Mestrado em Gestão de Sistemas e Tecnologias de Informação

Metodologia para Implementação da Diretiva NIS2

Dissertação para obtenção do Grau de Mestre

Elaborado por Pedro Miguel Pereira Esteves

Aluno nº 2023064

Orientador: Professor Doutor Fernando Eugénio Acabado Romana

Barcarena

Novembro de 2025

Atlântica, Instituto Universitário

Mestrado em Gestão de Sistemas e Tecnologias de Informação

Metodologia para Implementação da Diretiva NIS2

Dissertação para obtenção do Grau de Mestre

Elaborado por Pedro Miguel Pereira Esteves

Aluno nº 2023064

Orientador: Professor Doutor Fernando Eugénio Acabado Romana

Barcarena

Novembro de 2025

DECLARAÇÃO

Nome: Pedro Miguel Pereira Esteves

Endereço eletrónico: geoesteves@sapo.pt

Telefone: 936061133

Número do Bilhete de Identidade: 12121419

Título do Trabalho: Metodologia para Implementação da Diretiva NIS2

Orientador: Professor Doutor Fernando Eugénio Acabado Romana

Declaro que concedo à Atlântica, Instituto Universitário uma licença não-exclusiva para arquivar e tornar acessível, o presente trabalho, no todo ou em parte.

Retenho todos os direitos de autor relativos ao presente trabalho, e o direito de o usar futuramente

Assinatura: Pedro Miguel Pereira Esteves

Atlântica, Barcarena 15/11/2025

O autor é o único responsável pelas ideias expressas neste documento.

"Todo o nosso progresso tecnológico, que tanto se louva, o próprio cerne da nossa civilização, é como um machado na mão de um criminoso."

Albert Einstein.

Ao Francisco e à Ana

Aos meus irmãos

Aos meus pais.

Agradecimentos

A conclusão desta dissertação representa o culminar de mais um desafio pessoal, académico e profissional, que apenas foi possível graças ao contributo, apoio e incentivo de várias pessoas, às quais expresso o meu profundo agradecimento.

Em primeiro lugar, gostaria de manifestar o meu agradecimento especial à Ana Assunção, pelo apoio incondicional, pela paciência e pela revisão deste trabalho. Ao meu filho, deixo igualmente uma palavra de carinho, pela compreensão e pela "ausência" sentida ao longo dos últimos meses.

Manifesto o meu agradecimento ao Professor Doutor Fernando Eugénio Acabado Romana, pela orientação, disponibilidade e acompanhamento ao longo do desenvolvimento desta investigação. Agradeço também a todos os professores do mestrado, pelos conhecimentos transmitidos, bem como aos meus colegas do curso pela partilha de conhecimento e espírito de união que marcou esta caminhada. A vocês, "que ninguém fique para trás"!

Agradeço igualmente a todos os profissionais que participaram nos inquéritos e entrevistas, cuja disponibilidade e contributos foram fundamentais para a concretização desta dissertação. Um especial agradecimento ao Rodrigo Medeiros, pela partilha de conhecimento e contributos que foram determinantes para o enriquecimento deste trabalho.

Por último, mas não menos importante, agradeço o apoio dos meus colegas de trabalho que têm sido importantes para o meu crescimento pessoal e profissional. Uma palavra de especial apreço à Ecoambiente, S.A., pela oportunidade de frequentar esta formação, pela confiança demonstrada e pelas condições que tem proporcionado para o desenvolvimento da minha atividade profissional.

A todos, o meu sincero obrigado.

Resumo

Metodologia para Implementação da Diretiva NIS2

A crescente dependência das Tecnologias de Informação Comunicação (TIC), impulsionada pela Transformação Digital (TD) e por tecnologias emergentes como a Inteligência Artificial (IA), *big data*, *Internet of Things (*IoT*)* ou computação na nuvem, tem contribuído significativamente para o desenvolvimento económico e social das sociedades. Todavia, esta evolução tem criado uma maior exposição a ciberameaças, cada vez mais frequentes e sofisticadas. Como resposta a este cenário, a União Europeia (UE) aprovou a Diretiva (UE) 2022/2555 (NIS2), que revoga a Diretiva (UE) 2016/1148 (NIS), com o objetivo de reforçar a resiliência das redes e sistemas de informação no espaço europeu. Este estudo pretende desenvolver uma metodologia prática para apoiar as organizações – especialmente as Pequenas e Médias Empresas (PME) – na implementação proporcional e prática dos requisitos desta Diretiva.

Para atingir este objetivo, foi adotada uma investigação mista, combinando a revisão da literatura com a análise quantitativa (questionários) e qualitativa (entrevistas). A revisão da literatura permitiu clarificar os principais conceitos deste estudo – TIC, TD, Segurança da Informação (SI) e cibersegurança – bem como compreender a evolução das políticas nacionais e europeias orientadas para reforçar a cibersegurança. A análise efetuada revelou ainda que a NIS2 introduz requisitos mais rigorosos que a sua antecessora, nomeadamente o alargamento do âmbito de aplicação, o reforço das medidas de gestão dos riscos, a imposição de medidas relativas à cadeia de abastecimento e a atribuição de maiores responsabilidades aos órgãos de gestão. Adicionalmente, estabelece um regime de supervisão e sancionatório, que não estavam previstos na NIS.

Os resultados da análise quantitativa revelam que as organizações inseridas em setores com maior regulação – como a banca, infraestruturas digitais e energia – apresentam níveis de maturidade em cibersegurança mais elevados, enquanto que as restantes organizações demonstram fragilidades significativas. A componente qualitativa, baseada em entrevistas a especialistas de cibersegurança, confirmou estas assimetrias e permitiu identificar os principais desafios enfrentados pelas organizações, nomeadamente, a falta

de recursos humanos especializados, as limitações financeiras, a complexidade técnica e as dificuldades na gestão da cadeia de abastecimento.

Com base nesta análise, foi desenvolvida uma metodologia prática e adaptável, que pretende ser um instrumento de apoio, especialmente para as PME, na adoção faseada da Diretiva NIS2, alinhada com o perfil de risco e capacidade de cada entidade.

O Estudo reconhece algumas limitações, nomeadamente a impossibilidade de integrar a análise da Lei n.º 59/2025, que transpõe a Diretiva para ordenamento jurídico português, bem como o número reduzido de respostas ao inquérito. Para investigações futuras, recomenda-se o alargamento da amostra, bem como a validação prática da metodologia proposta em diferentes setores de atividade.

Palavras-chave: NIS2, cibersegurança, tecnologias de informação e comunicação

Abstract

Methodology for Implementing the NIS2 Directive

The growing dependence on Information and Communication Technologies (ICT), driven by Digital Transformation (DT) and by emerging technologies such as Artificial Intelligence (AI), big data, the Internet of Things (IoT) and cloud computing, has significantly contributed to the economic and social development of societies. However, this evolution has also increased exposure to cyber threats, which are becoming more frequent and sophisticated. In response to this scenario, the European Union (EU) approved Directive (EU) 2022/2555 (NIS2), which revokes Directive (EU) 2016/1148 (NIS), with the aim of strengthening the resilience of networks and information systems across the European space. This study aims to develop a practical methodology to support organisations — particularly Small and Medium-Sized Enterprises (SMEs) — in the proportional and effective implementation of the requirements established by this Directive.

To achieve this objective, a mixed-method approach was adopted, combining a literature review with quantitative (questionnaires) and qualitative (interviews) analyses. The literature review made it possible to clarify the key concepts underpinning the study — ICT, DT, Information Security (IS) and cybersecurity — as well as to understand the evolution of national and European policies directed at strengthening cybersecurity. The analysis further revealed that NIS2 introduces more stringent requirements than its predecessor, namely through the expansion of its scope, the reinforcement of risk management measures, the imposition of obligations relating to the supply chain, and the increased responsibilities assigned to management bodies. Additionally, it establishes a supervision and sanctioning regime that was not foreseen in the original NIS Directive.

The quantitative analysis shows that organisations operating in more heavily regulated sectors — such as banking, digital infrastructures and energy — display higher levels of cybersecurity maturity, whereas organisations in less regulated sectors demonstrate significant vulnerabilities. The qualitative component, based on interviews with cybersecurity specialists, confirmed these disparities and identified the main challenges

faced by organisations, namely the lack of specialised human resources, financial constraints, technical complexity and difficulties in managing supply chains.

Based on this analysis, a practical and adaptable methodology was developed to support organisations — particularly SMEs — in the phased adoption of the NIS2 Directive, aligned with their risk profile and organisational capacity.

The study acknowledges several limitations, including the inability to incorporate an analysis of Law No. 59/2025, which transposes the Directive into the Portuguese legal framework, as well as the limited number of valid survey responses. For future research, it is recommended to expand the sample size and to conduct a practical validation of the proposed methodology across different sectors of activity.

Keywords: NIS2, Cybersecurity, Information and Communication Technologies

Índice

Índice de figuras

Lista de abreviaturas

ANC – Autoridades Nacionais Competentes

AR – Assembleia da República

CCTV – *Closed-Circuit Television*

CE – Comissão Europeia

CER – *Critical Entities Resilience*

CNCS – Centro Nacional de Cibersegurança

CNPD – Comissão Nacional de Proteção de Dados

CRA – *Cyber Resilience Act* | Regulamento de Ciber-Resiliência

CSA – Cyber Solidarity Act | Regulamento de Cibersolidariedade

CSIRT – *Computer Security Incident Response Teams*

DDoS – *Distributed Denial of Service*

DORA – *Digital Operational Resilience Act*

EDN – Estratégia Digital Nacional

EDR – *Endpoint Detection and Response*

EM – Estado-Membro

ENSC – Estratégia Nacional de Segurança do Ciberespaço

ENISA – Agência da União Europeia para a Cibersegurança

ERM – *Enterprise Risk Management*

IDC – *International Data Corporation*

IA – Inteligência Artificial

IoT – *Internet Of Things*

ISO/IEC – *International Organization for Standardization / International Electrotechnical Commission*

ISP – *Internet Service Providers*

KPI – *Key Performance Indicators*

MDR – *Managed Detection and Response*

ML – *Machine Learning*

MGSTI – Mestrado em Gestão de Sistemas e Tecnologias de Informação

NDR – *Network Detection and Response*

NIS – *Network and Information Systems* | **SRI** – Segurança das Redes e da Informação

NIS 2 – *Network and Information Systems 2* | **SRI 2** – Segurança das Redes e da Informação 2

OSE – Operadores de Serviços Essenciais

PCM – Presidência do Conselho de Ministros

PCN – Plano de Continuidade de Negócio

PME – Pequenas e Médias Empresas

PRD – Plano de Recuperação de Desastres

PRI – Plano de Resposta a Incidentes

PSI – Política de Segurança da Informação

QACC – Quadro de Avaliação de Capacidades de Cibersegurança

QNRCS – Quadro Nacional de Referência para a Cibersegurança

RACI – *Responsible, Accountable, Consulted, Informed*

RGPD – Regulamento Geral de Proteção de Dados

SI – Segurança da Informação

SIEM – *Security Information and Event Management*

SPSS – *Statistical Package for the Social Sciences*

TD – Transformação Digital

TI – Tecnologias de Informação

TIC – Tecnologias de Informação e Comunicação

TFUE – Tratado sobre o Funcionamento da União Europeia

UE – União Europeia

UE-CyCLONe – Rede Europeia de Organizações de Coordenação de Cibercrises

Introdução

A rápida Transformação Digital e a crescente interligação das sociedades têm conduzido os sistemas de rede e de informação a desempenharem um papel central no dia-a-dia de cidadãos, empresas e países. A utilização generalizada das Tecnologias de Informação e Comunicação, impulsionada pela internet, tornou-se particularmente importante em setores críticos como a economia, a saúde, a educação, a energia e os transportes. Atividades quotidianas como o entretenimento, as compras online, a comunicação, o acesso aos serviços bancários, a formação e o trabalho remoto são hoje disponibilizados no ciberespaço.

O aumento da utilização de dispositivos móveis e a rápida evolução de tecnologias digitais como a Inteligência Artificial, a M*achine Learning* (ML), a *Internet Of Things*, a computação na nuvem e a *edge computing*, têm contribuído para aumentar significativamente a complexidade e a interdependência das infraestruturas digitais. Este avanço tecnológico tem gerado um enorme volume de dados interconectados, promovendo o crescimento exponencial do tráfego digital, como demonstrado pela previsão da *International Data Corporation - IDC* (IDC, 2021). De acordo com a IDC, em 2025 existirão cerca de 55,7 mil milhões de dispositivos IoT, responsáveis por produzir cerca de 80 *zettabytes* de dados.

A utilização massiva de tecnologia, associada à rápida TD e interligação crescente das sociedades, intensificou a partilha de dados, aumentando as relações de dependência e interdependência entre as infraestruturas utilizadas. Uma falha numa infraestrutura crítica, como na internet, pode afetar outros serviços dela dependentes, como a banca, a saúde, a energia ou os transportes, com graves consequências para os utilizadores e para a sociedade em geral.

Esta crescente conetividade e interdependência dos serviços e produtos digitais aumenta igualmente os riscos e vulnerabilidades, expondo o espaço digital a ciberameaças cada vez mais sofisticadas, frequentes e complexas. Torna-se, por isso, essencial garantir “um ciberespaço mundial, aberto, livre, estável e seguro, no qual se apliquem inteiramente os direitos humanos, as liberdades fundamentais e o Estado de direito” (EU, 2025a).

No contexto europeu, o aumento da dependência de sistemas de informação e de serviços digitais impulsionou a criação de legislação específica destinada a reforçar a segurança cibernética e a garantir a continuidade dos serviços essenciais. A Diretiva (UE) 2016/1148 (*Network and Information Security Directive* – NIS) foi a primeira tentativa de estabelecer um elevado nível de segurança nas redes e sistemas de informação da União Europeia. Esta tinha como como principal objetivo "estabelece medidas destinadas a alcançar um elevado nível comum de segurança das redes e dos sistemas de informação na União, a fim de melhorar o funcionamento do mercado interno" (UE, 2016).

A NIS pretendia promover esforços coordenados entre os Estados-Membros (EM), nomeadamente na implementação de medidas de segurança robustas, estratégias de gestão de risco e mecanismos de resposta a incidentes. Contudo, a rápida evolução tecnológica e o aumento das ameaças cibernéticas evidenciaram limitações na eficácia da Diretiva NIS, o que motivou a sua revisão. Em 2022, a UE aprovou a Diretiva (UE) 2022/2555 (*Network and Information Security Directive* – NIS2), com o objetivo de colmatar as lacunas identificadas na NIS e responder de forma mais eficaz aos desafios atuais e emergentes no domínio da cibersegurança. Ao revogar a sua antecessora, a nova Diretiva veio reforçar o quadro normativo europeu, introduzindo requisitos mais rigorosos e abrangentes, adaptados às novas realidades tecnológicas e aos riscos atuais. De acordo com a NIS2, os EM deveriam ter adotado e publicado, até 17 de outubro de 2024, as disposições necessárias para dar cumprimento à Diretiva.

