Estas medidas têm como objetivo salvaguardar a segurança do Estado, a saúde pública e a moralidade, enquanto abordam os desafios colocados pela informatização da sociedade (Avdeev et al., 2020). Em setores específicos, como a aviação, os quadros jurídicos existentes estão a ser adaptados para responder aos desafios únicos colocados pelas ciberameaças, como por exemplo através de testes de stress cibernético, com simulações de ataques, proteção de dados em tempo real, certificação de fornecedores e parceiros, protocolos de emergência e colaboração internacional, realçando a natureza interdisciplinar do direito da cibersegurança (Klenka, 2021).

Para promover a estabilidade no ciberespaço, é necessário um regime internacional de normas que regule o comportamento dos Estados. Este regime deve complementar as estratégias de dissuasão cibernética e ser aplicado por uma autoridade capaz de garantir o seu cumprimento, como o Conselho de Segurança da ONU. O estabelecimento de tais normas é essencial para manter a estabilidade geopolítica e abordar as operações cibernéticas patrocinadas pelo Estado (Taddeo, 2018).

1.2.7. **Regime Jurídico de Segurança no Ciberespaço**

O Regime Jurídico da Segurança no Ciberespaço (RJSC) em Portugal é uma estrutura reguladora fundamental que visa salvaguardar as infraestruturas críticas e reforçar a segurança da informação nos setores público e privado. Este quadro foi estabelecido em resposta à crescente prevalência de ciberameaças, alinhando-se com as diretivas da União Europeia, particularmente a Diretiva SRI, que enfatiza a necessidade de os prestadores de serviços essenciais aderirem a normas de segurança rigorosas (Fuster & Jasmontaite, 2020). O RJSC é parte integrante do quadro jurídico europeu mais vasto relativo à cibersegurança, que procura harmonizar as medidas de

cibersegurança entre os estados-membros, reforçando assim a resiliência coletiva contra as ciberameaças (Taherdoost, 2022).

O RJSC estabelece que as organizações devem adotar uma abordagem à gestão da segurança baseada no risco, seguindo normas internacionais como a ISO 27001, 27002 e 27005, para a implementação de sistemas de gestão da segurança da informação (Assembleia da República, 2018). A ISO 27001 é a norma central da família ISO 27000, focada na criação de um Sistema de Gestão de Segurança da Informação (SGSI). O seu objetivo é garantir a confidencialidade, integridade e disponibilidade dos dados por meio de uma abordagem baseada em riscos (ISO/IEC 27001:2022). A ISO 27002 é um manual prático que detalha como aplicar os 93 controlos listados no Anexo A da ISO 27001. A sua função é responder aos problemas da segurança, oferecendo orientações específicas para cada controlo (ISO/IEC 27002:2022). A ISO 27005 complementa a ISO 27001 ao fornecer uma metodologia estruturada para avaliação e tratamento de riscos. É essencial para organizações que procuram aprofundar a análise de ameaças (ISO/IEC 27005:2022).

Estas abordagens envolvem a criação de planos de segurança, a formação contínua dos colaboradores e a aplicação de práticas avançadas de segurança, como a segregação de redes e a proteção de dados pessoais. As empresas são também incentivadas a efetuar auditorias periódicas e a manter relatórios anuais que documentem as suas práticas de cibersegurança, oferecendo maior transparência e resiliência contra ataques (Antunes et al., 2021).

Nos termos do RJSC, e de acordo com a Lei n.º 46/2018 de 13 de agosto, os Operadores de Serviços Essenciais (OSE) e os Prestadores de Serviços Digitais estão obrigados a implementar medidas robustas de segurança da informação, a efetuar avaliações de risco e a comunicar prontamente incidentes de cibersegurança às autoridades competentes. Este requisito regulamentar é crucial para promover uma postura proativa de cibersegurança entre as organizações, permitindo-lhes mitigar eficazmente os riscos e cumprir as obrigações legais.

1.2.8. **Centro Nacional de Cibersegurança (CNCS)**

O Centro Nacional de Cibersegurança (CNCS) é a entidade portuguesa responsável por coordenar a segurança digital do país, garantindo que organizações públicas e privadas adotem medidas robustas contra ciberameaças. A sua atuação abrange desde a definição de políticas nacionais até a resposta prática a incidentes, com impacto direto na resiliência de setores críticos (CNCS, n.d.).

O CNCS lidera a Estratégia Nacional para a Segurança do Ciberespaço, focada em três eixos: resiliência, inovação e capacitação. Desenvolveu o Quadro Nacional de Referência para a Cibersegurança (QNRCS), que define requisitos mínimos como autenticação multifatorial (MFA) e gestão de backups (CNCS, n.d.).

O CNCS protagoniza o Exercício Nacional de Cibersegurança, onde simula ataques em larga escala para testar a prontidão de entidades. Em 2024, os exercícios foram dedicados ao Setor da Energia, com um cenário centrado em ameaças de cibersegurança dirigidas à infraestrutura energética da UE, decorrentes de atritos causados pela tensão geopolítica entre a União Europeia e uma nação estrangeira fictícia (CNCS, n.d.).

1.2.9. **Diretiva SRI (NIS Directive)**

A Diretiva relativa aos Sistemas de Redes e Informação (SRI) é o primeiro instrumento jurídico da UE a centrar-se na notificação de incidentes e na partilha de informações como requisitos fundamentais, com base em estudos que demonstram a importância dessas informações para a defesa cibernética (Ducuing, 2021). Define as infraestruturas críticas e os operadores de serviços essenciais, impulsionando melhorias na cibersegurança dos serviços (Bagnato, 2020; Wallis & Johnson, 2020). Além disso, moderniza o quadro jurídico da UE em relação à cibersegurança e procura reforçar a resiliência e a resposta da UE aos ciberataques (Ferguson, 2022). O setor privado tem assistido a uma mudança de papel na regulamentação da SRI, deixando de ser objeto de regulamentação para se tornar um agente ativo na definição de políticas, fornecendo conhecimentos técnicos para a resiliência das redes (Carrapico & Farrand, 2016). Além disso, a Diretiva SRI coloca desafios na prática, exigindo quadros de conformidade e de avaliação da maturidade da cibersegurança (Biasin & Kamenjašević, 2022).

A Diretiva SRI foi objeto de uma reforma, que conduziu à proposta da Diretiva SRI 2, que procura modernizar o quadro jurídico da UE em vigor relativo à cibersegurança, corrigindo simultaneamente as deficiências que impediram a Diretiva SRI de desbloquear todo o seu potencial (Chiara, 2022). Além disso, a Diretiva SRI tem implicações para vários setores, incluindo os cuidados de saúde, como se vê no contexto dos desafios de cibersegurança decorrentes da Lei da IA e das propostas da Diretiva SRI 2 para dispositivos médicos (Biasin & Kamenjašević, 2022). A literatura também enfatiza a importância do diálogo, da parceria e da capacitação para a segurança das redes e da informação, destacando a mudança do papel do setor privado de objeto de regulamentação para formador de regulamentação no contexto da Diretiva

SRI (Carrapico & Farrand, 2016). De um modo geral, a Diretiva SRI representa um passo significativo dado pela UE para reforçar a segurança das redes e dos sistemas de informação, com implicações para vários sectores e um destaque na notificação de incidentes, na partilha de informações e na modernização dos quadros jurídicos da cibersegurança.

1.2.10. **Gestão de Incidentes de Segurança**

No domínio da cibersegurança, a gestão eficaz dos incidentes de segurança é fundamental para as organizações que pretendem defender-se contra uma série de ameaças. Os sistemas de gestão de incidentes de segurança são compostos por ferramentas tecnológicas (por exemplo, ferramentas de gestão de Informações e Eventos de Segurança (SIEM) e ferramentas de orquestração, automatização e resposta de segurança (SOAR)), metodologias padronizadas e equipas especializadas (por exemplo, CSIRTs) (Bhatt et al., 2014). Funcionam em quatro etapas: deteção, análise, resposta e recuperação. Em Portugal, existe o CERT.PT, que utiliza a plataforma *MISP* para partilhar conhecimentos sobre ameaças.

Estes sistemas desempenham um papel crucial neste cenário, fornecendo capacidades de monitorização, registo e análise em tempo real que facilitam a deteção rápida de atividades maliciosas. Estes sistemas evoluíram significativamente, integrando funcionalidades avançadas como a análise de grandes volumes de dados para aumentar a sua eficácia na identificação de áreas de alto risco e na mitigação de potenciais ameaças (González-Granadillo et al., 2021).

A abordagem proativa da procura de ameaças e a utilização de análises avançadas são boas práticas essenciais no domínio da cibersegurança. Estas estratégias permitem que as organizações se mantenham à frente das ciberameaças em evolução, identificando vulnerabilidades antes de estas poderem ser exploradas (Tuyishime, 2023). A integração de inteligência artificial (IA) e machine learning (ML) melhora a deteção e resposta a incidentes através de métodos como análise de anomalias, como a DarkTrace, automação de respostas via plataformas SOAR, como o *IBM Resilient*, e análise preditiva de ameaças, por exemplo *CrowdStrike Falcon* (Ban et al., 2023). A melhoria contínua através de atividades pós-incidente, como a análise da causa raiz e a partilha de conhecimentos, é vital para aumentar a resiliência organizacional. Este processo de aprendizagem iterativa permite que as organizações aperfeiçoem as suas políticas e defesas com base nos conhecimentos adquiridos em incidentes anteriores (Oriola et al., 2021).

1.2.11. **Aplicação e monitorização da conformidade**

A conformidade com a cibersegurança é crucial para as organizações protegerem os seus ativos digitais e manterem a confiança das partes interessadas. A aplicação eficaz e os mecanismos de monitorização são essenciais para garantir a adesão às políticas e regulamentos de cibersegurança (Marotta & Madnick, 2021).

Mecanismos de controlo da conformidade

- Auditorias e certificações: As auditorias internas desempenham um papel significativo na aplicação da conformidade em relação à cibersegurança, fornecendo uma avaliação objetiva da postura de segurança de uma organização. Ajudam a identificar vulnerabilidades e a garantir a adesão às políticas e regulamentos de cibersegurança (Krykliy & Pavlenko, 2019). As certificações, como a ISO/IEC 27001, também servem de referência para a conformidade, fornecendo um quadro estruturado para a gestão da segurança da informação (Harris & Martin, 2021).
- Sanções e enquadramentos legais: O incumprimento da regulamentação pode resultar em sanções graves, incluindo multas e ações judiciais. As organizações devem estar cientes das leis e regulamentos aplicáveis às suas operações para evitar essas consequências (Harris & Martin, 2021). A convergência das normas globais de cibersegurança realça a importância de abordagens regulamentares harmonizadas para impor a conformidade de forma eficaz (Uzougbo et al., 2024).