O presente trabalho tem como objetivo contribuir para a operacionalização da Diretiva NIS2, procurando descomplicar a sua interpretação e apoiar as organizações na implementação de medidas técnicas, operacionais e organizativas necessárias para garantir a conformidade com a legislação. Não se pretende elaborar um manual técnico sobre tecnologias de cibersegurança, nem um manual jurídico sobre a Diretiva, mas sim propor *guidelines* que permitam às entidades compreender e aplicar as medidas adequadas, fortalecendo a sua postura de cibersegurança e assegurar a conformidade com a NIS2.

Neste contexto, é importante reconhecer que a aplicação da Diretiva NIS2 não será homogénea em todas as organizações abrangidas. Sendo o tecido empresarial português

predominantemente constituído por Pequenas e Médias Empresas (PME), que são fundamentais para a economia nacional (DGAE, 2025), estas deparam-se frequentemente com constrangimentos de ordem técnica, financeira e organizacional, que poderão dificultar a compreensão e aplicação das exigências da NIS2.

Foi a pensar nestas organizações que surgiu o presente estudo, que tem como objetivo ajudá-las a interpretar a NIS2 e os seus requisitos.

Importa ainda referir que, durante a realização desta investigação, foi aprovada a Lei n.º 59/2025, em 22 de outubro de 2025, que autoriza o Governo a aprovar o regime jurídico da cibersegurança, transpondo para a legislação nacional a Diretiva (UE) 2022/2555, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União. Esta atualização normativa evidencia a pertinência e a atualidade do tema em análise neste estudo. Contudo, devido à fase avançada em que o presente trabalho se encontrava, não foi possível integrar a análise deste novo quadro legislativo.

Este enquadramento introdutório pretende situar o leitor no contexto que justifica a relevância e necessidade desta investigação, estabelecendo a base conceptual e normativa sobre a qual serão desenvolvidos os capítulos seguintes.

Enquadramento

Nas últimas décadas, a evolução da tecnologia tem desempenhado um papel determinante no desenvolvimento das sociedades, num contexto de globalização e redução das fronteiras geográficas, possibilitando uma partilha mais ampla de dados, informação e conhecimento. Esta rápida evolução, impulsionada pela inovação e pelo conhecimento, conduziu-nos à chamada Era Digital, uma nova fase económica e social, em que as TIC são uma das principais alavancas do desenvolvimento das sociedades atuais (Castells, M., 2010, Mansell, R., 2021 e Henman, F., 2022).

As tecnologias digitais têm vindo a alterar profundamente a vida das pessoas, organizações e países, transformando as formas de comunicação, de trabalho e de interação social (UE, 2025b). Como refere a UE (2024c):

> a digitalização tem o potencial de criar soluções para muitos dos desafios que a Europa e os cidadãos europeus atualmente enfrentam e oferece oportunidades, nomeadamente, criando postos de trabalho, promovendo a educação, impulsionando a competitividade e a inovação, combatendo as alterações climáticas e facilitando a transição ecológica.

A internet, enquanto infraestrutura global de comunicação, assume um papel central neste processo, como "um verdadeiro criador de valor que reformulou a economia e a sociedade", tornando-se fundamental para a sociedade e a economia a nível mundial (UE, 2025b).

A importância das TIC não se verifica apenas em contextos de normalidade, sendo especialmente importante em momentos de crise. A pandemia provocada pelo coronavírus SARS-CoV-2 (COVID 19), veio demostrar a resiliência da internet e das tecnologias digitais, que se revelaram fundamentais para a manutenção da atividade económica, social e institucional. Durante esse período, a articulação entre a internet e as ferramentas digitais transformou significativamente o quotidiano, contribuindo para mudanças estruturais nas formas de viver, trabalhar e comunicar.

Na sequência da pandemia, a digitalização foi considerada um passo incontornável para a recuperação económica e para a resiliência de vários setores de atividade. Neste contexto, a UE identificou a digitalização como vetor estratégico, capaz de acelerar a transição tecnológica e de preparar as sociedades e economias dos EM para a Era Digital (UE, 2025c).

A necessidade de um espaço digital seguro ganhou especial relevância na sequência da pandemia, com a UE a intensificar os seus esforços para criar "um ambiente digital seguro para os cidadãos e empresas, de uma forma inclusiva e acessível a todos", e que "salvaguarde os valores da UE e proteja os direitos fundamentais e a segurança dos cidadãos, reforçando simultaneamente a soberania digital da Europa" (UE, 2025c).

Tal como a pandemia, também a guerra da Rússia contra a Ucrânia revelou a importância fundamental das TIC para a resiliência das sociedades. No domínio da comunicação e da informação, as tecnologias digitais foram cruciais para manter os cidadãos e a comunidade internacional informados em tempo real, contrariar a desinformação e reforçar a diplomacia pública (*European Parliament Research Service*, 2022). Ao nível da continuidade de serviços críticos, as TIC desempenharam um papel fundamental na manutenção de funções governativas, educativas e de saúde, sendo especialmente importante o exemplo do programa *Starlink*, por exemplo, que assegurou as comunicações em zonas afetadas pelo conflito (Bojor, L., Petrache, T. & Cristescu, C. (2024).

No campo da cibersegurança, a intensificação de ciberataques contra infraestruturas militares e civis críticas na UE demonstrou a interdependência entre ataques físicos e digitais, reforçando a necessidade de dotar as organizações e países de defesas robustas para proteger as suas infraestruturas críticas (ENISA, 2023, 2024). Simultaneamente, as plataformas digitais facilitaram a mobilização de solidariedade, apoios financeiros e logísticos no apoio à Ucrânia, transformando o espaço digital num verdadeiro "campo de batalha paralelo" (NATO, 2024; UE, 2023), confirmando a importância de proteger quer o espaço físico, quer o espaço virtual.

Estes eventos demonstram que o espaço digital não é apenas um meio complementar de atuação, mas parte integrante da segurança digital, o que torna imprescindível a compreensão da natureza e evolução do ciberespaço – um ambiente virtual onde circula informação digital e onde as pessoas e organizações interagem social, cultural e economicamente. Este fenómeno contribuiu para o aumento da conectividade entre sociedades, mas também para o aparecimento de novas ameaças digitais, incluindo o roubo de dados, ataques a sistemas de informação, fraudes, manipulação de informação, etc.

Perante este cenário, a UE tem vindo a definir e a implementar uma estratégia de cibersegurança orientada para o reforço da segurança e da resiliência das redes e dos sistemas de informação. O objetivo é assegurar que cidadãos e organizações possam utilizar serviços e ferramentas digitais de forma fiável e segura em todo o espaço europeu. Como refere a própria União na Diretiva (UE) 2022/2555, esta estratégia visa:

> desenvolver as capacidades de cibersegurança em toda a União, atenuar as ameaças aos sistemas de rede e informação utilizados para prestar serviços essenciais em setores-chave e garantir a continuidade de tais serviços face a incidentes, contribuindo assim para a segurança da União e para o eficaz funcionamento da sua economia e sociedade.

Para que esta estratégia europeia tenha sucesso, a UE tem criado um conjunto de atos jurídicos destinados a impor aos EM a adoção de medidas de cibersegurança que abranjam as infraestruturas críticas e as entidades consideradas essenciais e importantes. À data da redação deste estudo, destacam-se além da Diretiva NIS2, o Regulamento de Cibersegurança da União Europeia (2019), o Regulamento DORA – *Digital Operational Resilience Act* (2022), o Regulamento de Ciber-Resiliência (2024) e o Regulamento de Ciber-Solidariedade (2024). Em conjunto, estes instrumentos procuram reforçar as capacidades coletivas de resposta a ciberataques de grande escala e promover a cooperação internacional, com vista a garantir a segurança e a estabilidade do ciberespaço.

A consolidação deste quadro legislativo representa, assim, um marco fundamental no reforço da segurança e da resiliência das redes e sistemas de informação na UE, num contexto marcado pelo agravamento do panorama de ciberameaças. É neste enquadramento que surge a Diretiva NIS2, enquanto instrumento central da estratégia europeia para cibersegurança. Contudo, a sua implementação coloca grandes desafios às organizações, sobretudo devido à ausência de uma metodologia prática e adaptável que facilite a sua interpretação e aplicação.

Esta lacuna constitui o ponto de partida e o principal motivo desta investigação, que visa propor uma metodologia que responda a esta necessidade e contribua para garantir um elevado nível comum de cibersegurança na União.

Definições

A área da cibersegurança é complexa e nem sempre os termos são de fácil compreensão por parte dos leitores. Importa, assim, clarificar as principais definições utilizadas no presente trabalho para ajudar a compreender o tema apresentado.

Para efeitos deste estudo, entende-se por:

- Ameaça: *any circumstance or event with the potential to adversely impact organizational operations and assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, or modification of information, and/or denial of service"*[1]*;*
  Ameaças contra dados: também conhecido por "violação de dados pessoais", é "uma violação da segurança que provoque, de modo acidental ou ilícito, a destruição, a perda, a alteração, a divulgação ou o acesso, não autorizados, a dados pessoais transmitidos, conservados ou sujeitos a qualquer outro tipo de tratamento"[2];

[1]*National Institute of Standards and Technology. (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). U.S. Department of Commerce*.
[2] Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho.

- Ataque*:* "a*n attempt to gain unauthorized access to system services, resources, or information, or an attempt to compromise system integrity*"[3];
- *Blockchain: "is a secure database shared across a network of participants, where up-to-date information is available to all participants at the same time"[4];*
- *Boot*: "rede de computadores infetados (*drones*) por software malicioso e controlados à distância, sem o conhecimento dos utilizadores, com a finalidade de enviar mensagens eletrónicas não solicitadas, roubar informações ou lançar ciberataques coordenados"[5];
- Burla online: também conhecida por "*pharming*", "é a combinação de "*phishing*" e "*farming*" (cultivo), é um golpe online similar ao *phishing*"[6];
- *CEO Fraud*: "ocorre quando um colaborador autorizado a fazer pagamentos é ludibriado (por alguém que se faz passar, frequentemente, pela chefia da organização) no sentido de pagar uma fatura falsa ou realizar uma transferência não autorizada da conta bancária da organização"[7];
- Ciberataque: "*refers to an attack through IT in cyber space, which is directed against one or several IT system(s). Its aim is to undermine the objectives of ICT security protection (confidentiality, integrity and availability) partly or totally*."[8];
- Ciberespaço: "*a global domain within the information environment consisting of the interdependent network of information systems infrastructures including the internet, telecommunications networks, computer systems, and embedded processors and controllers"*[9];

[3] https://nvlpubs.nist.gov/nistpubs/ir/2013/nist.ir.7298r2.pdf

[4] https://www.mckinsey.com/featured-insights/mckinsey-explainers/what-is-blockchain#/

[5] https://www.eca.europa.eu/Lists/ECADocuments/BRP_CYBERSECURITY/BRP_CYBERSECURITY_PT.pdf.

[6] https://www.kaspersky.com.br/resource-center/definitions/pharming

[7] https://www.europol.europa.eu/sites/default/files/documents/4_ceo-bec_fraud.pdf.

[8] Austria's Cyber Space Security Strategy 2013.

[9] https://csrc.nist.gov/glossary/term/cyberspace?

- Ciberameaça: "uma circunstância, um evento ou uma ação potencial suscetíveis de lesar, perturbar ou ter qualquer outro efeito negativo sobre as redes e os sistemas de informação, os seus utilizadores e outras pessoas"[10];
- Cybercrime: "*consists of criminal acts committed online by using electronic communications networks and information systems*."[11];
- Cibercriminoso: "*are individuals or teams of people who use technology to commit malicious activities on digital systems or networks with the intention of stealing sensitive company information or personal data, and generating profit"*[12];
- Ciberesiliência: *"Cyber resilience means being not only prepared for cyber threats, but also capable of whithstanding and recovering from them, and adapting to ongoing risks*"[13];
- Ciberespionagem: "ameaça geralmente direcionada aos setores industriais, às infraestruturas críticas e estratégicas em todo o mundo, incluindo entidades governamentais, transportes, provedores de telecomunicações, empresas de energia, hospitais e bancos. Foca-se na geopolítica, no roubo de segredos comerciais e de Estado, de direitos de propriedade intelectual e de informações proprietárias em campos estratégicos"[14];
- Cibersabotagem: "*refers to any sabotage activity facilitated by or using cyber space*"[15];
- Cibersegurança: "todas as atividades necessárias para proteger de ciberameaças as redes e os sistemas de informação, os seus utilizadores e outras pessoas afetadas"[16];
- Computação na Nuvem: também conhecida por "*cloud computing*", "é a disponibilização de serviços informáticos, incluindo servidores, armazenamento,

[10] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho.

[11] https://home-affairs.ec.europa.eu/policies/internal-security/cybercrime_en

[12]https://www.trendmicro.com/vinfo/us/security/definition/cybercriminals#:~:text=Cybercriminals%20are%20individuals%20or%20teams,personal%20data%2C%20and%20generating%20profit

[13] https://finance.ec.europa.eu/digital-finance/cyber-resilience_en

[14] ENISA, Threat Landscape 2018.

[15] ENISA: ENISA overview of cybersecurity and related terminology. Versão 1. 2017.

[16] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho.

bases de dados, rede, software, análise e informações, através da internet ("a *cloud*") para disponibilizar mais rapidamente inovação, recursos flexíveis e poupanças no dimensionamento"[17];

- Computação Periférica: também conhecida por "e*dge computing"*, "é uma tecnologia de rede que permite que dispositivos em locais remotos processem dados e executem ações em tempo real. Funciona ao minimizar a latência da rede através do processamento da maioria dos dados na "periferia" da rede - como pelo próprio dispositivo ou por um servidor próximo - e enviando apenas os dados mais relevantes para o centro de dados principal para processamento quase instantâneo"[18];
- Dados pessoais: "informações relativas a uma pessoa singular identificada ou identificável (titular dos dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador como, por exemplo, um nome, um número de identificação, dados de localização, identificadores em linha ou um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular"[19];
- Diretiva: "é um ato legislativo que fixa um objetivo que os países da UE têm de alcançar. No entanto, cabe a cada país organizar as suas próprias leis para alcançar esses objetivos"[20];
- Engenharia social: "o ato de enganar um indivíduo no sentido de este revelar informação sensível, obtendo assim o acesso não autorizado ou cometendo fraude, com base numa associação com este indivíduo de modo a ganhar a sua confiança"[21];
- *Fake news*: também conhecidas como "notícias falsas", "são as narrativas que, embora anunciadas como notícias e contendo partes de textos copiados de jornais ou de sites do mesmo género, integram conteúdos ou informações falsas,

17 https://azure.microsoft.com/pt-pt/resources/cloud-computing-dictionary/what-is-cloud-computing.
18 https://azure.microsoft.com/pt-pt/resources/cloud-computing-dictionary/what-is-edge-computing.
19 Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho.
20 https://european-union.europa.eu/institutions-law-budget/law/types-legislation_pt
21 https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-63-3.pdf

imprecisas, enganadoras, concebidas, apresentadas e promovidas para intencionalmente causar dano público ou obter lucro"[22];

- Exfiltração de dados: "também conhecida como extrusão de dados ou exportação de dados – é o roubo de dados: a transferência intencional, não autorizada e oculta de dados de um computador ou outro dispositivo. A exfiltração de dados pode ser realizada manualmente ou automatizada usando malware"[23];
- Incidente: "evento com um efeito adverso real na segurança das redes e dos sistemas de informação"[24];
- Indústria 4.0: "conhecida como 4ª Revolução Industrial, é a integração de tecnologias digitais inteligentes em processos de produção e industriais. Esta engloba um conjunto de tecnologias que incluem redes industriais de *internet of things*, *artificial intelligence*, *big data*, robótica e automação"[25];
- *Infostealers*: "são um tipo de código malicioso (*malware*) desenvolvido para recolher dados sensíveis de um sistema. Os *infostealers* recolhem dados extremamente sensíveis tais como palavras-passe, *cookies*, detalhes bancários, carteiras de criptomoedas, emails e outros documentos"[26];
- Internet das Coisas: também conhecida como "i*nternet of things"*, "é a extensão da conectividade de rede e capacidade de computação para objetos, dispositivos, sensores e outros artefactos que normalmente não são considerados computadores"[27];
- Inteligência Artificial: também conhecida como "a*rtificial intelligence"*, "é a capacidade que uma máquina para reproduzir competências semelhantes às humanas como é o caso do raciocínio, a aprendizagem, o planeamento e a criatividade"[28];

[22] ERC 2019: https://www.parlamento.pt/Documents/2019/abril/desinformacao_contextoeuroeunacional-ERC-abril2019.pdf

[23] https://www.ibm.com/br-pt/think/topics/data-exfiltration

[24] Lei nº 46/2018, de 13 de agosto.

[25] https://www.sap.com/brazil/products/scm/industry-4-0/what-is-industry-4-0.html

[26] CNCS. (2025). Relatório de Cibersegurança em Portugal – Riscos e Conflitos, do Centro Nacional de Cibersegurança 2025.

[27] The Internet of Things: Na Overview, The Internet Society, 2015.

[28] https://www.europarl.europa.eu/topics/pt/article/20200827STO85804/o-que-e-a-inteligencia-artificial-e-como-funciona

- *Insider*: também conhecido como "ameaça interna", "pode existir em todas as empresas ou organizações. Qualquer colaborador atual ou ex-colaborador, sócio ou fornecedor, que tenha, ou tenha tido acesso aos ativos digitais da organização pode abusar, voluntaria ou involuntariamente, desse acesso. Os três tipos mais comuns de ameaças internas são: malicioso, que age intencionalmente; negligente, que é desleixado ou não está em conformidade com as políticas e instruções de segurança; e comprometido, que age involuntariamente como instrumento de um atacante real"[29];
- Hacktivista: "orientado a realizar ações de protesto contra decisões políticas/geopolíticas que afetam matérias nacionais e internacionais"[30];
- *Malware*: "também conhecido como código malicioso, é um termo genérico que descreve qualquer *software* ou *firmware* concebido para executar um processo não autorizado que tenha um impacto negativo na confidencialidade, integridade ou disponibilidade de um sistema"[31];
- *Machine learning*: "é um subconjunto da inteligência artificial que permite que um sistema aprenda e melhore de maneira autónoma, usando redes neurais e aprendizagem profunda, sem ter sido programado explicitamente para isso, ao ser alimentado com grandes quantidades de dados"[32];
- Negação de Serviço Distribuída: também conhecida como "*Distributed Denial of Service* (DDoS)", "é um ataque distribuído de negação de serviço, uma forma maliciosa de interromper o tráfego de um servidor, serviço ou rede, através da sobrecarga do mesmo"[33];
- *Phishing*: "é um tipo de engenharia social que utiliza e-mails, mensagens de texto ou de correio de voz aparentemente fidedignos para convencer as pessoas a divulgar informações confidenciais ou clicar numa ligação desconhecida"[34];

[29] ENISA, Threat Landscape 2018.

[30] ENISA, Threat Landscape 2018.

[31] https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

[32] https://cloud.google.com/learn/what-is-machine-learning?hl=pt-BR

[33] https://www.cncs.gov.pt/pt/intercop-ddos/

[34]https://www.microsoft.com/pt-pt/security/business/security-101/what-is-cybersecurity?msockid=11f0594558e0614b1ccf4c5c5987602d

- *Ramsomware*: "é definido como um tipo de ataque em que agentes maliciosos assumem o controlo dos ativos de um alvo e exigem um resgate em troca da restituição da disponibilidade desses ativos ou para evitar a divulgação pública dos dados do alvo"[35];
- Risco: "uma circunstância ou um evento, razoavelmente identificáveis, com um efeito adverso potencial na segurança das redes e dos sistemas de informação"[36];
- Segurança da Informação: "proteção dos sistemas de informação contra o acesso ou a modificação não autorizados da informação, durante o seu armazenamento, processamento ou transmissão, e contra a negação de serviço a utilizadores autorizados ou o fornecimento de serviço a utilizadores não autorizados, incluindo as medidas necessárias para detetar, documentar e contrariar tais ameaças."[37];
- Segurança dos sistemas de rede e informação: "a capacidade dos sistemas de rede e informação para resistir, com um dado nível de confiança, a eventos suscetíveis de pôr em causa a disponibilidade, a autenticidade, a integridade ou a confidencialidade dos dados armazenados, transmitidos ou tratados, ou dos serviços oferecidos por esses sistemas de rede e informação, ou acessíveis por intermédio destes"[38];
- *Sextortion*: "a prática de forçar alguém a fazer algo, particularmente a realizar atos sexuais (ou a pagar um resgate), através de uma ameaça de publicação de dados ou imagens de natureza íntima ou com cariz sexual da vítima (ameaça que por vezes não corresponde a uma possibilidade efetiva, apresentando-se detalhes técnicos, como a palavra--passe da vítima, de modo a tornar a ameaça mais credível)"[39];
- Sistemas de rede e informação: "um dispositivo ou grupo de dispositivos interligados ou associados, dos quais um ou mais executam, através de um programa, o tratamento automático de dados informáticos, bem como de dados

[35] https://www.enisa.europa.eu/topics/cyber-threats/threat-landscape

[36] Lei nº 46/2018, de 13 de agosto.

[37] https://apdsi.pt/glossario/s/seguranca-da-informacao/

[38] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho.

[39] CNCS. (2025). Relatórios de Cibersegurança em Portugal – Riscos e Conflitos, do Centro Nacional de Cibersegurança 2025.

informáticos armazenados, tratados, recuperados ou transmitidos por esse dispositivo ou grupo de dispositivos, tendo em vista o seu funcionamento, utilização, proteção e manutenção"[40];

- *Smishing*: é a "combinação das palavras SMS e *Phishing*, tratando-se da tentativa de adquirir informações pessoais, financeiras ou de segurança por texto mensagem"[41];
- Tecnologias de Informação e de Comunicação: "integração de métodos, processos de produção, hardware e software, com o objetivo de proporcionar a recolha, o processamento, a disseminação, a visualização e a utilização de informação, no interesse dos seus utilizadores"[42];
- Transformação Digital: "refere-se à utilização de tecnologias disruptivas para transformar digitalmente os negócios, ou seja, otimizar os serviços e produtos fornecidos, sustentar o crescimento económico e melhorar a experiência do utilizador"[43];
- *Vishing*: "*is the illegal access of data via voice over Internet Protocol (VoIP). Vishing is IP telephony's version of phishing and uses voice messages to steal identities and financial resources. The term is a combination of "voice" and "phishing"[44];*
- Vulnerabilidade: "é uma fragilidade, suscetibilidade ou falha, que afeta redes e sistemas de informação, produtos ou serviços de tecnologias da informação ou comunicação, passível de ser explorada por uma ciberameaça[45]";

[40] Diretiva (UE) 2013/40 do Parlamento Europeu e do Conselho.

[41] https://www.europol.europa.eu/sites/default/files/documents/3_phishing_vishing_sms.pdf

[42] https://apdsi.pt/glossario/t/tecnologias-da-informacao-e-comunicacao/

[43] M. Baslyman (2022). "Digital Transformation From the Industry Perspective: Definitions, Goals, Conceptual Model, and Processes," in IEEE Access, vol. 10, pp. 42961-42970, 2022, doi: 10.1109/ACCESS.2022.3166937

[44] https://www.techopedia.com/definition/4159/vishing

[45] Proposta de Lei n.º 50/XVI/1.ª

Identificação e enquadramento do problema de investigação

A rápida TD e interligação entre os países da UE fizeram com que os sistemas de rede e informação assumissem um papel central no quotidiano dos cidadãos, empresas e instituições europeias. Esta evolução tecnológica trouxe inúmeros benefícios, mas também atraiu um número crescente de ameaças no domínio da cibersegurança, que se tornaram mais frequentes e sofisticadas. Estas ameaças representam um risco real para o normal funcionamento dos sistemas de rede e informação, que podem ter impactos significativos nas atividades económicas e sociais no espaço europeu (ENISA, 2024a).

Com o objetivo de estabelecer um conjunto de medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União, e de proteger as organizações contra ameaças cibernéticas, assegurando a continuidade das atividades económicas, foi aprovada a Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022 – também designada por Diretiva SRI 2 ou NIS2. Esta nova Diretiva revoga a sua antecessora, a Diretiva (UE) 2016/1148 (Diretiva SRI 1) e mantém os três objetivos fundamentais que já orientavam a NIS, designadamente (CNCS, 2025a):

- Garantir que os EM asseguram um elevado nível de cibersegurança;
- Reforçar a cooperação europeia entre as autoridades competentes pela cibersegurança;
- Exigir que os principais operadores dos sectores-chave dos EM adotem as medidas de segurança necessárias e notifiquem às autoridades competentes qualquer incidente que tenha um impacto significativo na prestação dos seus serviços.

Este novo enquadramento legal introduz obrigações mais rigorosas para as entidades consideradas essenciais e importantes – de acordo com os anexos I e II da NIS2 –, impondo requisitos reforçados em matéria de cibersegurança e de reporte de incidentes. A sua implementação eficaz exige uma abordagem holística e coordenada, envolvendo todos os níveis da organização, desde a gestão de topo até aos serviços operacionais e administrativos.

Contudo, apesar da existência de orientações gerais para a aplicação da Diretiva NIS2, muitas organizações enfrentam desafios significativos na adaptação às novas exigências regulamentares, para garantir a conformidade. Esta dificuldade resulta, em grande medida, da ausência de metodologias práticas e ajustáveis à diversidade, dimensão e nível de maturidade das organizações na área de cibersegurança. Esta lacuna poderá traduzir-se numa implementação desigual e, nalguns casos, ineficaz, dos requisitos estabelecidos pela Diretiva, comprometendo a segurança e a resiliência do espaço digital europeu.

Deste modo, o problema central que se evidencia nesta investigação prende-se com a inexistência de metodologias práticas e adaptáveis que orientem as organizações – sobretudo as que não dispõem de recursos ou maturidade – na interpretação e aplicação da Diretiva NIS2.

O presente estudo procura dar resposta a essa necessidade, propondo o desenvolvimento de uma metodologia transversal e aplicável a diferentes realidades organizacionais, com especial enfoque naquelas que revelam maiores dificuldades na interpretação da Diretiva e dos seus requisitos.

Questão(ões) de investigação

A crescente utilização de tecnologias digitais para comunicar, trocar informação e fazer negócios tem exposto os indivíduos, organizações e Estados a riscos de cibersegurança. Torna-se, por isso, fundamental assegurar que os dispositivos eletrónicos, as redes de comunicação e os dados estão devidamente protegidos contra acessos não autorizados, roubo ou danos (Admass, W., et. al, 2024).

A implementação de medidas técnicas, operacionais e organizativas, para atenuar as ameaças aos sistemas de rede e informação das organizações, enfrenta múltiplos desafios, decorrentes da natureza dinâmica e complexa do ciberespaço, assim como da diversidade da origem das ameaças – inclui hackers, cibercriminosos, atores estatais, grupos terroristas ou *insiders* (Admass, W., et. al, 2024). Por outro lado, a heterogeneidade das organizações e dos setores de atividade dificulta a criação de metodologias homogéneas

para implementar as medidas que permitam assegurar um elevado nível comum de cibersegurança na UE, no geral, e em Portugal, em particular.

Neste enquadramento, o presente estudo tem como objetivo central o desenvolvimento de uma metodologia que permita superar os desafios na implementação da Diretiva NIS2. Assim, a investigação estrutura-se em torno da seguinte questão principal de investigação:

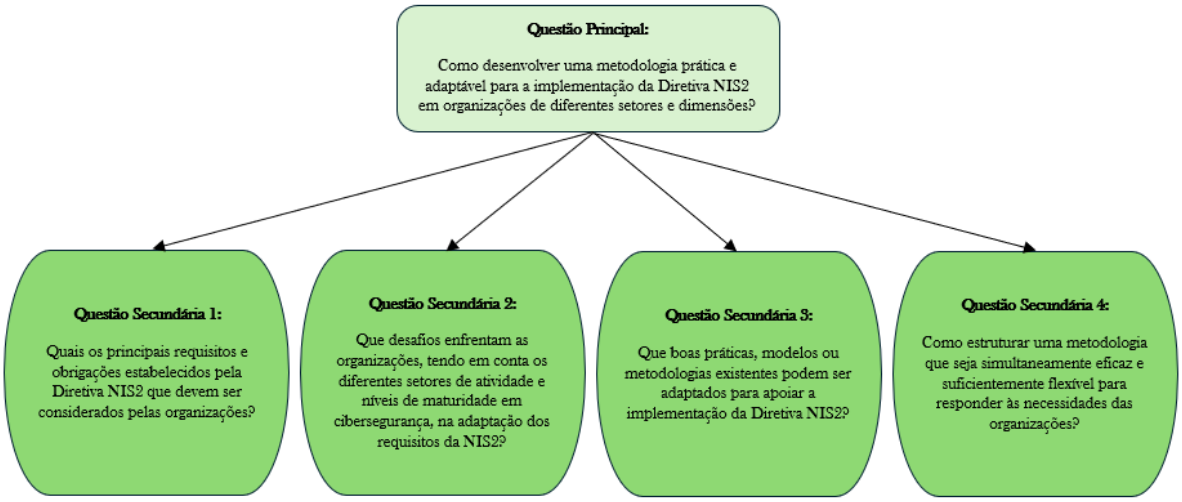
- Como desenvolver uma metodologia prática e adaptável para a implementação da Diretiva NIS2 em organizações de diferentes setores e dimensões?