Ferramentas de controlo e auditoria

- Sistemas de auditoria interna: As auditorias internas são ferramentas preventivas que ajudam a monitorizar a conformidade com a cibersegurança, avaliando a eficácia das medidas de segurança e identificando áreas de melhoria. São essenciais para assegurar a proteção contínua dos ativos e infraestruturas de informação (Krykliy & Pavlenko, 2019).
- Auditoria de sistemas de informação: Trata-se de avaliar as práticas de segurança dos utilizadores de tecnologia numa organização. Os auditores podem identificar incumprimentos e recomendar programas de formação e motivação para promover comportamentos pró-segurança entre os funcionários (Stafford et al., 2018).

Consequências da Não Conformidade

- Riscos legais e financeiros: A não conformidade com os regulamentos de cibersegurança pode levar a repercussões legais e financeiras significativas, incluindo multas, processos judiciais e potencial falência. As organizações devem implementar programas de conformidade robustos para mitigar esses riscos (Harris & Martin, 2021).
- Riscos de reputação: Deixar de proteger os dados dos clientes e outras informações confidenciais pode prejudicar gravemente a reputação de uma organização, levando à perda da confiança do cliente e de oportunidades de negócios. A manutenção da conformidade é crucial para preservar a reputação e a vantagem competitiva de uma organização (Harris & Martin, 2021).

1.2.12. **Tendências e desafios futuros na cibersegurança**

Na cibersegurança, as organizações enfrentam inúmeros desafios e oportunidades devido às tecnologias emergentes e à evolução das ameaças.

As ciberameaças estão a tornar-se cada vez mais sofisticadas, tirando partido da Inteligência Artificial e da aprendizagem automática para contornar as medidas de segurança tradicionais, o que complica os esforços de conformidade (Familoni, 2024). O aumento das ameaças persistentes avançadas (APT) e de outros vetores de ataque complexos exige uma inteligência proativa contra ameaças e mecanismos de defesa adaptados para manter a conformidade com as normas regulamentares (Obi et al., 2024).

A crescente complexidade das ameaças cibernéticas exige que as organizações adotem estratégias de cibersegurança adaptativas e proativas, capazes de integrar as tecnologias mais recentes e fomentar a colaboração intersetorial para enfrentar os desafios em constante evolução (Sendjaja et al., 2024). Essas estratégias devem incluir monitorização contínua, partilha de informações sobre ameaças e atualizações regulares nos protocolos de segurança, garantindo a capacidade de responder a novas vulnerabilidades e atender aos requisitos regulamentares em constante mudança (Saeed et al., 2023).

2. Descrição da Empresa

2.1. História e Missão

A NECHO TECHLAW é uma empresa especializada em serviços de consultoria e soluções tecnológicas ligadas à cibersegurança e conformidade legal. Fundada com o objetivo de proteger as infraestruturas digitais das organizações, a NECHO TECHLAW combina *expertise* em segurança da informação com um profundo entendimento das exigências regulatórias, oferecendo um conjunto abrangente de serviços para mitigar riscos cibernéticos e garantir a conformidade normativa.

2.2. Visão e Valores

A visão da NECHO TECHLAW é ser reconhecida como uma líder no setor de cibersegurança, destacando-se pela inovação, excelência e compromisso com a proteção das informações dos seus clientes. Os valores que guiam a empresa incluem integridade, competência, inovação e um foco centrado no cliente. Estes valores são refletidos em todas as suas operações e na abordagem personalizada aos desafios específicos de cada cliente.

2.3. Estrutura Organizacional

A estrutura organizacional da NECHO TECHLAW é projetada para facilitar uma resposta rápida e eficaz às necessidades dos clientes. A empresa é composta por equipas especializadas em:

- Consultoria de Cibersegurança: Focada na análise de riscos, desenvolvimento de políticas de segurança e implementação de medidas de proteção.
- Conformidade Legal: Especialistas em regulamentações de cibersegurança, incluindo o Regime Jurídico de Segurança do Ciberespaço (RJSC) e outras legislações relevantes.
- Desenvolvimento de Soluções: Engenheiros e desenvolvedores que criam e mantêm ferramentas e plataformas para melhorar a segurança da informação.
- Formação e Sensibilização: Equipa dedicada a programas de treino e consciencialização para *stakeholders* internos e externos.

2.4. Áreas de Atuação

A NECHO TECHLAW atua em diversas áreas da cibersegurança e conformidade, oferecendo serviços que incluem:

- Análise e Gestão de Riscos: Identificação e mitigação de vulnerabilidades em sistemas de TI.
- Implementação de Normas e Regulamentos: Ajuda empresas a cumprir com requisitos legais e normativos.
- Desenvolvimento de Políticas de Segurança: Criação de políticas e procedimentos personalizados para cada cliente.
- Ciberexercícios e Simulações: Realização de exercícios práticos para preparar organizações para responder a ciberincidentes.
- Consultoria em Infraestruturas Críticas: Foco em setores que exigem proteção robusta.

2.5. Principais Projetos

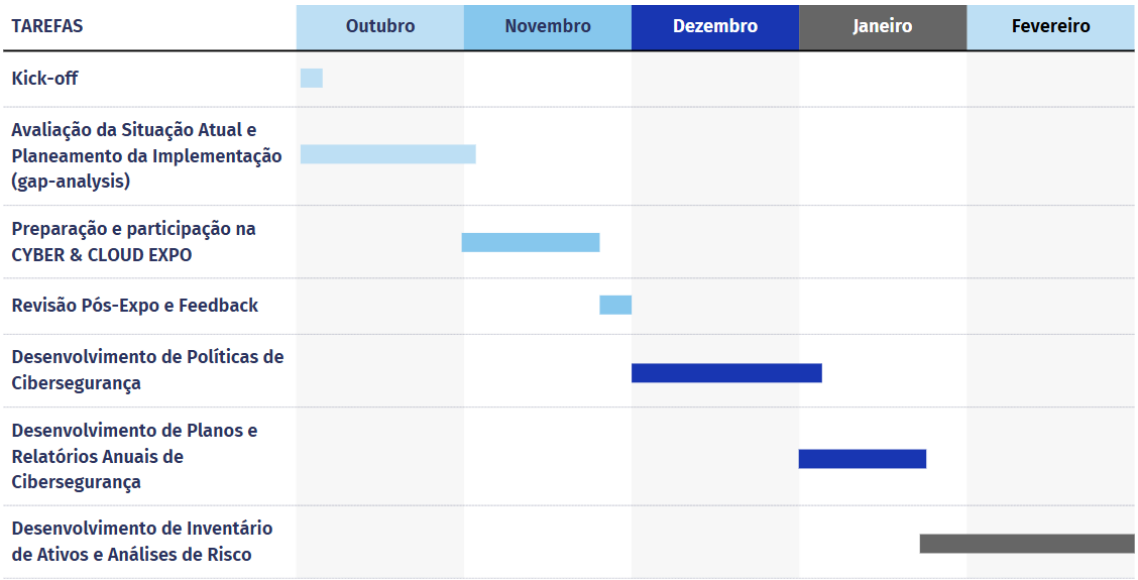
Ao longo dos anos, a NECHO TECHLAW tem se destacado em projetos de grande relevância, incluindo:

- Participação em Eventos de Cibersegurança: Como a CYBER & CLOUD EXPO, onde a empresa organiza ciberexercícios, sessões de treino e palestras.
- Implementação de Conformidade com o RJSC: Realização de projetos para garantir que grandes entidades do setor público e privado estejam em conformidade com as regulamentações de cibersegurança.
- Desenvolvimento de aplicações: Ferramentas inovadoras para gestão de riscos e conformidade, como é o caso da CYBERSECURE.

3. Atividades Desenvolvidas

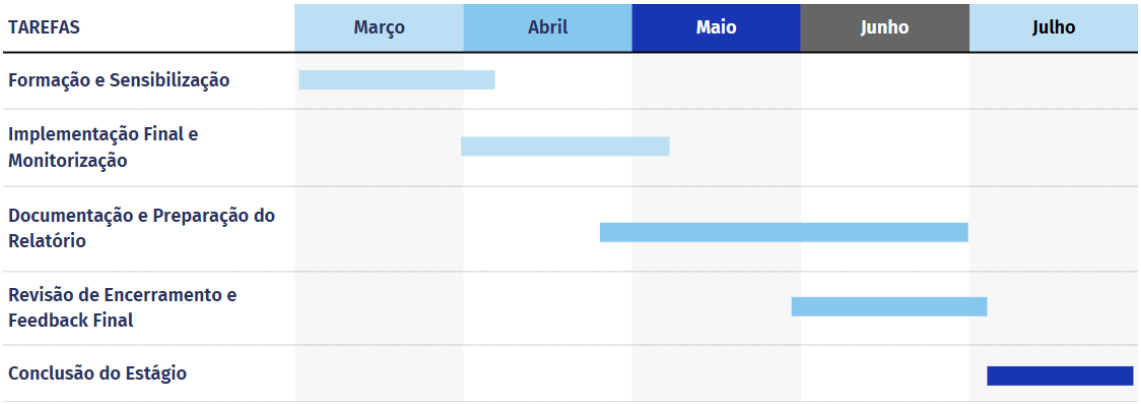
3.1. Cronograma Inicial do Estágio

Figura 1. *Cronograma*



Fonte: Própria

Figura 2. *Cronograma*



Fonte 1: Própria

- Kick-off do Projeto: Início oficial do estágio, com uma reunião inicial para definir expectativas e objetivos;
- Avaliação da Situação Atual e Planeamento da Implementação (gap-analysis): Análise da infraestrutura tecnológica e planeamento da implementação do regime jurídico;
- Preparação e participação na CYBER & CLOUD EXPO: Organização logística, definição do plano para o cyber tabletop exercise, e preparação de materiais e

equipamentos. Realização do cyber tabletop exercise para Operadores de Serviços Essenciais do sector das águas e representação da organização no evento.

- Revisão Pós-Expo e Feedback: Avaliação da participação no evento, recolha de feedback e identificação de áreas de melhoria;
- Desenvolvimento de Políticas de Cibersegurança: Desenvolvimento e implementação de Políticas e Procedimentos com base na avaliação inicial e nos insights da gap analyses;
- Desenvolvimento de Planos de Cibersegurança e Relatórios Anuais de Cibersegurança: Desenvolvimento e implementação de Planos de Cibersegurança e Relatórios Anuais com base na avaliação inicial;
- Desenvolvimento de Inventário de Ativos e Análises de Risco: Desenvolvimento de Inventário de Ativos e respetivas Análises de Risco. Desenvolvimento de Planos de Ação com base na avaliação de risco;
- Formação e Sensibilização: Sessões de formação para as equipas e revisão das políticas. Elaboração de Plano de Comunicação Interna;
- Implementação Final e Monitorização: Implementação final da políticas em toda a organização e monitorização contínua para garantir conformidade;
- Documentação e Preparação do Relatório: Compilação de documentação relativa ao projeto e preparação do relatório final de estágio;
- Revisão de Encerramento e Feedback Final: Reuniões finais para avaliar o desempenho, recolher feedback e definir passos futuros;
- Conclusão do Estágio: Encerramento oficial do estágio.