Esta questão constitui o principal motivo que originou o interesse do tema desta investigação, uma vez que cada organização e cada setor apresentam contextos operacionais, perfis de risco e níveis de maturidade em cibersegurança distintos, o que dificulta a elaboração de uma metodologia suficientemente flexível para responder a essa diversidade.

De modo a explorar de forma abrangente as diferentes dimensões do problema e a construir uma resposta fundamentada à questão principal, a investigação contempla as seguintes questões secundárias (Figura 1):

1. Quais os principais requisitos e obrigações estabelecidos pela Diretiva NIS2 que devem ser considerados pelas organizações?
2. Que desafios enfrentam as organizações, tendo em conta os diferentes setores de atividade e níveis de maturidade em cibersegurança, na implementação dos requisitos da NIS2?
3. Que boas práticas, modelos ou metodologias existentes podem ser adaptados para apoiar a implementação da Diretiva NIS2?
4. Como estruturar uma metodologia que seja simultaneamente eficaz e suficientemente flexível para responder às necessidades das organizações?

Fig. 1 - Diagrama das questões do estudo



Fonte: elaboração própria, 2025

As questões orientadoras permitem explorar as várias dimensões do problema, desde a identificação de lacunas ao desenvolvimento e validação de uma metodologia prática. Embora a investigação se centre na resposta à questão principal, a consideração das questões secundárias é essencial para assegurar uma abordagem holística, rigorosa e fundamentada.

Objetivos propostos

Com o propósito de assegurar que a investigação produz resultados consistentes, relevantes e alinhados com a problemática em análise, foram definidos objetivos que visam estruturar as atividades a desenvolver, clarificar os métodos a utilizar e definir os mecanismos para acompanhar e avaliar a sua concretização. Importa salientar que, dado o carácter interdependente das questões de investigação, os objetivos propostos não se relacionam apenas com uma questão isolada, mas antes contribuem, de forma transversal e integrada, para a sua compreensão e resolução do conjunto das problemáticas em estudo.

Para alcançar o objetivo principal deste estudo – desenvolver uma metodologia prática e adaptável – foram identificados os seguintes objetivos específicos:

- Identificar e analisar o nível de maturidade das organizações em matéria de cibersegurança, através da aplicação de um questionário que permita avaliar o estado atual das práticas organizacionais, considerando como referência o Quadro Nacional de Referência para a Cibersegurança 2019 (QNRCS 2019) e o Quadro de Avaliação de Capacidades de Cibersegurança 2020 (QACC 2020);
- Identificar os principais desafios enfrentados pelas organizações na implementação de medidas técnicas, operacionais e organizativas necessárias para assegurar a conformidade com regulamentos, políticas e boas práticas na área da cibersegurança. Para o efeito, serão realizadas entrevistas a gestores, especialistas e profissionais das áreas das TIC, cibersegurança, incluindo consultores e responsáveis de *compliance,* com o objetivo de identificar os principais obstáculos associados à implementação das medidas previstas na Diretiva NIS2;

- Desenvolver uma metodologia prática e adaptável para a implementação da Diretiva NIS2, através do mapeamento dos seus requisitos e da identificação dos componentes críticos necessários à sua operacionalização. A metodologia proposta terá como base a análise de *frameworks* de referência (ex.: ISO/IEC 27000, *National Institute of Standards and Technology* – NIST 2.0, *Center for Internet Security Controls – CIS Controls* e o QNRCS 2019) e a integração de práticas reconhecidas, assegurando a sua aplicabilidade às diferentes organizações abrangidas pela Diretiva;

- Definir indicadores de desempenho *(Key Performance Indicators – KPI)* que permitam monitorizar a eficácia da implementação da Diretiva NIS2. Para tal, será proposto um sistema de monitorização baseado em KPI, que irá apoiar as organizações na avaliação contínua da conformidade regulamentar, na medição da eficácia das suas estratégias e na identificação de áreas a melhorar.

Os objetivos propostos visam abordar as questões de investigação de forma global, permitindo uma análise abrangente das capacidades de cibersegurança das organizações e das dificuldades associadas à implementação da Diretiva. Através da combinação de diferentes métodos de investigação – incluindo a aplicação de questionários, a realização

de entrevistas e a revisão da literatura especializada – será possível caracterizar o estado atual das organizações ao nível da cibersegurança, identificar os desafios e desenvolver soluções ajustadas à sua realidade.

Em síntese, a concretização destes objetivos permitirá alcançar uma metodologia útil, prática e adaptável para a implementação da Diretiva NIS2, alinhada com as necessidades e desafios específicos de cada organização.

Resultados esperados

Espera-se que este estudo conduza à definição de uma metodologia prática e adaptável para a implementação da Diretiva NIS2, aplicável a organizações de diferentes setores de atividade e dimensões. Pretende-se, deste modo, oferecer um instrumento de apoio que permita responder de forma prática e estruturada às exigências da Diretiva, contribuindo para o reforço da resiliência e da maturidade em cibersegurança.

Adicionalmente, prevê-se que a investigação proporcione respostas claras e fundamentadas às questões de investigação, assegurando uma avaliação sistemática dos objetivos definidos. O estudo deverá igualmente contribuir para o conhecimento científico sobre cibersegurança, no geral, e ao mesmo tempo, oferecer orientações práticas e inovadoras sobre como as organizações podem aplicar a Diretiva NIS2 de forma eficaz, em particular.

Reconhece-se ainda a importância de identificar as limitações inerentes ao processo de investigação e de apresentar recomendações que orientem futuros estudos. Desta forma, procura-se fomentar o aprofundamento do conhecimento e o desenvolvimento de práticas e metodologias mais robustas no domínio da conformidade com a Diretiva.

Metodologia e estrutura do documento

A metodologia adotada na realização deste estudo será a seguir detalhada, juntamente com as abordagens técnicas utilizadas na investigação. Serão descritos os métodos de recolha e análise de dados, bem como as principais etapas do processo de investigação, para colmatar a lacuna de conhecimento identificada.

Adicionalmente, é apresentada a estrutura do documento, fornecendo uma visão geral da sua organização interna e da lógica subjacente à disposição dos capítulos, de modo a garantir uma compreensão clara e coerente dos resultados e contribuições desta investigação.

Metodologia

Para a concretização dos objetivos definidos, foi adotada uma abordagem metodológica mista, combinando métodos qualitativos e quantitativos, com particular incidência no estudo exploratório. Esta opção metodológica revelou-se especialmente adequada ao objetivo central do estudo – desenvolver uma metodologia prática e adaptável para a implementação da Diretiva NIS2 – uma vez que permitiu obter uma compreensão aprofundada do tema em análise e, simultaneamente, transformar esse conhecimento em soluções aplicáveis em diferentes contextos organizacionais.

O estudo exploratório teve como principal objetivo permitir compreender a área da cibersegurança e da própria Diretiva NIS2, reconhecendo que a sua implementação exige um entendimento claro das respetivas exigências e implicações.

Complementarmente, e de forma a transformar esse conhecimento inicial numa solução prática e aplicável, recorreu-se aos princípios do *Design Science Research* (DSR). Esta abordagem metodológica foca-se no desenvolvimento de artefactos inovadores para responder a problemas reais e complexos.

A recolha de dados foi realizada de forma a assegurar a combinação entre diferentes fontes de informação e, assim, aumentar a validade e robustez dos resultados obtidos. Desta forma, foram utilizados três métodos: questionários, entrevistas e revisão da literatura.

Uma das metodologias utilizada foi a recolha dos dados através de um questionário online, desenvolvido na plataforma *Google Forms*, com o objetivo de avaliar o nível de maturidade das organizações em matéria de cibersegurança. Este questionário (Anexo I e II), baseado na ferramenta *CiberCheckUp* do Centro Nacional de Cibersegurança (CNCS), permitiu aferir o estado das organizações na área da cibersegurança, tendo como

referência o QNRCS 2019 e o QACC 2020. O questionário foi distribuído a profissionais de TIC e cibersegurança, através de correio eletrónico e da rede social *LinkedIn*.

Foram ainda realizadas cinco entrevistas estruturadas (Anexos III e IV) a profissionais das áreas de TIC e de cibersegurança. Estas entrevistas tiveram como objetivo aprofundar o conhecimento sobre o grau de preparação e implementação da Diretiva NIS2 nas organizações e compreender os principais desafios. As entrevistas foram estruturadas em quatro grupos temáticos relacionadas com a Diretiva, o que permitiu uma análise detalhada e comparável entre os participantes. A informação obtida complementou os resultados dos questionários e contribuiu para a construção da metodologia proposta.

Tanto o questionário como as entrevistas foram conduzidos em conformidade com os princípios éticos e de privacidade, assegurando a integridade e a credibilidade do estudo, a anonimização dos dados recolhidos, o consentimento informado dos participantes e o cumprimento rigoroso do Regulamento Geral de Proteção de Dados (RGPD). Estes fatores revelam-se essenciais para a proteção dos dados pessoais e para a garantia da integridade científica da investigação.

Os dados recolhidos foram analisados através de métodos quantitativos e qualitativos. As respostas ao questionário foram tratadas através de análise estatística descritiva, com o objetivo de caracterizar o nível de maturidade das organizações e identificar padrões pertinentes nas práticas de cibersegurança. Por outro lado, as entrevistas foram submetidas a uma análise temática, permitindo identificar os temas centrais e extrair conhecimento qualitativo sobre os desafios associados à implementação da Diretiva NIS2.

Adicionalmente, foi realizada uma revisão da literatura, abrangendo livros, legislação, artigos científicos e outros trabalhos académicos relacionados com a cibersegurança e com a Diretiva NIS2. Esta etapa foi muito importante para fundamentar teoricamente a investigação, para identificar boas práticas existentes e compreender a evolução do quadro legal e técnico nestas áreas. Esta análise permitiu ainda evidenciar a relevância do tema e contextualizar a importância da cibersegurança no panorama atual.

A metodologia adotada neste estudo procurou integrar diferentes abordagens e técnicas de recolha e análise de dados, com o objetivo de constituir uma base sólida para o desenvolvimento da metodologia proposta. A utilização do DSR possibilitou converter o conhecimento adquirido num artefacto prático – uma metodologia adaptável – que visa apoiar as organizações na implementação eficaz da Diretiva NIS 2.

Quanto ao tratamento e análise dos dados, foram utilizadas ferramentas e métodos apropriados que asseguraram a fiabilidade dos resultados e o cumprimento rigoroso das normas legais e éticas no processamento da informação.

Estrutura do Trabalho

O presente estudo encontra-se organizado de forma sistemática, com o objetivo de garantir a clareza, coerência e continuidade lógica do tema de investigação. Apresenta-se, de seguida, a estrutura do trabalho, descrevendo de forma sintética a articulação de cada um dos capítulos, desde a introdução até às considerações finais, assegurando uma visão integrada do estudo.

O trabalho está dividido em três partes distintas: introdução, desenvolvimento (subdividido em capítulos e subcapítulos) e conclusão, conforme se descreve a seguir:

- Introdução

  Apresenta o enquadramento do tema em análise, as principais definições e o contexto teórico necessário à sua compreensão. Nesta parte do trabalho são identificados o problema de investigação e as questões de investigação que orientam o estudo, seguidos da formulação dos objetivos e dos resultados esperados, em alinhamento com a problemática delineada. Por fim, é descrita a metodologia adotada, que orienta o percurso da investigação, e apresentada a estrutura do documento, proporcionando uma visão organizada e coerente do trabalho desenvolvido.
- Capítulo 1 – Revisão da literatura

  Tem como propósito realizar uma revisão da literatura relevante, com o objetivo de contextualizar o tema da investigação, identificar o estado da arte e os

principais contributos já produzidos sobre os temas abordados. Aborda a evolução das ameaças e ciberataques em Portugal e na Europa, considerando a sua frequência, sofisticação e complexidade crescentes. Este capítulo permite evidenciar lacunas de conhecimento e fundamentar a importância e originalidade do estudo, construindo o enquadramento teórico que sustenta a análise e assegura o rigor científico da investigação.

- Capítulo 2 – Diretiva NIS2

  Apresenta uma análise detalhada da Diretiva (UE) 2022/2555 (NIS2), desmistificando os seus principais conceitos e comparando-a com a sua antecessora, a Diretiva (UE) 2016/1148 (NIS). Esta análise comparativa evidencia a evolução do enquadramento regulatório europeu, destacando as limitações identificadas da primeira Diretiva e as melhorias introduzidas com NIS2, nomeadamente no reforço das obrigações de gestão dos riscos e de incidentes, e na introdução de mecanismos mais exigentes de supervisão e sanções. O capítulo contribui, assim, para compreender o impacto e as implicações da nova Diretiva nas organizações abrangidas.

- Capítulo 3 – Avaliação e resultados dos inquéritos e entrevistas

  Expõe a análise exploratória desenvolvida no âmbito da investigação, em articulação com os princípios do DSR. O capítulo apresenta e discute os dados recolhidos através de inquéritos e entrevistas, procurando compreender o nível de maturidade das organizações em matéria de cibersegurança e os principais desafios associados à implementação da Diretiva NIS2. A conjugação de dados quantitativos e qualitativos permite uma visão integrada e fundamentada da realidade atual, servindo de base à construção da proposta metodológica apresentada no capítulo seguinte.

- Capítulo 4 – Proposta de metodologia para implementar a NIS2

  Apresenta a metodologia desenvolvida para apoiar a implementação da Diretiva NIS2 nas organizações, independentemente da sua dimensão ou setor de atividade. A proposta resulta da análise exploratória e da identificação das principais necessidades e desafios enfrentados pelas entidades, integrando boas práticas de cibersegurança, requisitos normativos e orientações operacionais. O

objetivo é disponibilizar um referencial estruturado, adaptável e pragmático, que permita às organizações reforçar as suas capacidades de gestão de risco e conformidade, assegurando uma implementação eficaz e sustentável da Diretiva.