3.2. Realização de Ciberexercícios

Os ciberexercícios desempenham um papel crucial no fortalecimento da preparação de uma organização para responder eficazmente a uma variedade de ciberameaças (Ukwandu et al., 2020). Estes exercícios proporcionam ambientes simulados onde as equipas de TI e de segurança da informação podem aprofundar o seu conhecimento dos ciberataques e praticar a aplicação de contramedidas eficazes para atenuar as violações (Ukwandu et al., 2020). Ao modelar os ciberataques, as organizações podem poupar recursos e preparar-se melhor para potenciais incidentes (Al-Mohannadi et al., 2016). A importância dos ciberexercícios pode ser destacada pelos seguintes aspetos:

- Avaliação de Capacidades: os ciberexercícios permitem que as organizações avaliem a eficácia das suas políticas e procedimentos de cibersegurança em situações reais.
- Treino Prático: Oferecem um ambiente seguro para que os funcionários pratiquem a resposta a incidentes, melhorando as suas habilidades e confiança.
- Identificação de Lacunas: Ajudam a identificar vulnerabilidades e lacunas nos sistemas de segurança, permitindo que as organizações façam melhorias proativas.
- Consciencialização: Aumentam a consciencialização dos funcionários sobre ciberameaças e a importância de práticas de segurança robustas.
- Melhoria Contínua: Fornecem *feedback* valioso que pode ser usado para ajustar e melhorar as políticas e procedimentos de segurança.
- Cooperação e Coordenação: Fortalecem a cooperação entre diferentes departamentos e equipas, promovendo uma resposta coordenada a ciberincidentes.

3.2.1. CYBER & CLOUD Expo

Um dos ciberexercícios realizados durante o estágio foi na CYBER & CLOUD Expo. Este evento reuniu Operadores de Serviços Essenciais (OSEs) do setor das águas, para um exercício de simulação de um ciberataque. O objetivo principal foi testar e melhorar a capacidade de resposta dos OSEs a ciberincidentes.

O ciberexercício realizado foi estruturado como um jogo. O formato do jogo foi explicado aos participantes, detalhando as regras e o fluxo do exercício. Foi incluída a explicação sobre como seriam enviados os *injects* e como é que os participantes deveriam responder aos mesmos. No fim, consoante os acertos, teriam uma pontuação. O cenário deste jogo, simulava uma situação onde os sistemas do controlo de águas estavam sob ataque, representando desafios significativos para a continuidade dos serviços essenciais.

Os participantes foram organizados em equipas com funções específicas, incluindo CEO, Tecnologia (TECH), Legal e Comunicação. Cada grupo recebeu um tempo limitado para responder aos *injects*, tomando decisões críticas de acordo com sua área de responsabilidade. As decisões dos CEOs envolviam estratégias gerais de mitigação, enquanto a equipa TECH focava na resposta técnica ao incidente. A equipa Legal avaliava as implicações jurídicas das ações, e a equipa da Comunicação geria a comunicação interna e externa durante a crise.

3.2.2. Ciberexercício no SIMAS, em Oeiras

O ciberexercício no SIMAS em Oeiras seguiu um formato similar ao da CYBER & CLOUD Expo, mas com a utilização da ferramenta CyberSecure, desenvolvido pela NECHO TECHLAW, para facilitar a simulação e a resposta aos incidentes.

Assim como no exercício anterior, os participantes foram divididos em equipas com responsabilidades específicas (CEO, TECH, Legal e Comunicação). A ferramenta CyberSecure facilitou a gestão dos *injects* e das respostas, permitindo uma monitorização em tempo real das ações tomadas pelas equipas.

Este ciberexercício foi inspirado num modelo existente, fornecido pela Cybersecurity & Infrastructure Security Agency (CISA). O documento CISA Tabletop Exercise Package (CTEP) é uma ferramenta essencial utilizada para preparar as infraestruturas de água contra ciberameaças. Este pacote de exercícios foi estruturado para avaliar a prontidão dos sistemas de tratamento de água em caso de ciberataques, com uma simulação detalhada de incidentes que podem comprometer operações críticas.

O CTEP para sistemas de água está dividido em três módulos principais:

1. Módulo de Identificação e Proteção

Neste módulo, o exercício aborda a deteção precoce de vulnerabilidades em sistemas de controlo remoto, especificamente nas infraestruturas de água. Um dos cenários simulados envolve a descoberta de falhas de segurança num software popular usado para acesso remoto. A vulnerabilidade permitia a execução de código malicioso antes da autenticação no servidor. O documento propôs uma análise detalhada de como as entidades de água gerem *patches* de segurança e controlam o acesso remoto. A simulação enfatizou a necessidade de atualizar regularmente os sistemas e reforçar as políticas de controlo de acesso, alinhadas com as recomendações da CISA.

2. Módulo de Deteção e Resposta

No segundo módulo, os cenários simulados envolvem a interrupção de operações críticas, como o controlo de válvulas e bombas de água. Um incidente particularmente desafiador foi a falha no sistema de cloração, que aumentou os níveis de cloro para níveis perigosos. A simulação avaliou a resposta das equipas de Tecnologia Operacional (TO) e TI na mitigação dos efeitos e na recuperação do controlo

dos sistemas. O documento sublinhou a importância da segmentação de redes TO e TI e da implementação de mecanismos para proteger operações sensíveis contra intrusões.

3. Módulo de Recuperação

O último módulo foca-se na recuperação de um ciberataque. Simulou-se uma situação em que vários dispositivos de controlo foram comprometidos através de *ransomware*, o que exigiu das equipas de resposta a decisão sobre o pagamento do resgate e a restauração dos dados. A análise centrou-se na capacidade das infraestruturas de água de operarem manualmente em caso de falha dos sistemas automáticos, bem como na prontidão das equipas de gestão de incidentes.

3.2.3. Exemplo de um *Inject* e respetivas respostas

Os *injects* eram algo parecido com o seguinte:

"*Inject* – Programa suspeito

Um funcionário, a trabalhar numa estação de tratamento de água, repara num programa (código) em execução numa linha de comandos de uma consola de controlo. Esta estação de trabalho é responsável pelo controlo das bombas e pela configuração do fluxo de água. A linha de comandos termina e fecha-se rapidamente. O funcionário notifica a Direção de Sistemas da Informação (DSI)."

Os jogadores tinham de responder com as seguintes opções:

CEO: 1. Avaliação de Impacto e Resposta Rápida - Decidir convocar uma reunião de emergência com o TECH para entender o impacto potencial e definir medidas de contenção. 2. Comunicação e Transparência - Determinar a comunicação proativa com os *stakeholders* internos sobre o incidente, assegurando que medidas estão sendo tomadas para mitigar riscos.

TECH: 1. Revisão de Acesso e Privilégios - Avaliar e ajustar, se necessário, as políticas de controlo de acesso para minimizar o risco de instalação de software não autorizado. 2. Isolamento e Análise Forense - Decidir imediatamente isolar o sistema ou a rede afetada e iniciar uma análise forense do software suspeito para entender as suas funcionalidades e origem.

Legal: 1. Avaliação de Impacto sobre a Proteção dos Dados (DPIA) - Avaliar o potencial impacto do software suspeito na privacidade e segurança dos dados pessoais tratados pela organização. 2. Notificação à CNPD - Preparar a notificação do incidente à CNPD, conforme necessário, especialmente se houver risco para os dados pessoais.

Comunicação: 1. Gestão da Comunicação Interna - Assegurar que a equipa esteja informada sobre o incidente, evitando rumores e garantindo uma mensagem consistente. 2. Declaração Preparatória - Preparar uma declaração pública proativa, caso o incidente se torne conhecido externamente, destacando as ações de mitigação em andamento.

Os ciberexercícios realizados durante o estágio na NECHO TECHLAW demonstraram ser extremamente benéficos, proporcionando:

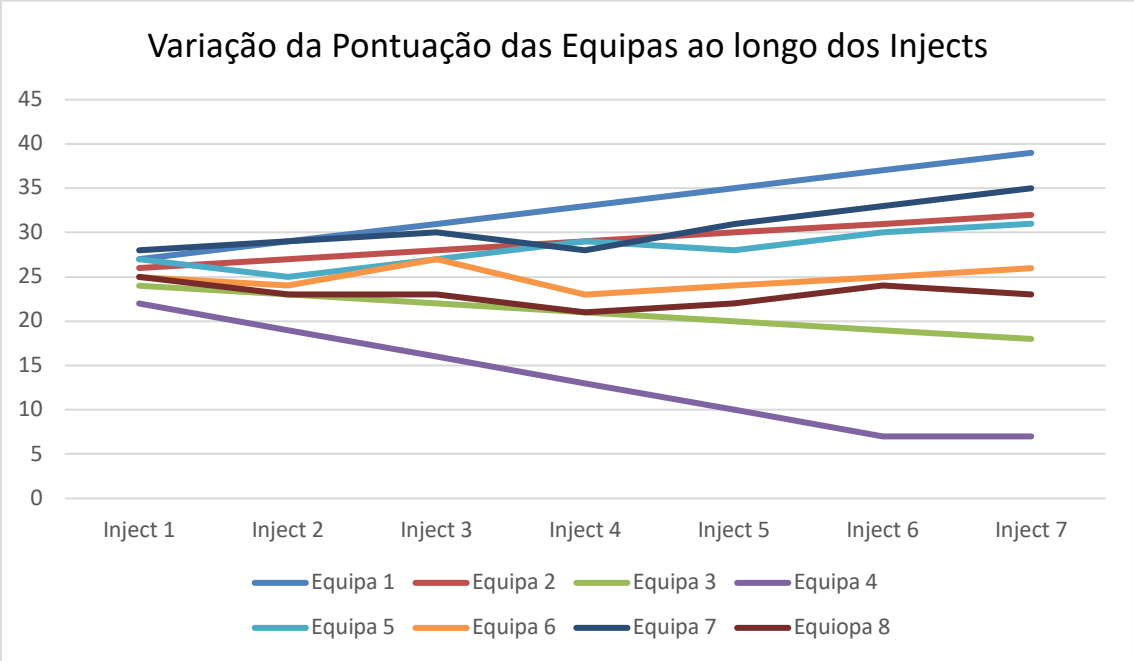
- Avaliação Realista de Capacidades: Testaram a eficácia das respostas a incidentes num ambiente simulado.
- Treino Prático: Ofereceram uma oportunidade para os participantes praticarem as suas habilidades e ganharem confiança nas suas respostas a incidentes.
- Identificação de Vulnerabilidades: Revelaram pontos fracos e áreas de melhoria nos sistemas de segurança.
- Aumento da Consciencialização: Melhoraram a compreensão dos funcionários sobre as ciberameaças e a importância das práticas de segurança.
- Melhoria Contínua: Os *feedbacks* dos exercícios foram utilizados para ajustar e aprimorar as políticas e procedimentos de segurança.
- Fortalecimento da Cooperação: Promoveram uma resposta coordenada e colaborativa entre diferentes equipas e departamentos.

3.2.4. Resultados dos Ciberexercícios

Sendo um “jogo”, as equipas iniciavam com 25 “cybercoins” e iam perdendo ou ganhando consoante acertassem ou errassem nas respostas aos injects.