- Conclusões

  Reúne as principais conclusões do estudo, relacionando os resultados obtidos com os objetivos e a questão de investigação. O capítulo destaca os contributos teóricos e práticos da investigação, a relevância da metodologia proposta para a implementação da NIS2 e as limitações identificadas. São igualmente apresentadas recomendações para trabalhos futuros, com vista ao aprofundamento da investigação sobre cibersegurança e a conformidade regulatória em contexto organizacional.

Por fim, são incluídos no final do documento, a lista de referências utilizadas e os anexos considerados relevantes para o estudo.

1. Revisão da Literatura

Este capítulo procede a uma revisão da literatura que articula, de forma encadeada, a relação entre a transformação digital, os fundamentos conceptuais da segurança da informação e da cibersegurança, e a evolução das ameaças no ciberespaço em Portugal e na UE.

A revisão inicia-se com uma reflexão sobre a importância das TIC na sociedade atual, cuja rápida evolução estimulou alterações significativas na economia, na sociedade e nas organizações. Este progresso tecnológico, alavancado pelas mais recentes tecnologias digitais (IA, computação na nuvem, IOT, comunicações 5G e 6G, entre outras) transformou de forma significativa as dinâmicas de interação.

A TD criou oportunidades e benefícios significativos, mas trouxe também consigo novas vulnerabilidades e riscos em matéria de segurança da informação e proteção de dados. Para uma melhor compreensão do estudo, será efetuada uma abordagem aos conceitos de segurança da informação, proteção de dados e cibersegurança, uma vez que, embora frequentemente utilizados como sinónimos, apresentam diferenças conceptuais relevantes.

O reconhecimento da importância destes temas está patente nos esforços desenvolvidos ao nível nacional e europeu para consolidar uma cultura de segurança digital e reforçar a resiliência das economias e sociedades. Como resultado destes esforços, a estratégia de Portugal tem evoluído de forma gradual, acompanhando o progresso tecnológico e o aumento das ameaças digitais, e incentivado pelas políticas europeias na área da cibersegurança. Do mesmo modo, a estratégia europeia tem seguido uma trajetória progressiva e integrada, refletindo a necessidade de responder à crescente sofisticação das ameaças cibernéticas, através do reforço do quadro normativo, com o objetivo de proteger os cidadãos, as organizações e as infraestruturas críticas, promovendo simultaneamente a resiliência, a confiança e a segurança no mercado único digital.

A rápida evolução da TD tem sido acompanhada por um aumento contínuo da magnitude, frequência e impacto dos incidentes de cibersegurança, tornando as ciberameaças um dos principais fatores de risco para a segurança digital, estabilidade económica e proteção dos

direitos fundamentais, incluindo a privacidade e a proteção de dados pessoais. A análise da evolução das ciberameaças nos últimos anos, assim como a identificação das principais tipologias e tendências dos ciberataques, permite compreender os principais riscos associados.

Face a este cenário, tornou-se imperativo o desenvolvimento de quadros estratégicos e normativos capazes de reforçar a resiliência digital e garantir um elevado nível comum de segurança das redes e dos sistemas de informação. É neste contexto que se insere a Diretiva (UE) 2022/2555, também conhecida como Diretiva SRI 2 (Diretiva relativa à Segurança das Sedes e da Informação 2) ou NIS2 (*Directive on Security of Network and Information Systems* 2), que representa um passo fundamental para a política europeia de cibersegurança, não apenas do papel que desempenha no robustecimento da capacidade coletiva de prevenção e mitigação de ciberameaças, mas também do contributo para a consolidação da confiança no espaço digital europeu.

Em Portugal, a sua futura implementação representa, igualmente, um marco decisivo na consolidação da segurança das redes e dos sistemas de informação, justificando, assim, uma abordagem prospetiva que permita compreender o seu potencial impacto, os desafios que coloca e as implicações que poderá ter no reforço da cibersegurança a nível nacional.

1.1. Tecnologias de Informação e Comunicação na Era Digital

Nas últimas décadas, a evolução tecnológica assumiu um papel determinante no desenvolvimento das sociedades contemporâneas. No atual contexto de globalização, as barreiras geográficas e a distância deixaram de constituir obstáculos significativos à circulação de dados, informação e conhecimento, permitindo uma interconectividade sem precedentes. Vivemos, assim, numa verdadeira "era social", onde uma sociedade moderna e desenvolvida se mede, em grande parte, pela sua capacidade de integrar e dinamizar fluxos de informação, destacando-se particularmente aquelas que apostam, de forma estratégica, na utilização de ferramentas tecnológicas (Julião, 2003).

Esta rápida evolução tecnológica, sustentada pelo conhecimento e pela inovação, num contexto de crescente importância dos fluxos de informação, conduz-nos a uma

Sociedade da Informação. Trata-se de uma nova etapa económica e social na história da humanidade, em que as TIC afirmam-se como uma das principais alavancas do desenvolvimento das sociedades. Este modelo assenta, em grande medida, na evolução e utilização quotidiana das TIC em várias áreas, desde a pessoal e profissional ao lazer, com impactos significativos em setores tão diversos como os transportes, a educação, a saúde ou o ambiente.

Nas últimas décadas, a crescente evolução das TIC transformou de forma rápida e profunda a forma como as sociedades, no geral, e os indivíduos e as organizações, em particular, interagem entre si (Bambi, et al., 2025). Neste enquadramento, Castells e Cardoso (2006) salientam que "o desenvolvimento económico e social dos países, cidades ou zonas na Era da Informação" está intrinsecamente ligado à utilização "das ferramentas tecnológicas e à sua integração nos circuitos produtivos e de relacionamento pessoal necessitando, todo o país, cidade ou zona, de realizar a inserção efetiva das mesmas no tecido empresarial e ao nível do Estado".

Neste contexto, as TIC assumem um papel central nas sociedades modernas, na medida em que fomentam:

> as potencialidades do sector da informação para a criação de emprego sustentável, para a transformação das organizações no sentido de um aumento da sua produtividade, para a melhoria da qualidade de vida das populações e ainda para a coesão económica e social (MSI, 1997).

As TIC são frequentemente utilizadas como sinónimo de Tecnologias de Informação (TI). No entanto, importa referir que, apesar de serem conceitos muito próximos, ambos se referem a áreas distintas. Segundo Awati et al. (2025), as TIC representam uma "lista mais abrangente de componentes relacionados com sistemas de computador e tecnologias digitais", enquanto as TI estão mais focadas na gestão das "tecnologias relacionadas com a informação e os seus diversos aspetos técnicos, incluindo software, hardware e redes". De acordo com os mesmos autores, a gestão de TI não inclui "considerações sobre

dispositivos de telecomunicações e tecnologias digitais, enquanto as TIC sim". Desta forma, podemos considerar que as TI constituem um subconjunto das TIC.

No entanto, o rápido desenvolvimento tecnológico torna a própria definição de TIC dinâmica, uma vez que estas englobam várias tecnologias, que estão em constante transformação. Apesar dessa evolução, o objetivo central das TIC mantém-se: permitir a partilha de informação entre pessoas, organizações e países. Neste sentido, importa clarificar, ainda que de forma sintética, o conceito de TIC.

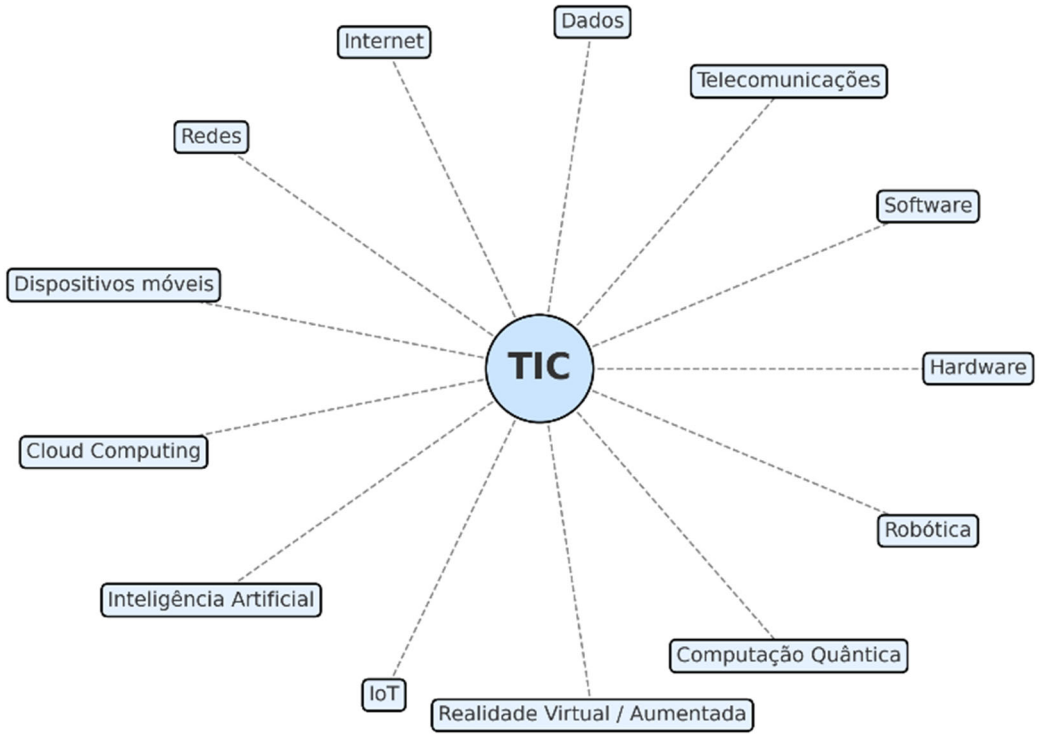
Segundo Silva (2001), as TIC são um conjunto de ferramentas que "convergem a informática, o audiovisual e as telecomunicações na constituição de uma rede comunicativa universal". Ou seja, o autor defende que as TIC resultam da interligação entre as TI e as Telecomunicações e, em conjunto, constituem uma rede de comunicação global. Neste mesmo sentido, Awati et al. (2025), acrescentam que "as TIC constituem a infraestrutura e os componentes que possibilitam a computação moderna", sublinhando que estas ferramentas visam "melhorar a forma como os seres humanos criam, processam e partilham dados ou informações entre si".

Para estes autores, as TIC contribuem para "melhorar as suas capacidades em diversas áreas, incluindo negócios, educação, medicina, resolução de problemas do mundo real e até atividades de lazer relacionadas com desporto, música e cinema". De forma complementar, Rouse (2016, citado por Bambi et al., 2025) refere que as TIC correspondem "à integração das telecomunicações, computadores e outras ferramentas digitais para aceder, armazenar, transmitir e manipular informações", abrangendo "uma vasta gama de tecnologias", entre as quais a "internet, redes sem fios, telemóveis e outros meios de comunicação".

Constata-se, assim, que não existe uma definição universalmente aceite para as TIC, uma vez que o conceito se encontra intimamente associado à evolução das próprias tecnologias, dos dispositivos e das necessidades ao longo do tempo. Todavia, para efeitos do presente estudo, e de forma simplificada, entende-se que as TIC correspondem a um conjunto de tecnologias destinadas à recolha, armazenamento, processamento, consulta,

análise e transmissão de informação, abrangendo, entre outros elementos, o hardware, o software, as telecomunicações, os dados e, naturalmente, a Internet (Figura 2).

Fig. 2 - Componentes das TIC



Fonte: elaboração própria, 2025

Segundo Awati et al. (2025), a lista de componentes das TIC está em constante expansão e continuará a crescer, em resultado do progresso tecnológico. Se no passado os computadores e telefones, que existem há várias décadas, constituíam a base das TIC, atualmente essa lista integra também os dispositivos móveis, como *smartphones*, *smartwatches* e *tablets*, bem como televisões inteligentes, sensores e *robots*.

Com a contínua evolução tecnológica, podemos incluir nas TIC tecnologias mais modernas e disruptivas, entre as quais a IA, o IoT, as comunicações 5G e 6G, o *ML*, a realidade virtual, a computação quântica e a robótica (Awati et al., 2025).

Em síntese, e de acordo com Awati et al. (2025), qualquer tecnologia, infraestrutura, componente ou dispositivo que permita a comunicação, a partilha de dados e a

conectividade global entre indivíduos, organizações e países pode ser integrado no conceito de TIC.

Com base nesta definição mais abrangente, importa salientar que, no início do século XXI, as TIC entraram numa nova fase de desenvolvimento marcada pela crescente integração das tecnologias digitais, dando origem à denominada Era Digital. Este período foi impulsionado pela convergência de várias inovações, com destaque para as tecnologias móveis – em especial os smartphones – que democratizaram o acesso à internet e a conteúdos digitais, em qualquer contexto geográfico. Paralelamente, o avanço das tecnologias como a computação na nuvem, a IA e a análise de grandes volumes de dados, impulsionaram a criação de novos serviços digitais, transformando significativamente setores como o comércio eletrónico, a educação e a formação online, e as plataformas colaborativas (Bambi et al., 2025). Estes desenvolvimentos tiveram um papel importante no desencadear da TD, vista como fundamental na reconfiguração dos modelos de interação, produção e prestação de serviços.

No mesmo sentido evolutivo, o crescimento das redes sociais – como o Facebook, rede X e o Instagram – introduziu novas formas de comunicação e partilha de informação em tempo real (Bambi et al., 2025). Estas plataformas tornaram-se componentes essenciais da infraestrutura digital moderna, exercendo um impacto significativo na forma como estas tecnologias influenciam, desde relações pessoais a formas de trabalhar, e até movimentos políticos (Bambi et al., 2025).

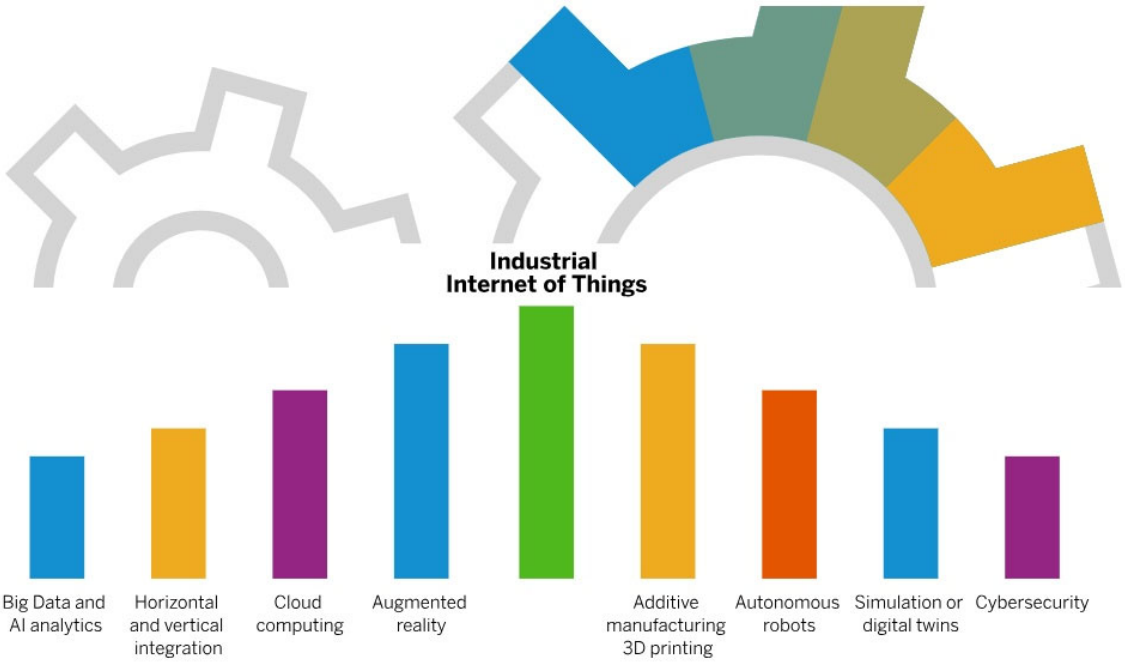
Para além da influência das redes sociais, o processo de digitalização foi acelerado por um acontecimento global sem precedentes. Em março de 2020, a Organização Mundial da Saúde declarou a COVID-19 como uma pandemia, levando vários países a adotarem medidas de confinamento e restrição à circulação de pessoas para controlar a propagação do vírus e mitigar os seus impactos nos sistemas de saúde. A limitação das atividades presenciais – como trabalhar, estudar ou realizar compras – gerou uma aceleração sem paralelo na adoção massiva das ferramentas digitais (Bambi et al., 2025).

De acordo com Laberge (2020), durante a pandemia, as empresas aceleraram a digitalização das suas operações externas e internas num período equivalente a três a

quatro anos, enquanto a incorporação de produtos digitais nos seus portfólios evoluiu ao ritmo correspondente a sete anos. Para estes autores, a necessidade de implementar o trabalho remoto, o ensino à distância e o comércio eletrónico, evidenciou o papel crítico das TIC, no geral, e das tecnologias digitais, em particular, na manutenção da conectividade e continuidade das atividades sociais e económicas em tempos de crise (2020).

Estas tecnologias têm contribuído de tal forma para o desenvolvimento das sociedades que são identificadas como a base da Quarta Revolução Industrial – ou Indústria 4.0 (Figura 3). Além disso, estas constituem motores de transformação social, permitindo a transição de interações predominantemente presenciais para conexões que ocorrem no espaço das tecnologias digitais.

Fig. 3 - Tecnologias da Indústria 4.0



Fonte: SAP, 2024

Apesar dos benefícios das TIC, surgem vários problemas e desafios com a sua utilização, em particular, no que se refere às ameaças à cibersegurança e às preocupações com a privacidade dos dados (Bélanger & Crossler, 2019). Como salientam Awati et al. (2025), "a digitalização dos dados, o uso crescente da internet de alta velocidade e a expansão da

rede global criaram novas oportunidades para o crime". Segundo estes autores, um número crescente de cibercriminosos tem explorado estas tecnologias "para conceber novos esquemas para obter acesso não autorizado a sistemas de informação pessoais, empresariais ou governamentais", com o objetivo de "roubar dinheiro, propriedade intelectual ou informações privadas". Acresce ainda que muitos dos cibercrimes praticados visam sistemas que controlam infraestruturas críticas, procurando provocar disrupção, caos e até pânico generalizado (Awati et al., 2025).

Numa sociedade progressivamente mais global e digital, onde as ameaças à segurança da informação e dos sistemas são constantes, a cibersegurança consolidou-se como uma componente essencial da economia digital, "pois o desenvolvimento bem-sucedido de tecnologias e plataformas digitais depende diretamente da proteção dos dados dos utilizadores, sistemas e transações" (Ashrapova e Apsilyam, 2025). De acordo com estes autores, embora as tecnologias emergentes como o IoT, a IA, a computação na nuvem e o *blockchain*, proporcionem novas oportunidades de negócio, introduzem igualmente múltiplas vulnerabilidades suscetíveis de serem exploradas por cibercriminosos, que podem afetar entidades públicas e privadas, cada vez mais dependentes das tecnologias digitais.

No atual contexto da Era Digital, a cibersegurança passou a fazer parte da estratégia das organizações, desde a cultura aos processos corporativos "pois qualquer violação na segurança pode minar a confiança nas tecnologias digitais, afetando negativamente o desenvolvimento de todo o ecossistema digital" (Ashrapova e Apsilyam, 2025). A cibersegurança passou, assim, a ser fundamental na proteção das infraestruturas críticas de ameaças externas e internas, garantindo a confidencialidade, integridade e disponibilidade dos dados.

1.2. Segurança da Informação: conceitos e evolução

Este ponto tem como objetivo efetuar um enquadramento conceptual, apresentando os principais termos utilizados no domínio da Segurança da Informação (SI), considerados neste estudo: cibersegurança, proteção de dados e a própria segurança da informação. Esta abordagem pretende distinguir os principais conceitos associados à SI e evidenciar

as relações existentes entre eles. Tal clarificação revela-se fundamental para assegurar a compreensão dos conceitos que serão utilizados ao longo desta investigação.

Atualmente, a SI, a proteção de dados e a cibersegurança são essenciais para as organizações, pois constituem os pilares para a confiança, a continuidade e a resiliência das suas atividades (Ceko, E. (2024). No entanto, embora muitas vezes os conceitos sejam utilizados como sinónimos, a segurança da informação, a proteção de dados e a cibersegurança têm focos e âmbitos diferentes, ainda que complementares.

Fig. 4 - segurança da informação, cibersegurança e proteção de dados

Fonte: elaboração própria, 2025

A SI é corresponde a um conceito mais abrangente, centrado na proteção dos sistemas informáticos contra a divulgação ou modificação indevida, o acesso não autorizado ou destruição de dados. O seu principal objetivo é assegurar a integridade, a confidencialidade e a disponibilidade da informação (G. Wang, & Wendy, 2019, citados por Taherdoost, H., 2022).

Neste sentido, Reid e van Niekerk (2014) aprofundam esta perspetiva ao defenderem que a SI é um processo contínuo, destinado a proteger a informação contra uma grande variedade de ameaças, assegurando a continuidade do negócio e a mitigação de riscos. Os autores sublinham igualmente que este processo implica a defesa da informação e dos sistemas de informação contra acessos não autorizados, divulgação, utilização, modificação, consulta e destruição indevida, reiterando que o principal objetivo da SI é

garantir a integridade, a confidencialidade e a disponibilidade da informação, independentemente da sua natureza física ou digital.

Os autores (2014) acrescentam ainda que a SI é definida como a "proteção da informação e dos seus elementos críticos, incluindo os sistemas e hardware que utilizam, armazenam e transmitem essa informação", contra as ameaças. Estas podem ter origens variadas, sendo as mais comuns os ataques cibernéticos ou físicos, os erros humanos – por omissão ou negligencia –, falhas de equipamentos ou software, bem como desastres naturais ou provocados pelo Homem (NIST, 2012).

A norma ISO/IEC 27000:2018 comprova a perspetiva apresentada pelos autores anteriormente referidos, ao definir um conjunto de requisitos no domínio da SI, centrados na preservação da confidencialidade, integridade e disponibilidade da informação, independentemente do seu formato (Makhija, A. (2021). Adicionalmente, a norma reconhece que outros aspetos – como a autenticidade, a responsabilidade e o não repúdio – podem igualmente integrar o âmbito da proteção da informação. A salvaguarda destes princípios fundamentais contribui de forma decisiva para a continuidade das operações, a resiliência dos sistemas e a sustentabilidade das organizações.

A relevância da SI reflete-se igualmente nas prioridades da UE. Nesse sentido, foi adotada em 2016 a primeira legislação europeia especificamente dedicada à Segurança das Redes e da Informação (SRI), conhecida como a Diretiva NIS, com o objetivo de estabelecer um elevado nível comum de segurança das redes e dos sistemas de informação na União. Posteriormente, em 2022, a UE aprovou a nova Diretiva SRI 2, que veio substituiu e reforçar o enquadramento anterior. Ambas as Diretivas serão analisadas no capítulo seguinte.

Deste modo, podemos assumir que a SI é baseada em processos, pessoas, tecnologia e procedimentos necessários para garantir os controlos de segurança da informação, para proteger sistemas e equipamentos, por forma a garantir o seu principal objetivo: integridade, confidencialidade e disponibilidade dos dados.

No contexto atual, um dos subdomínios mais críticos da SI é a proteção de dados, cuja importância aumentou com a TD e a crescente hiperconectividade entre diferentes sistemas de informação. A rápida progressão tecnológica nos últimos anos tem colocado novos desafios a este domínio, em particular devido ao aumento exponencial da partilha e recolha de dados, dentro e fora da UE.

À semelhança da SI, também a proteção de dados tem um âmbito alargado, com destaque para a proteção de dados pessoais e não pessoais. Os dados pessoais dizem respeito à "informação relativa a uma pessoa singular identificada ou identificável" (UE, 2016). A identificação pode ser de forma direta, através de um identificador específico – como um número único, por exemplo, o número do cartão de cidadão –, ou de forma indireta, com base numa ou mais características associadas à identidade física, económica, social ou cultural do indivíduo (UE, 2016).

Para além dos dados pessoais, importa considerar também os dados não pessoais, que englobam informação relevante para a segurança, operação e continuidade do negócio de uma organização. Este tipo de dados pode incluir, dependendo da organização, segredos comerciais, dados operacionais, relatórios internos, propriedade intelectual ou informação técnica sensível, cuja proteção é igualmente importante para a preservação dos interesses estratégicos e competitivos das organizações.

A relevância e complexidade associadas à proteção dos dados forçou a UE e os seus EM a adotarem medidas que estabelecem princípios, direitos e obrigações neste domínio, com o objetivo de salvaguardar o tratamento dos dados de forma lícita, transparente e segura, protegendo quer os direitos fundamentais dos indivíduos como os interesses estratégicos das organizações. Nesse sentido, destaca-se a nível jurídico e europeu, o Regulamento (UE) 2016/679, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecido por RGPD. A nível nacional, destaca-se a Lei n.º 58/2019, que assegura a execução do RGPD no ordenamento jurídico português (Assembleia da República - AR, 2019).

Apesar de não serem vinculativas, existem um conjunto de boas práticas, requisitos técnicos e orientações dedicadas à gestão da proteção de dados. Entre estas destaca-se a

norma ISO/IEC 27701:2019, orientada para a gestão da privacidade dos dados, e que tem como objetivo garantir as boas práticas à luz do RGPD, que entrou em vigor em 2018. De acordo com a *International Organization for Standardization e a International Electrotechnical Commission* (2019), a ISO/IEC 27701: 2019 especifica os requisitos e fornece orientações para estabelecer, implementar, manter e melhorar continuamente os Sistemas de Gestão da Informação de Privacidade, complementando as normas ISO/IEC 27001 e ISO/IEC 27002 no âmbito da proteção de dados.

Todavia, a proteção de dados não pode ser analisada isoladamente, uma vez que o avanço das tecnologias digitais tem criado simultaneamente novas oportunidades e introduzindo novos riscos associados à sua utilização. Segundo Lember, V., et al (2019), embora estas tecnologias tenham alterado significativamente a forma como os dados são produzidos e geridos, introduzem igualmente riscos e ameaças significativas, sobretudo no âmbito da segurança, privacidade e proteção da informação.

O aumento da hiperconectividade entre sistemas, a crescente dependência de infraestruturas digitais e a circulação exponencial de dados tornam os ambientes digitais mais vulneráveis a ameaças. Neste contexto, os desafios colocados por este novo paradigma digital ultrapassam o âmbito tradicional da proteção de dados e da segurança da informação, exigindo uma abordagem mais abrangente, estratégica e proativa. Torna-se, por isso, evidente que a proteção eficaz do ambiente digital exige mais do que a simples salvaguarda dos dados. Esta requer uma abordagem holística e integrada, centrada na cibersegurança e capaz de assegurar a resiliência dos sistemas, a continuidade das operações e a confiança no ciberespaço.

De acordo com Wang e Wendy (2019), a cibersegurança consiste num conjunto de práticas, processos e medidas destinadas a proteger indivíduos e organizações contra quebras de segurança, incidentes e ataques intencionais dirigidos aos sistemas e infraestruturas digitais. Complementando esta visão, Reid e van Niekerk (2014) alargam o âmbito do conceito ao sublinharem que a cibersegurança engloba a proteção da informação e das TIC, assegurando a confidencialidade, integridade e disponibilidade dos recursos no ciberespaço.

Na mesma linha de pensamento, Admass et. al (2024) corroboram com a perspetiva de Wang e Wendy (2019), ao definirem a cibersegurança como um processo contínuo de proteção e salvaguarda de sistemas informáticos, redes e dados contra ameaças cibernéticas, cuja ocorrência pode comprometer a confidencialidade, integridade e acessibilidade dos sistemas de informação.

Por sua vez, Andronache, A., & Althonayan, A. (2018), ampliam esta perspetiva ao considerarem a cibersegurança como um conceito mais abrangente, que integra não apenas a proteção de sistemas e dados, mas também ferramentas, processos, métodos e estratégias essenciais na proteção dos ativos digitais contra acessos não autorizados, perda ou violação da informação. Esta última perspetiva destaca a natureza multidimensional do conceito de cibersegurança, englobando não apenas questões técnicas, mas também componentes organizacionais e estratégicas, para a proteção eficaz do ambiente digital.

A mesma opinião tem o CNCS, que define cibersegurança:

> como o conjunto de medidas e ações necessárias para prevenir, monitorizar, detetar, analisar e corrigir redes e sistemas de informação face às ameaças a que estão expostos, tentando manter um estado de segurança desejado e garantir a confidencialidade, integridade, disponibilidade e não repúdio da informação (2025).

A crescente complexidade associada ao conceito de cibersegurança e a sua importância multidimensional, têm levado os Estados e entidades internacionais a repensar as suas estratégias de proteção do espaço digital. Neste contexto, a UE reconheceu a cibersegurança como um pilar fundamental na soberania digital, promovendo, na última década, um conjunto de atos legislativos destinados a reforçar a proteção dos sistemas, das redes e dos dados no seu espaço europeu.