Assim, no primeiro ciberexercício obtivemos a seguinte variação das pontuações:

Figura 3. *Variação das Pontuações*



Fonte: própria

3.3. Implementação do Regime Jurídico de Segurança no Ciberespaço

Entre as principais regulamentações que visam assegurar a proteção do ciberespaço em Portugal, destaca-se o Regime Jurídico da Segurança do Ciberespaço (RJSC).

O RJSC estabelece requisitos específicos para a segurança da informação, que incluem a identificação e gestão de riscos, a implementação de medidas de segurança, e a notificação de incidentes. A conformidade com o RJSC é fundamental para garantir a resiliência das operações e a proteção dos dados contra ciberameaças.

Neste contexto, a NECHO TECHLAW realizou a implementação do RJSC em duas grandes empresas de serviços essenciais, sendo uma do setor aeroportuário e outra do setor público municipal. Devido à sensibilidade das informações, os nomes das empresas não serão mencionados. Este trabalho visou assegurar que ambas as organizações estavam em conformidade com o RJSC, reforçando a sua capacidade de prevenir, detetar e responder a incidentes de cibersegurança.

A implementação do RJSC nas empresas seguiu um processo estruturado que envolveu várias etapas críticas:

1. Determinar um Ponto de Contacto Permanente e um Responsável de Segurança.

2. Inventário de Ativos.
3. Análise de Criticidade e Risco.
4. Plano de Ação.
5. Plano de Segurança.
6. Normas e Procedimentos.
7. Notificação de Incidentes.
8. Relatório Anual de Cibersegurança.

3.3.1. Determinar um Ponto de Contacto Permanente e um Responsável de Segurança

Importância do Ponto de Contacto Permanente

A designação de um ponto de contacto permanente é uma etapa essencial na implementação do Regime Jurídico da Segurança do Ciberespaço (RJSC) em qualquer organização. Este papel é vital para a comunicação eficaz entre a empresa e as autoridades reguladoras, garantindo que todas as questões de cibersegurança são tratadas de forma coordenada e oportuna. O ponto de contacto permanente serve como o elo principal entre a organização e os órgãos de fiscalização, facilitando o fluxo de informações sobre a conformidade com as regulamentações e a notificação de incidentes. O profissional é responsável por reportar incidentes de segurança, responder a solicitações de informações e manter as autoridades informadas sobre as medidas de segurança implementadas. Além disso, o ponto de contacto deve estar sempre atualizado sobre as novas regulamentações e melhores práticas em cibersegurança, garantindo que a empresa permanece em conformidade e bem preparada para responder a novas ameaças.

Tabela 4. *Informações do Ponto de Contacto Permanente*

Ponto de Contacto Permanente					
Nome da entidade	Nome do ponto ou pontos de contacto permanente	Endereço de correio eletrónico principal	Endereço de correio eletrónico alternativo	Número de telefone fixo principal	Número de telefone móvel principal

Fonte: própria

Designação do Responsável de Segurança

Paralelamente, a nomeação de um responsável de segurança é igualmente crucial. Este profissional tem a responsabilidade de liderar a estratégia de cibersegurança da organização, garantindo que todas as medidas necessárias são implementadas para proteger os ativos digitais e a informação sensível da empresa. O responsável de segurança deve possuir um profundo conhecimento técnico e uma compreensão abrangente das ciberameaças e das melhores práticas de mitigação.

O responsável de segurança é encarregue de desenvolver e implementar políticas e procedimentos de segurança, realizar análises de risco, coordenar treinos de consciencialização para colaboradores, e responder a incidentes de segurança. Este papel exige uma combinação de habilidades técnicas, capacidades de gestão e um forte entendimento das regulamentações aplicáveis, como o RJSC. A liderança eficaz do responsável de segurança é fundamental para garantir que a organização mantém uma postura de segurança proativa e resiliente.

Tabela 5. *Informações do Responsável de Segurança*

Responsável de Segurança					
Nome da entidade	Nome do Responsável de Segurança	Cargo do Responsável de Segurança	Endereço de correio eletrónico	Número de telefone fixo principal	Número de telefone móvel principal

Fonte: própria

Desafios e soluções

A designação destes papéis apresenta vários desafios, incluindo a necessidade de selecionar profissionais qualificados e a integração eficaz das suas funções nas operações diárias da empresa. É essencial que tanto o ponto de contacto permanente quanto o responsável de segurança recebam treino adequado e tenham acesso a recursos suficientes para desempenhar as suas funções de forma eficaz.

Para superar estes desafios, a organização deve investir em treino contínuo e desenvolvimento profissional para estes indivíduos. Além disso, a implementação de tecnologias de segurança avançadas e a criação de uma cultura de cibersegurança dentro da empresa são medidas essenciais para apoiar as suas atividades. A colaboração estreita entre o ponto de contacto permanente e o responsável de

segurança também é crucial para garantir que todas as iniciativas de segurança são coordenadas e alinhadas com os objetivos estratégicos da organização.

Em ambas as empresas, tanto o papel do ponto de contacto permanente como o do responsável de segurança foi atribuído à mesma pessoa, por escolha das entidades. Ambas pertencem à equipa de IT.

3.3.2. Inventário de ativos

Importância do Inventário de Ativos

Ativos são todos os sistemas de informação e comunicação, os equipamentos e os demais recursos físicos e lógicos considerados essenciais, geridos ou detidos pela entidade, que suportam, direta ou indiretamente, um ou mais serviços. Também as redes e sistemas de informação da organização que se encontram no exterior das suas instalações físicas devem ser identificados e catalogados no inventário de ativos.

A criação de um inventário de ativos é uma etapa essencial na implementação do Regime Jurídico da Segurança do Ciberespaço (RJSC). Esta é a etapa mais demorada, pois é necessário identificar todos os ativos da entidade. Em ambas as empresas foram identificados mais de 100 ativos. O processo para os identificar passou por reunir com cada departamento para saber quais os softwares e hardwares utilizados em cada local. Isto tudo foi sendo feito com o apoio do técnico de IT que foi validando as respostas.

Estrutura do Inventário de Ativos

Um inventário de ativos inclui informações detalhadas sobre todos os componentes de hardware, software, dados e redes.

Tabela 6. *Inventário de Ativos (Pt.1)*

Inventário de Ativos								
#	Nome do Ativo* (Hardware/Software)	Tipologia CNCS*	Tipo	TI/TO	Categoria	Fabricante*	Tipo de propriedade sobre o ativo*	Ativos diretamente acessíveis publicamente através da Internet*

Fonte: própria

Tabela 7. *Inventário de Ativos (Pt.2)*

Inventário de Ativos									
#	Serviço/Processo suportado pelo ativo*	Modelo/Versão*	Endereço IP*	Fully Qualified Domain Name*	Número de Inventário*	Número de Série*	Localização*	Endereço Hardware*	Tipo de contrato de suporte*

Fonte: própria

*Todos os campos identificados com um asterisco (*) são de preenchimento obrigatório, para o CNCS.

Exemplo de Ativos:

- Nome do Ativo: Microsoft Office 365
- Tipologia CNCS: Aplicações e Plataformas de Software
- Tipo: Software de Produtividade
- TI/TO: TI
- Categoria: Informação
- Fabricante: Microsoft
- Tipo de Propriedade sobre o Ativo: Ativo Gerido
- Ativos diretamente acessíveis publicamente através da Internet: Sim
- Serviço/Processo suportado pelo Ativo: Edição de documentos, planilhas, apresentações e comunicação colaborativa
- Modelo/Versão: V. 2301
- Endereço IP: N/A
- FQDN: office.com
- Número de Inventário: N/A
- Número de Série: LIC-123456
- Localização: Nuvem (Servidores Microsoft)
- Endereço Hardware: N/A
- Tipo de contrato de suporte: Contrato Enterprise com suporte 24/7

- Nome do Ativo: Desktop HP EliteDesk 800 G6
- Tipologia CNCS: Dispositivos Físicos, Redes e Sistemas de Informação

- Tipo: Computador Desktop
- TI/TO: TI
- Categoria: Tecnológicos
- Fabricante: HP
- Tipo de Propriedade sobre o Ativo: Detido
- Ativos diretamente acessíveis publicamente através da Internet: Não
- Serviço/Processo suportado pelo Ativo: Operações diárias de escritório, acesso a sistemas internos
- Modelo/Versão: EliteDesk 800 G6 (Intel Core i7-10700)
- Endereço IP: 192.168.1.50
- FQDN: N/A
- Número de Inventário: INVENT-002
- Número de Série: SN-789012
- Localização: Escritório Principal, Sala 23, Câmara Municipal
- Endereço Hardware: 00:1A:2B:3C:4D:5E
- Tipo de contrato de suporte: Garantia estendida HP até 2030

Desafios na Criação do Inventário de Ativos

A criação de um inventário de ativos pode apresentar vários desafios. Um dos principais desafios é a abrangência, pois a infraestrutura tecnológica das organizações é extensa e complexa. Outro desafio é a precisão, uma vez que erros ou omissões no inventário podem comprometer a eficácia das medidas de segurança. A infraestrutura tecnológica também está em constante evolução, com novos ativos sendo adicionados e antigos sendo desativados regularmente. Manter o inventário atualizado é um desafio contínuo. Além disso, grandes organizações podem ter milhares de ativos, o que torna a identificação e documentação um processo demorado e complexo.

Benefícios de um inventário de ativos bem elaborado

Apesar dos desafios, a criação de um inventário de ativos bem elaborado traz inúmeros benefícios para a organização. Entre os principais benefícios estão:

- Melhor Gestão de Riscos;
- Conformidade com o regulamento;
- Resposta a Incidentes;
- Planeamento de Segurança.

3.3.3. Análise de Criticidade e Risco

Importância da análise de Criticidade e Risco

A análise de criticidade e risco dos ativos é também uma etapa crucial na implementação do Regime Jurídico da Segurança do Ciberespaço (RJSC) e na gestão da cibersegurança em geral. Este processo envolve a avaliação detalhada de cada ativo identificado no inventário para determinar a sua importância para as operações da organização e os riscos associados a ele. A análise de criticidade e risco permite priorizar os esforços de segurança, focando recursos e medidas de proteção nos ativos mais críticos e vulneráveis.

Para a elaboração da análise da Criticidade, utilizou-se a matriz da ISO 27005, combinando impacto operacional, financeiro, reputacional e legal. A análise de Risco foi feita com base numa avaliação qualitativa (baixo, médio, alto) feita através de cenários e ameaças, do ENISA Threat Landscape 2023.

A principal dificuldade foi o facto de estas avaliações serem um pouco subjetivas, sendo diferentes em cada departamento. O ideal é todas seguirem os mesmos critérios e não haver subjetividade.

Processo da análise de Criticidade

A análise de criticidade envolve a avaliação da importância de cada ativo para a continuidade dos negócios da organização. Os ativos são classificados com base em critérios como impacto operacional, impacto financeiro, impacto na reputação e impacto legal ou regulatório. Este processo ajuda a identificar quais os ativos essenciais para a operação da organização e devem receber a maior atenção em termos de segurança.