Entre os diversos instrumentos legislativos desenvolvidos no domínio da cibersegurança, destaca-se a Diretiva NIS, que constituiu o primeiro quadro normativo europeu especificamente orientado para alcançar um elevado nível comum de segurança das redes

e dos sistemas de informação nos EM. No entanto, face à rápida evolução do contexto digital e ao aumento da complexidade e frequência das ameaças cibernéticas, a Diretiva NIS foi revogada e substituída pela Diretiva NIS2, que reforça e atualiza o enquadramento jurídico europeu, alargando o seu âmbito de aplicação e introduzindo requisitos mais exigentes em matéria de segurança e cooperação (UE, 2022b).

Em termos gerais, e tendo em conta as diferentes perspetivas, pode afirmar-se que a cibersegurança foca-se na proteção do ciberespaço contra ciberataques e outras ameaças digitais, enquanto a segurança da informação abrange a proteção da informação, num sentido mais amplo, independentemente da sua natureza ou suporte. Deste modo, o âmbito da cibersegurança está circunscrito ao espaço digital, enquanto que a SI tem um âmbito mais alargado, englobando a proteção dos dados e dos ativos tecnológicos.

No domínio da SI, importa mencionar o papel das normas internacionais, como as ISO da série ISO/IEC 2700x na promoção da conformidade das organizações com os atos legislativos europeus, bem como a legislação nacional aplicável, no domínio da SI, da proteção de dados e da cibersegurança. Estes referenciais desempenham um papel muito importante no apoio às organizações (privadas ou públicas) na implementação de medidas para garantir a SI como um todo, através da disponibilização de um conjunto de requisitos, regras e métodos, que traduzem os requisitos legais e regulatórios, facilitando a sua aplicação prática.

Deste modo, ambos os instrumentos são complementares: enquanto os atos legislativos (europeus e nacionais) definem o quadro jurídico, as normas internacionais operacionalizam a sua aplicação, garantindo níveis mais elevados de conformidade, segurança e proteção de dados.

1.3. A cibersegurança em contexto nacional

A crescente digitalização dos processos organizacionais, a ampla utilização das TIC e a interconexão de sistemas, serviços e dispositivos, tornam a SI, no geral, e a cibersegurança, em particular, elementos centrais na proteção e resiliência das organizações e do próprio Estado.

A crescente dependência das tecnologias digitais no suporte aos processos de negócio, na disponibilização de serviços e informação através de plataformas digitais, bem como a proliferação de equipamentos interconectados, aumentam consideravelmente a superfície de exposição a riscos e a ameaças no ciberespaço (CNCS, 2022a).

Perante este cenário de elevada vulnerabilidade digital, impõe-se uma abordagem nacional concertada, assente na consciencialização, no compromisso e na implementação de medidas de SI e cibersegurança nas organizações (públicas ou privadas). Só desta forma será possível garantir um ambiente seguro para o desenvolvimento de qualquer atividade económica ou social (CNCS, 2022a).

Em Portugal, a resposta a estes desafios materializa-se através de um conjunto de instrumentos e iniciativas estratégicas e legislativas que visam reforçar a proteção dos dados, redes e sistemas de informação e a resiliência digital. A construção de um quadro estratégico e regulatório em matéria de SI e cibersegurança tem se desenvolvido de forma gradual e de acordo com a evolução tecnológica e desafios emergentes no ciberespaço.

Para uma melhor compreensão da evolução do enquadramento nacional em matéria de SI e cibersegurança, apresentam-se nos parágrafos seguintes, por ordem cronológica, e sem pretender uma descrição exaustiva, os principais atos jurídicos, iniciativas e estratégias desenvolvidas em Portugal.

A Lei n.º 41/2004, de 18 de agosto, foi o primeiro ato jurídico nacional no âmbito do tratamento e proteção de dados pessoais e da privacidade. Esta lei transpôs para a ordem jurídica nacional a Diretiva n.º 2002/58/CE, no setor das comunicações eletrónicas, e estabelecia regras fundamentais sobre a segurança e a confidencialidade das comunicações, bem como obrigações dos prestadores de serviços em caso de violação de dados (AR, 2004).

A Lei n.º 46/2012, de 29 de agosto, transpõe a Diretiva n.º 2009/136/CE, na parte que altera a Diretiva n.º 2002/58/CE, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas, procedendo à primeira alteração à Lei n.º 41/2004 e à segunda alteração ao Decreto-Lei n.º 7/2004 (AR, 2012). Esta lei atualiza

e reforça a Lei nº 41/2004, adaptando-a novas exigências europeias e tecnológicas, sobretudo em matéria de notificação de incidentes, consentimento e segurança.

Em 2014, foi criado o Centro Nacional de Cibersegurança, dentro do Gabinete Nacional de Cibersegurança, pelo Decreto-Lei n.º 69/2014. Através do Decreto-Lei n.º 136/2017, o CNCS adquire a sua designação atual, sendo atribuída a este centro a competência de Autoridade Nacional de Cibersegurança, cujo "objetivo é contribuir para uma utilização livre, confiável e segura do ciberespaço de interessa nacional" (CNCS, 2025b).

Fig. 5 - Centro Nacional de Cibersegurança

Fonte: CNCS, 2025

Enquanto coordenador operacional e autoridade nacional responsável pela cibersegurança junto das entidades do Estado e das entidades privadas, o CNCS amplia o seu campo de ação, abrangendo não apenas entidades específicas, mas também a sociedade no seu todo. (CNCS, 2025b).

Com o objetivo de cumprir a sua missão, o CNCS promove um conjunto de iniciativas direcionadas aos cidadãos e organizações, com vista à sensibilização e formação especializada que fomente a adoção de comportamentos mais seguros e responsáveis no manuseamento das tecnologias e na navegação no espaço digital. Em paralelo, o CNCS dedica-se à produção e disseminação de alertas, orientações e boas práticas que visam reforçar a segurança e a responsabilidade na utilização das tecnologias digitais por parte dos indivíduos e organizações. Adicionalmente, o CNCS elabora e divulga

recomendações técnicas, bem como produz normativos e referenciais, especialmente concebidos para ajudar as organizações na implementação de medidas eficazes de cibersegurança (CNCS, 2025b). O CNCS dedica-se ainda à produção de conhecimento sobre o estado da cibersegurança nacional, definindo, entre outros aspetos, o nível nacional de alerta.

Através do seu serviço CERT.PT[46] (*Computer Emergency Response Team Portugal*), acreditado internacionalmente, e em estreita articulação com as demais entidades competentes, realiza a coordenação da resposta a incidentes que afetem o ciberespaço de interesse nacional. Este serviço visa melhorar a eficácia da reação a incidentes de cibersegurança em Portugal, facilitando a partilha de informação relevante e coordenando ações de mitigação e de resolução junto das diversas entidades implicadas, articulando com as restantes autoridades – nacionais e internacionais – em caso de incidentes (CNCS, 2025b). O CERT.PT é a equipa especializada responsável por prevenir, detetar, analisar e responder a incidentes de segurança informática (*Computer Security Incident Response Team* – CSIRT) em Portugal.

Complementando estas dimensões de atuação, o CNCS exerce ainda as competências de regulação e de supervisão para os diferentes setores de atividade económica, no seguimento da Lei n.º 46/2018, que estabelece o Regime Jurídico da Segurança do Ciberespaço.

No seguimento das iniciativas para o desenvolvimento nacional em matéria de cibersegurança, foi aprovada, em 2015, a primeira versão da Estratégia Nacional de Segurança do Ciberespaço (ENSC). Esta estratégia tinha como objetivo:

> aprofundar a segurança das redes e da informação, como forma de garantir a proteção e defesa das infraestruturas críticas e dos serviços vitais de informação, e potenciar uma utilização livre, segura e eficiente do ciberespaço por parte de

[46] CERT.PT: equipa de resposta a incidentes de segurança informática nacional, que funciona no CNCS e possui, entre outras, as seguintes competências: exercer a coordenação operacional na resposta a incidentes; monitorizar os incidentes com implicações a nível nacional; assegurar a cooperação com entidades públicas e privadas; e intervir na reação, análise e mitigação de incidentes;

todos os cidadãos, das empresas e das entidades públicas e privadas (Presidência do Conselho de Ministros – PCM, 2015).

A ENSC representou, assim, o primeiro passo na definição das políticas nacionais de cibersegurança, ao estabelecer as bases para a construção de um ecossistema digital mais seguro e resiliente. No entanto, a crescente evolução tecnológica, acompanhada pelo aumento de ameaças cada vez mais complexas, e a necessidade de alinhamento com o quadro jurídico europeu, tornou necessária a adoção de instrumentos jurídicos mais robustos e vinculativos.

É neste enquadramento que se insere a Lei n.º 46/2018, de 13 de agosto, que transpõe para a ordem jurídica interna a Diretiva NIS, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Esta lei aplica-se a entidades da administração pública, aos operadores de infraestruturas críticas, aos operadores de serviços essenciais, aos prestadores de serviços digitais, bem como quaisquer outras entidades que utilizem redes e sistemas de informação (AR, 2018).

Paralelamente ao reforço do enquadramento jurídico em matéria de cibersegurança promovido pela Lei n. 46/2018, tornou-se necessário assegurar a proteção de dados pessoais num contexto de crescente digitalização e interconexão de sistemas. Com a entrada em vigor do RGPD, a sua execução para a ordem jurídica nacional foi assegurada pela Lei nº 58/2019, de 8 de agosto, que adaptou o quadro jurídico português às disposições do regulamento e estabeleceu as regras aplicáveis ao tratamento de dados pessoais e à livre circulação desses dados, contribuindo para reforçar a confiança digital e complementar as medidas previstas no domínio da cibersegurança. Torna-se evidente que a proteção de dados pessoais e cibersegurança são dois conceitos indissociáveis na era digital.

Num ciberespaço caracterizado pela ausência de fronteiras definidas, a proteção destes dados enfrenta desafios constantes decorrentes do rápido avanço tecnológico, da proliferação de novas ameaças e da conectividade permanente. Neste contexto, a articulação entre medidas de proteção de dados e estratégias de cibersegurança revela-se

importante para salvaguardar a segurança da informação, a privacidade dos cidadãos e a confiança nas interações digitais (Alves, 2021, e Mohsin, 2022).

No seguimento da política legislativa, e após a primeira ENSC, foi aprovada, em 2019, a Estratégia Nacional de Segurança do Ciberespaço 2019-2023 (ENCS 2019-2023), como resposta à rápida evolução tecnológica, ao surgimento de novas ameaças e vulnerabilidades no espaço digital. Esta nova ENSC assenta em três eixos estratégicos: maximizar a resiliência, fomentar a inovação e criar e garantir recursos. A concretização destes três objetivos permitirá a Portugal tornar-se num País "mais seguro e próspero, através de uma ação inovadora, inclusiva e resiliente, que preserve os valores fundamentais do Estado de Direito democrático e garanta o regular funcionamento das instituições face à evolução digital da sociedade" (PCM, 2019).

Com o propósito de afirmar Portugal como um País próspero e inovador, capaz de utilizar as tecnologias digitais como catalisador para a melhoria da qualidade de vida da população e do reforço da competitividade económica, foi aprovada em 2024 a Estratégia Digital Nacional (EDN) para o digital até 2030.

Fig. 6 - Princípios orientadores da Estratégia Digital Nacional

Fonte: EDN, 2024-2030

A EDN e a cibersegurança estão interligadas na medida em que a EDN reconhece, no seu quarto princípio orientador, que a segurança e proteção de dados e de sistemas são fundamentais para a adoção confiável e segura das tecnologias digitais (PCM, 2024). Neste sentido, a EDN pretende implementar "medidas de cibersegurança robustas para proteção das infraestruturas críticas e dos dados contra ameaças e ataques cibernéticos", "políticas robustas de proteção e segurança de dados para construir a confiança dos cidadãos no uso das novas tecnologias" e "adotar políticas de monitorização contínua para avaliar o desempenho da infraestrutura e permitir melhorias e ajustes rápidos" (PCM, 2024).

Durante a realização deste estudo, foi aprovada a Lei n.º 59/2025, de 22 de outubro, que autoriza o Governo a transpor a Diretiva (UE) 2022/2555, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União (AR, 2025). Este novo regime jurídico impõe às entidades públicas e privadas, pertencentes a setores considerados críticos – como a energia, transportes, banca, saúde, infraestruturas digitais, administração pública (setores essenciais); bem como a gestão de resíduos, indústria alimentar, produtos químicos, serviços postais (setores importantes) – a adoção de medidas rigorosas de gestão dos riscos e resposta a incidentes. Pretende-se com esta nova legislação fortalecer a resiliência digital e promover uma cultura de segurança mais robusta e transversal em Portugal.

Contudo, atendendo à fase em que o estudo se encontrava, não foi possível incluir a respetiva análise, em particular no que respeita à concretização nacional das obrigações previstas pela NIS2. Posteriormente, no capítulo seguinte, será aprofundado o conjunto de aspetos fundamentais que são abrangidos pela Diretiva NIS2, desde a sua base legal até às suas exigências técnicas, processuais e operacionais.

À luz do enquadramento apresentado, este conjunto de instrumentos demonstra o compromisso nacional na construção de um ciberespaço mais seguro, resiliente e confiável. A articulação entre a ENCS, as obrigações legais e a atuação do CNCS, contribui para promover uma cultura de cibersegurança nas organizações, proteção de dados e para assegurar a resiliência dos sistemas de rede e informação das entidades essenciais e importantes.

1.4. A cibersegurança em contexto europeu

A progressiva TD da economia e da sociedade europeias transformou a cibersegurança num pilar estratégico, fundamental para a proteção dos cidadãos, das organizações e das infraestruturas críticas.

Devido ao crescimento exponencial das ameaças no espaço digital e à sua complexidade, a UE tem vindo a desenvolver um conjunto de atos legislativos com o objetivo de garantir um elevado nível comum de segurança das redes e dos sistemas de informação em todos os EM.

Para uma melhor compreensão deste quadro normativo, será efetuada uma análise cronológica, sem pretender uma descrição exaustiva, dos principais Regulamentos, Diretivas e Estratégias Europeias, que permitirá entender a progressiva consolidação da cibersegurança no espaço da União.