Tabela 8. *Classificação da Criticidade do Ativo*

CLASSIFICAÇÃO DA CRITICIDADE DO ATIVO Importância do Ativo para a prestação dos serviços da organização				
Impactos Operacionais	Impactos Financeiros	Impacto nas pessoas (Segurança, Saúde, Satisfação)	Impacto Legal/Regulatório	Criticidade

Fonte: própria

Exemplo de análise da Criticidade:

- Nome do Ativo: Microsoft Office 365
- Impactos Operacionais: Médio
- Impactos Financeiros: Médio
- Impacto nas Pessoas: Alto
- Impacto Legal/Regulatório: Médio
- Criticidade: Médio

- Nome do Ativo: Desktop HP EliteDesk 800 G6
- Impactos Operacionais: Alto
- Impactos Financeiros: Baixo
- Impacto nas Pessoas: Médio
- Impacto Legal/Regulatório: Baixo
- Criticidade: Médio

Processo da análise de risco

A análise de risco complementa a análise de criticidade ao identificar e avaliar as ameaças e vulnerabilidades associadas a cada ativo crítico. Este processo segue uma metodologia estruturada, a ISO 27005, que fornece diretrizes para a gestão de riscos de segurança da informação. O processo segue por:

1. Identificação de Ameaças;
2. Identificação de Vulnerabilidades;
3. Avaliação de Impacto e Probabilidade;
4. Cálculo do Risco.

Tabela 9. *Análise de Risco (Pt.1)*

Análise de Risco						
	Risco		Ameaças Credíveis		Vulnerabilidades	
Ativo	Cenário	Consequências	Ameaças Comuns	Descrição	Categoria	Descrição

Fonte: própria

Tabela 10. *Análise de Risco (Pt.2)*

Análise de Risco					
Impactos Legais/Regulatórios	Perdas Operacionais ou Financeiras	Perdas de Produtividade	Perdas de Parceiros	Impacto na Reputação e Imagem	Impacto na Segurança e Saúde

Fonte: própria

Tabela 11. *Análise de Risco (Pt.3)*

Análise de Risco					
Impacto	Probabilidade	Nível do Risco	Dono do Risco	Critério de Aceitação do Risco	Opção de Tratamento do Risco

Fonte: própria

Exemplo de análise de Risco:

- Nome do Ativo: Microsoft Office 365
- Cenário do Risco: Comprometimento de credenciais via phishing, levando a acessos não autorizados a dados sensíveis.
- Consequências: Exfiltração de dados confidenciais, violação do RGPD, interrupção de serviços.
- Ameaças Comuns: Phishing, ataques de *brute force*, exploração de vulnerabilidades em APIs.
- Descrição: Credenciais de utilizadores são roubadas via e-mails de phishing, permitindo acesso a documentos confidenciais armazenados no OneDrive/SharePoint.
- Categoria das Vulnerabilidades: Software e Pessoas
- Impactos Legais/Regulatórios: Alto
- Perdas Operacionais ou Financeiras: Médio
- Perdas de Produtividade: Médio
- Perdas de Parceiros: Alto
- Impacto na Reputação e Imagem: Muito Alto
- Impacto na Segurança e Saúde: Baixo
- Impacto: Alto
- Probabilidade: Alto
- Nível do Risco: Alto

- Dono do Risco: Responsável da Segurança da Informação
- Critério de Aceitação do Risco: Não aceitável
- Opção de Tratamento do Risco: Mitigar

- Nome do Ativo: Desktop HP EliteDesk 800 G6
- Cenário do Risco: Infeção por malware via USB não autorizada, comprometendo dados locais e acesso à rede interna.
- Consequências: Perda de dados, propagação de ransomware na rede interna, interrupção de operações.
- Ameaças Comuns: Malware, roubo físico, acesso não autorizado.
- Descrição: Um funcionário conecta um USB infetado ao desktop, permitindo a instalação de ransomware que criptografa arquivos locais e se propaga pela rede.
- Categoria das Vulnerabilidades: Hardware e Pessoas
- Impactos Legais/Regulatórios: Médio
- Perdas Operacionais ou Financeiras: Médio
- Perdas de Produtividade: Alto
- Perdas de Parceiros: Médio
- Impacto na Reputação e Imagem: Alto
- Impacto na Segurança e Saúde: Baixo
- Impacto: Médio
- Probabilidade: Médio
- Nível do Risco: Médio
- Dono do Risco: Gestor de TI
- Critério de Aceitação do Risco: Não aceitável
- Opção de Tratamento do Risco: Mitigar

1.2.4. Plano de ação

Importância do Plano de ação

O Plano de Ação serve como instruções detalhadas que orientam a execução das medidas necessárias para mitigar os riscos identificados durante a análise de criticidade e risco dos ativos. Traduz as estratégias de segurança em ações práticas, com prazos definidos, responsabilidades atribuídas e recursos alocados. A criação de

um Plano de Ação bem estruturado é fundamental para garantir que as iniciativas de segurança sejam implementadas de maneira eficiente e eficaz.

Estrutura do Plano de ação

Um Plano de Ação típico deve incluir os seguintes componentes:

1. Objetivos e Metas;
2. Ações a serem executadas;
3. Responsabilidades: Designação dos responsáveis por cada ação;
4. Recursos Necessários;
5. Prazos;
6. Riscos e Contingências.

Exemplo do Plano de ação

- Objetivos e Metas: Reduzir o risco de ataques de ransomware em sistemas de bagagem em 90%; Implementar backups offline e treinar 100% da equipa operacional em resposta a incidentes.
- Ações a serem executadas: Atualizar firmware de dispositivos IoT , implementar backups diários offline em locais fisicamente seguros, realizar simulações de ransomware trimestrais.
- Responsabilidades: CISO - Coordenar atualizações e backups, Equipa de Operações - Executar simulações, Fornecedor de TI - Implementar EDR.
- Recursos Necessários: Ferramentas para varredura e backups, Equipa externa para consultoria em cibersegurança.
- Prazos: 3 meses
- Riscos e Contingências: Resistência da equipa a novos processos, Workshops de sensibilização com casos reais.

Monitorização e Revisão do Plano de Ação

Após o desenvolvimento do Plano de Ação, é crucial implementar um processo contínuo de monitorização e revisão. Este processo envolve a recolha regular de dados sobre o progresso das ações, a avaliação do desempenho em relação aos critérios de sucesso estabelecidos e a realização de ajustes conforme necessário. A monitorização

eficaz permite identificar problemas rapidamente e tomar medidas corretivas antes de afetarem significativamente a segurança da organização.

1.2.5. Plano de Segurança

Importância do Plano de Segurança

O Plano de Segurança serve como um guia abrangente que descreve as estratégias, políticas, procedimentos e medidas que a organização adotará para proteger os seus ativos críticos e mitigar os riscos de cibersegurança. A criação de um Plano de Segurança robusto é fundamental para garantir a resiliência da organização contra ciberameaças e para cumprir as exigências regulatórias.

Estrutura do Plano de Segurança

Um Plano de Segurança bem estruturado inclui os seguintes elementos:

- Definição das Políticas de Segurança;
- Implementação de Medidas de Proteção Física;
- Controlos Técnicos de Segurança;
- Gestão de Acessos;
- Plano de Resposta a Incidentes;
- Plano de Continuidade de Negócios;
- Programas de Treino e Consciencialização;
- Monitorização e Auditoria.

Benefícios do Plano de Segurança

A implementação de um Plano de Segurança bem estruturado traz vários benefícios para a organização:

- Redução de Riscos: Ajuda a identificar e mitigar riscos de cibersegurança, protegendo os ativos críticos da organização.
- Conformidade Regulamentar: Assegura que a organização está em conformidade com o RJSC e outras regulamentações relevantes.
- Resiliência Organizacional: Aumenta a capacidade da organização de resistir e se recuperar de incidentes de cibersegurança.

- Proteção de Dados Sensíveis: Protege informações sensíveis e confidenciais contra acessos não autorizados e violações de dados.
- Melhoria na Confiança dos *Stakeholders*: Reforça a confiança de clientes, parceiros e outros *stakeholders* na capacidade da organização de proteger seus dados e sistemas.

1.2.6. Notificação de Incidentes

Importância da Notificação de Incidentes

A notificação de incidentes é um componente crítico na gestão de cibersegurança e na implementação do RJSC. A capacidade de detetar, comunicar e responder rapidamente a incidentes de segurança é essencial para mitigar danos, restaurar operações normais e prevenir futuros incidentes. A notificação adequada permite que as organizações tomem ações imediatas e coordenadas, minimizando o impacto dos incidentes de cibersegurança.

Estrutura da Notificação de Incidentes

Um processo eficaz de notificação de incidentes deve incluir os seguintes elementos:

- Definição de Incidente: Clarificação do que constitui um incidente de cibersegurança dentro do contexto organizacional.
- Canal de Comunicação: Estabelecimento de canais de comunicação dedicados para notificação de incidentes.
- Critérios de Notificação: Determinação de critérios claros para quando e como os incidentes devem ser notificados.
- Procedimentos de Notificação: Procedimentos detalhados para a notificação interna e externa de incidentes.
- Equipa de Resposta a Incidentes: Designação de uma equipa responsável por gerir e responder a incidentes.
- Documentação e Relatórios: Processo de documentação detalhada de todos os incidentes e ações tomadas.
- Avaliação e Melhoria Contínua: Revisão e melhoria contínua dos processos de notificação e resposta a incidentes.

Benefícios da Notificação de Incidentes

A implementação de um processo robusto de notificação de incidentes traz vários benefícios, incluindo:

- Resposta Rápida e Coordenada: Facilita uma resposta rápida e coordenada a incidentes de segurança, minimizando o impacto nas operações e na reputação da organização.
- Conformidade Regulamentar: Assegura a conformidade com requisitos legais e regulamentares, evitando penalidades e sanções.
- Transparência e Confiança: Melhora a transparência e a confiança com clientes, parceiros e outras partes interessadas, demonstrando um compromisso com a segurança.
- Mitigação de Riscos: Ajuda a identificar e mitigar riscos de cibersegurança, fortalecendo a postura de segurança da organização.
- Aprendizagem e Melhoria: Proporciona oportunidades para aprendizagem e melhoria contínua dos processos de segurança.

1.2.7. Relatório Anual de Cibersegurança

Importância do Relatório Anual de Cibersegurança

O Relatório Anual de Cibersegurança serve para documentar e analisar todas as atividades de cibersegurança realizadas durante o ano, avaliando a eficácia das políticas implementadas, os incidentes de segurança ocorridos, e as melhorias feitas no sistema de segurança da informação. Além disso, o relatório anual ajuda a garantir a conformidade com os regulamentos de cibersegurança.

Estrutura do Relatório Anual de Cibersegurança

Um Relatório Anual de Cibersegurança bem estruturado deve incluir as seguintes seções:

1. Resumo Executivo
2. Descrição das Atividades de Cibersegurança
3. Análise de Incidentes de Segurança
4. Avaliação de Riscos e Vulnerabilidades
5. Revisão de Políticas e Procedimentos de Segurança
6. Planos de Continuidade de Negócios e Recuperação de Desastres

7. Formação e Sensibilização de *Stakeholders*
8. Investimentos e Recursos de Segurança
9. Planos para o Próximo Ano

Resumo Executivo

O resumo executivo deve conter uma visão geral das atividades de cibersegurança realizadas durante o ano. Deve destacar os principais sucessos, desafios e áreas de melhoria. Este resumo é destinado à alta administração e outras partes interessadas que precisam de uma compreensão rápida e clara do estado da cibersegurança da organização.

Descrição das Atividades de Cibersegurança

Nesta secção, é importante detalhar todas as atividades de cibersegurança realizadas ao longo do ano. Isto pode incluir:

- Implementação de novas tecnologias de segurança
- Atualizações de sistemas e redes
- Desenvolvimento de novas políticas e procedimentos de segurança
- Realização de auditorias internas e externas
- Monitorização contínua de ameaças e vulnerabilidades

Análise de Incidentes de Segurança

A análise de incidentes de segurança deve incluir uma descrição detalhada de todos os incidentes ocorridos, as medidas de resposta adotadas e as lições aprendidas. Para cada incidente, é importante documentar:

- Data e hora do incidente
- Tipo de incidente
- Impacto nos negócios
- Ações de contenção e recuperação
- Recomendações para prevenir futuros incidentes

Avaliação de Riscos e Vulnerabilidades

Nesta secção, a organização deve apresentar uma avaliação abrangente dos riscos e vulnerabilidades identificados durante o ano. Está incluída uma análise das áreas mais críticas e as medidas tomadas para mitigar esses riscos. A avaliação de risco pode seguir normas reconhecidas, como a ISO 27005.

Revisão de Políticas e Procedimentos de Segurança

A revisão de políticas e procedimentos de segurança é fundamental para garantir que a organização esteja sempre em conformidade com as melhores práticas e regulamentos. Esta secção deve detalhar qualquer revisão ou atualização de políticas de segurança, bem como a criação de novos procedimentos.

Planos de Continuidade de Negócios e Recuperação de Desastres

Os planos de continuidade de negócios e recuperação de desastres são essenciais para garantir que a organização possa continuar a operar durante e após um incidente de segurança. O relatório anual deve incluir uma revisão desses planos, destacando quaisquer testes realizados e melhorias implementadas.

Formação e Sensibilização de *Stakeholders*

A formação contínua e a sensibilização dos funcionários e outras partes interessadas são cruciais para a cibersegurança. Esta secção deve detalhar os programas de formação realizados durante o ano, os tópicos abordados e a eficácia desses programas na melhoria da postura de segurança da organização.

Investimentos e Recursos de Segurança

Os investimentos e recursos alocados para a cibersegurança refletem o compromisso da organização com a proteção dos seus ativos digitais. Esta secção deve apresentar um resumo dos investimentos feitos em tecnologias de segurança, contratação de pessoal especializado, e outras iniciativas de segurança.

Planos para o Próximo Ano

Finalmente, o relatório deve incluir planos detalhados para o próximo ano. Isso inclui:

- Objetivos de cibersegurança
- Projetos de melhoria contínua
- Iniciativas de formação e sensibilização
- Planeamento do orçamento e recursos

1.3. Formação “Responsável de Cibersegurança”

A empresa NECHO TECHLAW deu-me a oportunidade de realizar um curso, lecionado pelos mesmos. Este curso é projetado para fornecer conhecimentos aprofundados sobre os princípios, práticas e regulamentos de cibersegurança, preparando os participantes para enfrentar os desafios de um ambiente digital em constante evolução.

O curso de "Responsável de Cibersegurança" teve como principais objetivos:

1. Interpretar os conceitos e requisitos do RJSC e legislação complementar.
2. Auditar e avaliar a maturidade da organização em cibersegurança.
3. Inventariar e categorizar os ativos críticos.
4. Realizar análise de riscos nos ativos de informação.
5. Identificar e aplicar medidas técnicas e organizativas para gerir os riscos, usando a metodologia do QNRSC.
6. Elaborar uma Política de Segurança da Informação.
7. Criar o Plano de Cibersegurança da organização, alinhado com o RJSC.
8. Estabelecer uma Política e Procedimentos de Gestão de Incidentes.
9. Preparar o Relatório Anual de Cibersegurança, em conformidade com o RJSC.
10. Desenvolver um Plano de Ação para a conformidade regulatória da organização.
11. Produzir documentos e relatórios exigidos pelas Instruções Técnicas do CNCS.
12. Cumprir os requisitos do RJSC.
13. Implementar boas práticas de gestão de cibersegurança.

A formação foi dividida em vários módulos, cobrindo uma ampla gama de tópicos relevantes:

- Módulo 01: Enquadramento Normativo do RJSC

- Módulo 02: O “Responsável de Segurança” e “Ponto de Contato Permanente”
- Módulo 03: Política de Segurança da Informação (PSI)
- Módulo 04: Inventariação de ativos
- Módulo 05: Análise de Risco
- Módulo 06: Medidas técnicas e organizativas
- Módulo 07: Plano de (Ciber)Segurança
- Módulo 08: Gestão de Incidentes de Cibersegurança
- Módulo 09: Auditoria e Monitorização da Cibersegurança
- Módulo 10: Relatório Anual de Cibersegurança
- Módulo 11: Plano de Ação para a conformidade com o RJSC
- Módulo 12: A nova Diretiva NIS 2

Os benefícios de participar na formação de "Responsável de Cibersegurança" foram numerosos:

- Habilitação Profissional: Os participantes receberam certificações reconhecidas que comprovam a sua competência em cibersegurança.
- Capacidade de Liderança: Os formandos estão capacitados para liderar iniciativas de cibersegurança dentro das suas organizações.
- Redução de Riscos: As organizações beneficiam-se de uma redução significativa nos riscos de cibersegurança graças à implementação de práticas eficazes.
- Conformidade Legal: As empresas garantem conformidade com as normas e regulamentos de cibersegurança, evitando penalidades e melhorando a reputação.

4. Análise Crítica: Reflexão sobre o estágio

O estágio na NECHO TECHLAW proporcionou-me uma oportunidade única para aplicar os conhecimentos adquiridos ao longo do curso de Mestrado em Cibersegurança e Auditoria de Sistemas Informáticos num ambiente corporativo real. Esta experiência prática foi fundamental para consolidar a aprendizagem teórica e desenvolver competências práticas essenciais na área da cibersegurança. Nesta análise crítica, refletirei sobre os aspetos mais significativos do estágio, destacando as aprendizagens, os desafios enfrentados e as competências desenvolvidas.

4.1. Sumário dos Pontos Principais

O estágio realizado na NECHO TECHLAW foi uma experiência integral e enriquecedora que permitiu a aplicação prática dos conhecimentos adquiridos durante o curso de Mestrado em Cibersegurança e Auditoria de Sistemas Informáticos. Ao longo do estágio, foram abordados vários pontos cruciais que contribuíram para o desenvolvimento profissional e pessoal, destacando-se os seguintes:

1. Implementação do RJSC: A participação ativa na implementação do Regime Jurídico de Segurança do Ciberespaço em duas grandes entidades de serviços essenciais foi uma das atividades mais importantes. Este processo incluiu a determinação de pontos de contacto permanentes e responsáveis de segurança, a realização de inventários de ativos, análises de criticidade e risco, desenvolvimento de planos de ação e segurança, bem como a criação de normas e procedimentos.
2. Realização de Ciberexercícios: A organização e execução de ciberexercícios foram fundamentais para testar e validar a eficácia das políticas de cibersegurança. Estes exercícios, realizados tanto na CYBER & CLOUD EXPO quanto no SIMAS em Oeiras, proporcionaram um ambiente prático para a simulação de cenários de ataque e a avaliação das respostas em tempo real.
3. Formação em Cibersegurança: A participação e suporte na formação "Responsável de Cibersegurança" ajudaram a consolidar conhecimentos teóricos e práticos, promovendo uma cultura de cibersegurança dentro da organização.
4. Metodologias e Ferramentas Utilizadas: O uso de metodologias como a análise de processos e conformidade com a norma ISO 27005, juntamente com a utilização de ferramentas, foram essenciais para a análise de vulnerabilidades e implementação de medidas de mitigação.

4.2. Contribuições do Estágio e Competências desenvolvidas

O estágio na NECHO TECHLAW trouxe diversas contribuições significativas tanto para a organização quanto para mim:

- Fortalecimento da Postura de Segurança: As atividades desenvolvidas durante o estágio contribuíram para o fortalecimento da postura de cibersegurança das entidades envolvidas. A implementação do RJSC e a realização de ciberexercícios aumentaram a resiliência das infraestruturas tecnológicas e a consciência dos *stakeholders* em relação à importância da cibersegurança.
- Desenvolvimento de Competências Técnicas e Interpessoais: O estágio proporcionou o desenvolvimento de competências técnicas avançadas, como a análise de risco e a implementação de políticas de segurança, além de habilidades interpessoais essenciais, como a comunicação eficaz e a gestão de projetos.
- Conformidade Regulatória: A conformidade com o RJSC e outras legislações aplicáveis foi um dos principais resultados do estágio, garantindo que as entidades envolvidas estivessem alinhadas com as exigências legais e regulamentares, minimizando riscos de penalidades e melhorando a reputação organizacional.
- Melhoria da Cultura de Segurança: A formação e sensibilização contínuas, aliadas às atividades práticas realizadas, promoveram uma cultura organizacional de cibersegurança, essencial para a proteção dos ativos digitais e a continuidade dos negócios.

O estágio contribuiu significativamente para o desenvolvimento de diversas competências essenciais para a carreira em cibersegurança. A capacidade de realizar uma análise de criticidade e risco dos ativos foi aprimorada, permitindo identificar e mitigar vulnerabilidades de forma eficaz. A elaboração de inventários de ativos e a análise detalhada das infraestruturas tecnológicas foram competências técnicas importantes que foram desenvolvidas durante o estágio.

Além das competências técnicas, o estágio também proporcionou o desenvolvimento de competências interpessoais e de comunicação. A colaboração com pessoas de diferentes áreas e a necessidade de comunicar de forma clara e eficaz foram experiências valiosas.

5. Conclusão

Uma das aprendizagens mais significativas durante o estágio foi a compreensão profunda da implementação do Regime Jurídico da Segurança do Ciberespaço (RJSC), destacando a complexidade de alinhar exigências legais a ações operacionais. Em duas grandes organizações, a tradução de requisitos abstratos em políticas concretas exigiu não apenas conhecimento técnico, mas também habilidades de mediação entre equipas. A criação de documentos como planos de resposta a incidentes e a adoção de práticas como autenticação multifator e segmentação de redes reforçaram a postura proativa das empresas perante ciberameaças, consolidando uma cultura de segurança mais robusta.

A participação em ciberexercícios revelou-se igualmente transformadora, evidenciando a importância da colaboração multidisciplinar. As simulações de cenários como ransomware e phishing não testaram apenas a eficácia das políticas existentes, mas também fortaleceram a comunicação entre departamentos, criando um ecossistema mais coeso para resposta a crises. A experiência prática mostrou como a preparação contínua, aliada a treinos de consciencialização, pode reduzir vulnerabilidades humanas e técnicas, mitigando riscos antes que se tornem incidentes críticos.

Para as empresas, representou um passo significativo na modernização da sua postura de segurança. A conformidade com o RJSC evita não só riscos legais como também eleva a sua credibilidade no mercado. Em suma, o estágio reforçou que a cibersegurança é um processo dinâmico, onde a integração entre normas, tecnologia e pessoas é essencial para transformar obrigações legais em vantagens estratégicas.

Durante o estágio, um dos principais desafios enfrentados foi a necessidade de adaptar rapidamente a teoria à prática. Embora os conhecimentos teóricos sobre cibersegurança fossem sólidos, a aplicação desses conhecimentos num ambiente corporativo real exigiu um nível elevado de adaptabilidade e pensamento crítico. Cada organização possui as suas próprias particularidades e desafios específicos, o que tornou necessário ajustar as abordagens de cibersegurança para atender às necessidades individuais.

Outro desafio significativo foi a gestão de tempo e prioridades. O estágio envolveu múltiplas tarefas e projetos simultâneos, como a implementação do RJSC, a realização de ciberexercícios e o curso de Responsável de Cibersegurança. A capacidade de gerir eficazmente o tempo e priorizar tarefas foi crucial para garantir a conclusão bem-sucedida de todas as atividades.

O estágio na NECHO TECHLAW foi uma experiência extremamente valiosa e enriquecedora. Permitiu aplicar a teoria na prática, desenvolver novas competências e enfrentar desafios reais do campo da cibersegurança e do trabalho. A oportunidade de trabalhar em projetos críticos, como a implementação do RJSC e a realização de ciberexercícios, proporcionou uma compreensão profunda da importância da cibersegurança na proteção dos ativos digitais das organizações. O estágio não apenas consolidou o conhecimento adquirido durante o curso de mestrado, mas também me preparou para enfrentar os desafios futuros na carreira de cibersegurança com confiança e competência.

5. Referências Bibliográficas

Abdullayev, V., & Chauhan, D. A. S. (2023). SQL Injection Attack: Quick View. *Mesopotamian Journal of CyberSecurity*, *2023*, 30–34. https://doi.org/10.58496/MJCS/2023/006

Adu, J. P., Cúg, J., Amoah, J., Afful, C. R., & Jibril, A. B. (2024). Enhancing supply chain resilience: The role of security practices and performance in mitigating disruptions in ghana's manufacturing sector. *Journal of Infrastructure Policy and Development*, *8*(14), 7736. https://doi.org/10.24294/jipd7736

Alevizos, L., Ta, V., & Eiza, M. (2021). Augmenting zero trust architecture to endpoints using blockchain: a state-of-the-art review. *Security and Privacy*, 5(1). https://doi.org/10.1002/spy2.191

Al-Khafaji, B. and Rahma, A. (2022). Proposed new modification of aes algorithm for data security. *Global Journal of Engineering and Technology Advances*, 12(3), 117-122. https://doi.org/10.30574/gjeta.2022.12.3.0165

Almars, A. M. (2021). Deepfakes detection techniques using deep learning: A survey. *Journal of computer and communications*, *09*(05), 20–35. https://doi.org/10.4236/jcc.2021.95003

Al-Mohannadi, H., Mirza, Q., Namanya, A., Awan, I., Cullen, A., & Disso, J. (2016). Cyber-attack modeling analysis techniques: An overview. *2016 IEEE 4th International Conference on Future Internet of Things and Cloud Workshops (FiCloudW)*.

Antunes, M., Maximiano, M., Gomes, R., & Pinto, D. (2021). Information security and cybersecurity management: A case study with SMEs in Portugal. *Journal of Cybersecurity and Privacy*, *1*(2), 219–238. https://doi.org/10.3390/jcp1020012

Apcer. (2024). *Cibersegurança: Aumentar a confiança digital das empresas portuguesas*. https://apcergroup.com/pt/noticias-e-destaques/4354/ciberseguranca-aumentar-a-confianca-digital-das-empresas-portuguesas

Assembleia da República. (2018). "Lei n.º 46/2018". *Diário da República*, 1.ª série, 157 (agosto). https://data.dre.pt/eli/lei/46/2018/08/13/p/dre/pt/html

Avdeev, V. A., Avdeeva, O. A., Shagieva, R. V., Smirnova, V. V., Mashkin, N. A., & Taradonov, S. V. (2020). The mechanism of legal regulation in the conditions of globalization and formation of information environment. Regional aspect. *Journal of Environmental Management and Tourism*, *10*(7), 1517. https://doi.org/10.14505//jemt.v10.7(39).09

Bagnato, D. (2020). The network information systems directive (EU) 2016/1148: internet service providers and registraties. *Central and Eastern European eDem and eGov Days*, *338*, 111–122. https://doi.org/10.24989/ocg.v.338.9

Ban, T., Takahashi, T., Ndichu, S., & Inoue, D. (2023). Breaking alert fatigue: AI-assisted SIEM framework for effective incident response. *Applied Sciences (Basel, Switzerland)*, *13*(11), 6610. https://doi.org/10.3390/app13116610

BBC. (2023). *ChatGPT banned in Italy over privacy concerns.* https://www.bbc.com/news/technology-65139406

Bhatt, S., Manadhata, P. K., & Zomlot, L. (2014). The operational role of security information and event management systems. *IEEE security & privacy*, *12*(5), 35–41. https://doi.org/10.1109/msp.2014.103

Biasin, E., & Kamenjašević, E. (2022). Cybersecurity of medical devices: new challenges arising from the AI Act and NIS 2 Directive proposals. *International Cybersecurity Law Review*, *3*(1), 163–180. https://doi.org/10.1365/s43439-022-00054-x

Bleeping Computer. (2024). *Hacker hijacks Orange Spain RIPE account to cause BGP havoc.* https://www.bleepingcomputer.com/news/security/hacker-hijacks-orange-spain-ripe-account-to-cause-bgp-havoc/

Buttigieg, C. P., & Zimmermann, B. B. (2024). The digital operational resilience act: challenges and some reflections on the adequacy of Europe's architecture for financial supervision. *ERA Forum*, *25*(1), 11–28. https://doi.org/10.1007/s12027-024-00793-w

Butun, I., Osterberg, P., & Song, H. (2020). Security of the internet of things: Vulnerabilities, attacks, and countermeasures. *IEEE Communications Surveys & Tutorials*, *22*(1), 616–644. https://doi.org/10.1109/comst.2019.2953364

Carrapico, H., & Farrand, B. (2017). 'Dialogue, partnership and empowerment for network and information security': the changing role of the private sector from objects of regulation to regulation shapers. *Crime, Law, and Social Change*, *67*(3), 245–263. https://doi.org/10.1007/s10611-016-9652-4

Centro Nacional de Cibersegurança (CNCS). (n.d.). *Centro Nacional de Cibersegurança*. https://www.cncs.gov.pt

Chiara, P. G. (2022). The Cyber Resilience Act: the EU Commission's proposal for a horizontal regulation on cybersecurity for products with digital elements: An introduction. *International Cybersecurity Law Review*, *3*(2), 255–272. https://doi.org/10.1365/s43439-022-00067-6

Clausmeier, D. (2023). Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA). *International Cybersecurity Law Review*, *4*(1), 79–90. https://doi.org/10.1365/s43439-022-00076-5

CNN Portugal. (2022). *Já houve oito grandes ataques informáticos este ano em Portugal. Em dois, foi tudo destruído.* https://cnnportugal.iol.pt/ataques-informaticos/hackers/ja-houve-oito-grandes-ataques-informaticos-este-ano-em-portugal-em-dois-foi-tudo-destruido/20220607/629eb8690cf2ea4f0a4e9f90

CyberPeace. (2024). *Así fue el hackeo que sufrió Coppel y que afectó 1800 tiendas*. https://www.cyberpeace.tech/post/as%C3%AD-fue-el-hackeo-que-sufrio-coppel-y-que-afecto-1800-tiendas

da Costa Cabral, M. (2024). *Cibersegurança e Quadro Normativo Internacional - Da Fragilidade da Soft-Law à Necessária e Problemática Adoção de um Instrumento Convencional Vinculativo à Escala Global*. Leya.

Department of Homeland Security (DHS). (n.d.). *Increasing threats of deepfake identities*. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf

Diário de Notícias. (2024). *Novo quadro jurídico renova relevância da cibersegurança na gestão.* https://www.dn.pt/patrocinado-conferencia-novo-regime-juridico-da-

ciberseguranca-em-portugal/novo-quadro-juridico-renova-relevancia-da-ciberseguranca-na-gestao

Ducuing, C. (2021). Understanding the rule of prevalence in the NIS directive: C-ITS as a case study. *Computer Law and Security Report*, *40*(105514), 105514. https://doi.org/10.1016/j.clsr.2020.105514

European Commission. (2024). *European Digital Media Observatory (EDMO).* https://digital-strategy.ec.europa.eu/en/policies/european-digital-media-observatory

Familoni, B. T. (2024). Cybersecurity challenges in the age of Ai: Theoretical approaches and practical solutions. *Computer Science & IT Research Journal*, *5*(3), 703–724. https://doi.org/10.51594/csitrj.v5i3.930

Fuster, G. G., & Jasmontaite, L. (2020). Cybersecurity regulation in the European Union: The digital, the critical and fundamental rights. *The International Library of Ethics, Law and Technology* (pp. 97–115). Springer International Publishing.

Garg, T., Kagalwalla, N., Puthran, S., Churi, P., & Pawar, A. (2021). A novel approach of privacy-preserving data sharing system through data-tagging with role-based access control. *World Journal of Engineering*, 20(1), 12-28. https://doi.org/10.1108/wje-04-2021-0218

Gartner. (2024). *Leverage Cybersecurity Frameworks for Building and Optimizing Programs*.https://www.gartner.com/en/articles/cybersecurity-framework

González-Granadillo, G., González-Zarzosa, S., & Diaz, R. (2021). Security Information and Event Management (SIEM): Analysis, trends, and usage in critical infrastructures. *Sensors (Basel, Switzerland)*, *21*(14), 4759. https://doi.org/10.3390/s21144759

Gupta, S., Singhal, A., & Kapoor, A. (2016c). A literature survey on social engineering attacks: Phishing attack. *2016 International Conference on Computing, Communication and Automation (ICCCA)*. https://doi.org/10.1109/CCAA.2016.7813778

Hamidu, Z., Boachie-Mensah, F. O., & Issau, K. (2023). Supply chain resilience and performance of manufacturing firms: role of supply chain disruption. *Journal of*

Manufacturing Technology Management, *34*(3), 361–382. https://doi.org/10.1108/jmtm-08-2022-0307

Harris, M. A., & Martin, R. (2019). Promoting Cybersecurity Compliance. *Advances in Information Security, Privacy, and Ethics* (pp. 54–71). IGI Global.

IBM. (n.d.). *Homomorphic encryption*. https://www.ibm.com/think/topics/homomorphic-encryption?mhsrc=ibmsearch_a&mhq=homomorphic-encryption

Institute for Defense Analyses. (2011). *Cyberspace: The Fifth Operational Domain.* https://www.ida.org/-/media/feature/publications/2/20/2011-cyberspace---the-fifth-operational-domain/2011-cyberspace---the-fifth-operational-domain.ashx

Instituto da Defesa Nacional. (2017). *Contributos para uma Estratégia Nacional de Ciberdefesa*. https://www.defesa.gov.pt/pt/comunicacao/documentos/Lists/PDEFINTER_DocumentoLookupList/2017_IDN_Contributos-para-uma-estrategia-nacional-de-ciberdefesa.pdf

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). *Information security, cybersecurity and privacy protection* (ISO/IEC 27005:2022). *Guidance on managing information security risks*. https://www.iso.org/standard/80585.html

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). *Information security, cybersecurity and privacy protection* (ISO/IEC 27002:2022). *Information security controls*. https://www.iso.org/standard/75652.html

International Organization for Standardization (ISO) & International Electrotechnical Commission (IEC). (2022). *Information security, cybersecurity and privacy protection* (ISO/IEC 27001:2022). *Information security management systems - Requirements.* https://www.iso.org/standard/27001

Jaafar, G. A., Abdullah, S. M., & Ismail, S. (2019). Review of recent detection methods for HTTP DDoS attack. *Journal of Computer Networks and Communications*, *2019*, 1–10. https://doi.org/10.1155/2019/1283472

Jornal de Negócios. (2024). *Santander alvo de um ataque informático. Portugal não foi afetado*. https://www.jornaldenegocios.pt/empresas/banca---financas/detalhe/santander-alvo-de-um-ataque-informatico-portugal-nao-foi-afetado

Khalid, A., Zainal, A., Maarof, M. A., & Ghaleb, F. A. (2021). Advanced persistent threat detection: A survey. *2021 3rd International Cyber Resilience Conference (CRC)*. https://doi.org/10.1109/CRC50527.2021.9392626

Klenka, M. (2021). Aviation cyber security: legal aspects of cyber threats. *Journal of Transportation Security*, *14*(3–4), 177–195. https://doi.org/10.1007/s12198-021-00232-8

Ma, D., Li, R., Liu, Z., Guo, M., & Jin, X. (2024). Application of anti-mapping security access technology in network security protection. *Applied Mathematics and Nonlinear Sciences*, *9*(1). https://doi.org/10.2478/amns-2024-1547

Mallik, A., Ahsan, A., Shahadat, M. M. Z., & Tsou, J.-C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International journal of data and network science*, 77–92. https://doi.org/10.5267/j.ijdns.2019.1.001

Markopoulou, D., Papakonstantinou, V., & de Hert, P. (2019). The new EU cybersecurity framework: The NIS Directive, ENISA's role and the General Data Protection Regulation. *Computer Law and Security Report*, *35*(6), 105336. https://doi.org/10.1016/j.clsr.2019.06.007

Marotta, A., & Madnick, S. (2021). *Convergence and divergence of regulatory compliance and cybersecurity*. Issues in Information Systems, 22(1).

NATO. (2016). *NATO recognises cyberspace as a domain of operations at Warsaw Summit.* https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/

NewsRoom (2024). *Guardians of the Grid - Protecting Europe's Electricity Supply from Cyber Attacks.* https://moderndiplomacy.eu/2024/10/05/guardians-of-the-grid-protecting-europes-electricity-supply-from-cyber-attacks/

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (2017). *An introduction to information security*. National Institute of Standards and Technology.

Nifakos, S., Chandramouli, K., Nikolaou, C. K., Papachristou, P., Koch, S., Panaousis, E., & Bonacina, S. (2021). Influence of human factors on cyber security within healthcare organisations: A systematic review. *Sensors (Basel, Switzerland)*, *21*(15), 5119. https://doi.org/10.3390/s21155119

Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A. C., Onwusinkwue, S., & Ahmad, I. A. I. (2024). Comprehensive review on cybersecurity: Modern threats and advanced defense strategies. *Computer Science & IT Research Journal*, *5*(2), 293–310. https://doi.org/10.51594/csitrj.v5i2.758

O'Kane, P., Sezer, S., & Carlin, D. (2018). Evolution of ransomware. *IET Networks*, *7*(5), 321–327. https://doi.org/10.1049/iet-net.2017.0207

Oriola, O., Adeyemo, A. B., Papadaki, M., & Kotzé, E. (2021). A collaborative approach for national cybersecurity incident management. *Information and Computer Security*, *29*(3), 457–484. https://doi.org/10.1108/ics-02-2020-0027

Prasanna, S. R., & Premananda, B. S. (2021). Performance analysis of MD5 and SHA-256 algorithms to maintain data integrity. *2021 International Conference on Recent Trends on Electronics, Information, Communication & Technology (RTEICT)*.

Roopesh, M. (2024). Cybersecurity solutions and practices: firewalls, intrusion detection/prevention, encryption, multi-factor authentication. *AJBAIS*, 4(3), 37-52. https://doi.org/10.69593/ajbais.v4i3.90

Saeed, S., Altamimi, S. A., Alkayyal, N. A., Alshehri, E., & Alabbad, D. A. (2023). Digital transformation and cybersecurity challenges for businesses resilience: Issues and recommendations. *Sensors (Basel, Switzerland)*, *23*(15), 6666. https://doi.org/10.3390/s23156666

SANS. (2024). *Leadind Integrated Generative Artificial Intelligence (GenAI) and Machine Learning (ML) Cybersecurity*. https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt240333e5c2f73911/669aa9a235a68e6f196c1b57/Brochure_AI_ML-Courses_FINAL_7_24.pdf

Sendjaja, T., Irwandi, Prastiawan, E., Suryani, Y., & Fatmawati, E. (2024). Cybersecurity in the digital age: Developing robust strategies to protect against evolving global

digital threats and cyber attacks. *International Journal of Science and Society*, *6*(1), 1008–1019. https://doi.org/10.54783/ijsoc.v6i1.1098

Sophos. (2024). *The state of ransomware*. https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

SOS Intelligence. (2024). *Case Study: Maersk's Response to NotPetya - How Cybersecurity Best Practices Mitigated a Major Cyberattack*. https://sosintel.co.uk/case-study-maersks-response-to-notpetya-how-cybersecurity-best-practices-mitigated-a-major-cyberattack/

Stafford, T., Deitz, G., & Li, Y. (2018). The role of internal audit and user training in information security policy compliance. *Managerial Auditing Journal*, *33*(4), 410–424. https://doi.org/10.1108/maj-07-2017-1596

Sumy State University, Sumy, Ukraine, Krykliy, O., Pavlenko, L., & Sumy State University, Sumy, Ukraine. (2019). Internal audit as a preventive component in the bank's cybersecurity system. *Accounting and Finance*, *2(84)*, 124–133. https://doi.org/10.33146/2307-9878-2019-2(84)-124-133

Taddeo, M. (2018). Deterrence and norms to foster stability in cyberspace. *Philosophy & Technology*, *31*(3), 323–329. https://doi.org/10.1007/s13347-018-0328-0

Taherdoost, H. (2022). Understanding cybersecurity frameworks and information security standards—A review and comprehensive overview. *Electronics*, *11*(14), 2181. https://doi.org/10.3390/electronics11142181

Tekiner, E., Acar, A., Uluagac, A. S., Kirda, E., & Selcuk, A. A. (2021). SoK: Cryptojacking Malware. *2021 IEEE European Symposium on Security and Privacy (EuroS&P)*. https://doi.org/10.1109/EuroSP51992.2021.00019

Transport for London. (2024). *Cyber security incident in September 2024*. https://tfl.gov.uk/campaign/cyber-security-incident

Tuyishime, E., Balan, T. C., Cotfas, P. A., Cotfas, D. T., & Rekeraho, A. (2023). Enhancing cloud security—proactive threat monitoring and detection using a SIEM-based approach. *Applied Sciences (Basel, Switzerland)*, *13*(22), 12359. https://doi.org/10.3390/app132212359

UC Santa Cruz. (2024). *Ukraine blackouts caused by malware attacks warn against evolving cybersecurity threats to the physical world.* https://news.ucsc.edu/2024/05/ukraine-cybersecurity.html

Ukwandu, E., Farah, M. A. B., Hindy, H., Brosset, D., Kavallieros, D., Atkinson, R., Tachtatzis, C., Bures, M., Andonovic, I., & Bellekens, X. (2020). A review of cyber-Ranges and Test-Beds: Current and future trends. *Sensors (Basel, Switzerland)*, *20*(24), 7148. https://doi.org/10.3390/s20247148

Umam, C., Handoko, L. B., & Rizqi, G. M. (2018). Implementation and analysis high availability network file system based server cluster. *Jurnal Transformatika*, *16*(1), 31. https://doi.org/10.26623/transformatika.v16i1.841

Ur, M., Shaikh, R., Ullah, R., Akbar, R., Savita, K. S., & Mandala, S. (2024). Fortifying against ransomware: Navigating cybersecurity risk management with a focus on ransomware insurance strategies. *International Journal of Academic Research in Business and Social Sciences*, *14*(1), 1415–1430. https://doi.org/10.6007/ijarbss/v14-i1/20566

Uzougbo, N. S., Ikegwu, C. G., & Adewusi, A. O. (2024). Cybersecurity compliance in financial institutions: A comparative analysis of global standards and regulations. *International Journal of Science and Research Archive*, *12*(1), 533–548. https://doi.org/10.30574/ijsra.2024.12.1.0802

Visão. (2024). *Há mais uma vaga de sms falsas a correr, em nome da EDP, para tentar extorquir clientes.* https://visao.pt/atualidade/sociedade/2024-10-31-faturas-de-servicos-atencao-as-fraudes/

Wallis, T., & Johnson, C. (2020). Implementing the NIS Directive, driving cybersecurity improvements for Essential Services. *2020 International Conference on Cyber Situational Awareness, Data Analytics and Assessment (CyberSA)*.

Yu, J., Jiang, J., & Ye, W. (2024). Design and implementation of adaptive dynamic load balancing strategy based on server cluster. Em J. Zhang & N. Sun (Eds.), *Third International Conference on Electronic Information Engineering, Big Data, and Computer Technology (EIBDCT 2024)* (Vol. 40, p. 90). SPIE. http://dx.doi.org/10.1117/12.3031078

Yu, K., Taib, R., Butavicius, M. A., Parsons, K., & Chen, F. (2019). Mouse behavior as an index of phishing awareness. *Human-Computer Interaction – INTERACT 2019* (pp. 539–548). Springer International Publishing.

Zhang, H., Han, W., Lai, X., Lin, D., Ma, J., & Li, J. (2015). Survey on cyberspace security. *Science China Information Sciences*, *58*(11), 1–43. https://doi.org/10.1007/s11432-015-5433-4

Zscaler. (n.d.). *What is the SolarWinds Cyberattack?.* https://www.zscaler.com/br/resources/security-terms-glossary/what-is-the-solarwinds-cyberattack