No contexto da UE, a atividade legislativa relacionada com o ciberespaço tem vindo a intensificar-se de forma contínua desde a adoção, em 1994, do primeiro Plano de Ação para a Sociedade da Informação, pela UE (CNCS, 2020a). No entanto, os primeiros instrumentos legislativos relacionados com este tema datam do final da década 90, e início dos anos 2000, e centravam-se, principalmente, na proteção de dados pessoais e comunicações eletrónicas (UE, 2002a). Posteriormente, e ainda que de forma gradual, na última década o foco da UE evoluiu para a construção de um quadro jurídico harmonizado e eficaz que responda aos desafios colocados pelas ameaças digitais em constante mudança, abrangendo desde produtos e serviços digitais, até à resiliência operacional e resposta a incidentes de grande escala.

A evolução legislativa europeia nesta área teve início em 1995 com a adoção da Diretiva 95/46/CE, de 24 de outubro, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Esta Diretiva teve um papel fundamental no desenvolvimento da segurança digital no espaço europeu (apesar de não ser uma norma de cibersegurança), pois estabeleceu princípios e regras para a recolha, tratamento e circulação de dados pessoais.

Em 2001, a UE, através da Comunicação 2001/0298, decide elaborar uma Estratégia Global de Segurança das Redes Eletrónicas, com vista a melhorar a segurança das redes e dos sistemas de informação, a proteção de dados e o combate à cibercriminalidade. Apesar do documento estar focado nas comunicações eletrónicas, este já demonstrava a preocupação com a segurança da informação ao pretender garantir a disponibilidade, autenticidade, integridade e confidencialidade dos dados armazenados ou transmitidos (UE, 2001).

Posteriormente, em 2002, a UE aprovou a Diretiva 2002/21/CE, de 7 de março, relativa a um quadro regulamentar comum para as redes e serviços de comunicações eletrónicas, e a Diretiva 2002/58/CE, de 12 de julho, relativa ao tratamento de dados pessoais e à proteção da privacidade no sector das comunicações eletrónicas. Estas Diretivas faziam parte do "pacote de telecomunicações", um conjunto de iniciativas da UE que acompanharam a abertura do mercado interno das telecomunicações à concorrência, introduzindo obrigações de segurança e integridade das redes e serviços de comunicações eletrónicas e de proteção de dados pessoais e privacidade.

O desenvolvimento europeu no domínio da segurança digital não se limitou à aprovação de Diretivas setoriais, tendo a UE reconhecido a relevância de adotar medidas que reforçassem a segurança das redes e dos sistemas de informação, expandindo o seu âmbito de atuação para além do setor das telecomunicações. A importância da cibersegurança na agenda política da UE levou, assim, à aprovação em 2004, do Regulamento (CE) n.°460/2004, de 10 de março, que criou a Agência Europeia para a Segurança das Redes e da Informação (*European Union Agency for Cybersecurity* – ENISA). Esta agência tem como objetivo garantir um "nível de segurança das redes e da informação elevado e eficaz e com vista a desenvolver uma cultura de segurança das redes e da informação em benefício dos cidadãos, dos consumidores e das organizações", contribuindo para o normal funcionamento do mercado interno (UE, 2004).

Para além de assegurar um elevado nível de segurança, a ENISA presta igualmente apoio técnico e aconselhamento à Comissão Europeia e aos EM, promovendo e facilitando a cooperação entre os diferentes intervenientes dos setores público e privado, com o

objetivo de reforçar a segurança das redes e dos sistemas de informação em toda a UE (UE, 2004).

Posteriormente, em 2013, a UE apresentou a sua primeira Estratégia para a cibersegurança, intitulada um "ciberespaço aberto, seguro e protegido" (UE, 2013a). Esta estratégia tinha como principal objetivo estabelecer e financiar uma rede de centros nacionais de excelência no combate à cibercriminalidade, promovendo a formação especializada e o desenvolvimento de capacidades no domínio da cibersegurança. Esta estratégia assentava em cinco prioridades:

- Alcançar a resiliência cibernética;
- Redução drástica da cibercriminalidade;
- Desenvolver a política e as capacidades de defesa cibernética relacionadas com a política comum de segurança e defesa;
- Desenvolver os recursos industriais e tecnológicos para a cibersegurança;
- Estabelecer uma política internacional coerente em matéria de ciberespaço para a Europa e promover os valores fundamentais da UE.

Desta estratégia nasce também a primeira proposta para a Segurança das Redes e da Informação, que viria a ser aprovada em 2016.

No seguimento da consolidação das políticas europeias na área da segurança da informação e cibersegurança, tornou-se evidente que a proteção de dados pessoais e da privacidade constitui um elemento crucial para a construção de um ciberespaço seguro. A crescente digitalização da sociedade e da economia europeias revelou a necessidade da UE atualizar o enquadramento jurídico existente em matéria de proteção de dados e da privacidade. Neste sentido, para garantir os direitos fundamentais dos cidadãos, a UE aprovou em 2016 o Regulamento (UE) 2016/679, de 27 de abril, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Este regulamento reforça as normas de segurança e responsabilidades no tratamento de dados pessoais.

Um dos principais objetivos do RGPD é a criação de um quadro jurídico uniforme para a proteção das pessoas singulares no tratamento de dados pessoais, garantindo que esse

tratamento ocorre de forma lícita, leal e transparente. Este regulamento pretende igualmente salvaguardar os direitos e as liberdades fundamentais dos indivíduos, com especial destaque para o direito à proteção de dados pessoais, protegendo a sua livre circulação entre os EM e evitando que esta não seja restringida por motivos relacionados com a proteção desses dados, promovendo, assim, tanto a confiança no ambiente digital como o funcionamento do mercado único (UE, 2016a).

Este regulamento introduziu não apenas normas rigorosas para a proteção de dados e da privacidade, como também impôs a todas as organizações a adoção de práticas de cibersegurança adequadas, por forma a garantirem a confidencialidade, a integridade e a disponibilidade da informação, prevenindo acessos não autorizados, alterações indevidas, destruição ou divulgação ilícita de dados. Esta abordagem visa proteger os dados pessoais de violações que comprometam os direitos fundamentais dos cidadãos, como a privacidade (UE, 2016a).

Dada a criticidade da proteção de dados pessoais e o seu tratamento, o RGPD introduz ainda um regime sancionatório rigoroso, contribuindo para a harmonização europeia da aplicação das normas e para o reforço da responsabilização das organizações no tratamento de dados pessoais.

Embora o RGPD constitua um passo fundamental na proteção de dados pessoais e na salvaguarda da privacidade dos cidadãos no espaço digital, a crescente complexidade e interdependência das infraestruturas digitais europeias revelou ser necessário uma abordagem mais ampla e complementar no domínio da cibersegurança. Esta abordagem irá permitir garantir a resiliência, a integridade e a segurança das redes e dos sistemas de informação que dão suporte aos objetivos do RGPD: proteção de dados pessoais e salvaguarda da privacidade dos cidadãos (UE, 2016a).

Foi neste contexto que a UE aprovou em 2016 a Diretiva (UE) 2016/1148, de 6 de julho, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União. Esta Diretiva foi a primeira legislação europeia especificamente dedicada à segurança das redes e da informação, com o objetivo de reforçar a capacidade coletiva de prevenção, deteção e resposta a incidentes

cibernéticos, melhorando a resiliência de todos os seus EM. A NIS veio reforçar as competências das autoridades europeias de cibersegurança a nível nacional, aumentar a coordenação entre EM e assegurar a continuidade dos serviços que permitem o bom funcionamento da economia e da sociedade, altamente dependentes das TIC (UE, 20).

Esta Diretiva não veio apenas reforçar a política europeia para a segurança das redes e dos sistemas de informação, veio também introduzir um conjunto de disposições que definiram os pilares da cibersegurança em toda a União. Entre os principais requisitos evidencia-se a identificação de operadores de serviços essenciais – cuja atividade é fundamental para a manutenção de atividades sociais e económicas críticas, nomeadamente os setores da energia, os transportes, a saúde ou o setor bancário – e os fornecedores de serviços digitais – incluindo plataformas de comércio eletrónico, motores de busca e serviços de computação em nuvem –, a notificação obrigatória de incidentes com impacto significativo nas atividades prestadas por estas entidades, e a introdução de sanções proporcionais e dissuasoras no caso de haver incumprimento das obrigações estabelecidas (UE, 2016b).

Acresce ainda a necessidade de cada EM designar uma ou mais autoridades responsáveis pela supervisão da aplicação da NIS, e a criação de equipas de resposta a incidentes de segurança informática (CSIRT), também conhecidas por equipas de resposta a emergências informáticas (CERT) (UE, 2016b).

Em conjunto, estas medidas representam um avanço significativo no reforço da resiliência cibernética da União, promovendo a harmonização das práticas nacionais e contribuindo para o aumento da confiança no mercado digital europeu.

No entanto, apesar dos avanços significativos introduzidos pela Diretiva NIS, a rápida transformação digital e interligação das sociedades, o aumento das ameaças e sua complexidade e a crescente dependência digital das economias europeias, tornaram evidente a necessidade da UE adotar medidas complementares para reforçar ainda mais a política europeia de cibersegurança.

Neste contexto, a EU aprovou, em 2019, o Regulamento (UE) 2019/881, de 17 de abril, relativo à ENISA e à certificação da cibersegurança das TIC. Também conhecido como o Regulamento de Cibersegurança, este revoga o Regulamento (UE) n.º 526/2013 e tem como principais objetivos reforçar o mandato e ampliar as competências da ENISA, melhorar a harmonização das práticas de cibersegurança na União, estabelecer um quadro europeu de certificação de cibersegurança das TIC e contribuir para o reforço da resiliência e da capacidade de reposta dos EM a incidentes e ameaças cibernéticas (UE, 2019).

Pretende-se, com este regulamento, reforçar o apoio permanente e alargado aos EM e às instituições e entidades da UE na prevenção e resposta a incidentes de cibersegurança, aumentar o nível geral de segurança da informação no mercado interno europeu, promover um elevado nível comum de segurança das redes e dos sistemas de informação, e garantir um ambiente digital mais seguro para os cidadãos, empresas e instituições europeias.

À medida que o esforço europeu para a cibersegurança se consolidava, também a intensificação da digitalização e interligação das economias ampliavam os riscos associados às tecnologias digitais, tornando a sociedade, no geral, e o sistema financeiro, em particular, mais vulneráveis a ciberameaças. A dependência cada vez maior de TIC por parte das entidades do setor financeiro, expõe vulnerabilidades com potencial impacto sistémico no espaço europeu, exigindo uma resposta normativa mais abrangente e adaptada às necessidades deste domínio.

Neste contexto, a UE aprovou, em 2022, o Regulamento (UE) 2022/2554, de 14 de dezembro, relativo à resiliência operacional digital do setor financeiro, também conhecido como DORA – *Digital Operational Resilience Act*. Face ao aumento significativo de ataques cibernéticos, aliado a uma utilização crescente de serviços digitais externos, este regulamento pretende "harmonizar tipologias de entidades e Estados-Membros e aumentar a exigência dos requisitos de resiliência operacional digital, para robustecer o sistema financeiro" (Banco de Portugal, 2025).

A UE pretende com este regulamento estabelecer um quadro jurídico e diretamente aplicável em todos os EM, para aumentar a resiliência digital de todas as entidades do setor financeiro, independentemente da sua dimensão ou localização.

O DORA assenta em cinco pilares fundamentais – gestão de risco das TIC, notificações e reporte de incidentes, realização de testes de resiliência, partilha de dados e gestão de risco associado a prestadores de serviços TIC – que visam assegurar uma abordagem integrada e coerente à resiliência digital do setor financeiro (Vieira de Almeida, 2023). Estes estabelecem as bases para que as entidades abrangidas pelo regulamento possam proteger, detetar, conter, recuperar e reparar as suas capacidades afetadas por incidentes relacionados com as TIC (UE, 2022a).

O regulamento prevê ainda um regime harmonizado de sanções administrativas e medidas corretivas proporcionadas, eficazes e dissuasoras, com o objetivo de assegurar o cumprimento das suas disposições e garantir a eficácia do quadro europeu de resiliência operacional digital no setor financeiro (UE, 2022a).

Paralelamente ao reforço da resiliência operacional digital no setor financeiro, a UE reconheceu a necessidade de estabelecer um quadro jurídico transversal e aplicável a todos os setores essenciais da economia e não apenas no financeiro. Em simultâneo com a crescente sofisticação das ameaças cibernéticas, com a expansão do uso das tecnologias digitais em todos os setores da economia e com a necessidade de ultrapassar as limitações identificadas na Diretiva NIS (será discutido no capítulo seguinte), a UE aprovou, em 2022, a Diretiva (EU) 2022/20555, de 14 de dezembro, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União.

A Diretiva NIS2 veio revogar e substituir a Diretiva NIS, atualizando o quadro europeu de cibersegurança, através da introdução de medidas importantes para dar resposta ao aumento e complexidade das ameaças cibernéticas e às fragilidades identificadas na implementação da sua antecessora (UE, 2022b).

Com a adoção da NIS2, a UE procura responder aos desafios emergentes no espaço digital e ultrapassar as limitações identificadas na NIS. Pretende igualmente reforçar a

harmonização do quadro jurídico europeu de cibersegurança, decorrente da aplicação desigual da Diretiva anterior. Desta forma, a UE ambiciona assegurar uma implementação mais coerente e uniforme das medidas previstas entre os EM (UE, 2022b).

Complementarmente à abordagem estabelecida pela Diretiva NIS2 no domínio da cibersegurança, a UE aprovou, no mesmo ano, a Diretiva (UE) 2022/2557, de 13 de dezembro, relativa à resiliência das entidades críticas[47].

Também conhecida por Diretiva CER (*Critical Entities Resilience*), esta tem como objetivo reforçar a resiliência das entidades críticas face a riscos "naturais e de origem humana pertinentes, suscetíveis de provocar um incidente, incluindo os de natureza intersectorial ou transfronteiriça, acidentes, catástrofes naturais, emergências de saúde pública e ameaças híbridas e outras ameaças antagónicas, incluindo infrações terroristas" (UE, 2022c), que possam afetar a prestação de serviços essenciais.

Se por um lado a NIS2 foca-se na cibersegurança das redes e dos sistemas de informação e incide especificamente sobre ciberameaças e incidentes relacionados com as tecnologias digitais em setores essenciais e importantes, por outro, a Diretiva CER estabelece medidas destinadas a reforçar a resiliência física, estrutural e organizacional das entidades críticas, de modo a garantir que estas possam prestar serviços essenciais em caso de perturbações.

A Diretiva (UE) 2022/2557 prevê ainda um regime de sanções para as entidades que violem os seus requisitos, incumbindo aos EM a responsabilidade de definir as regras relativas às sanções aplicáveis decorrentes da violação das disposições nacionais adotadas nos termos da presente Diretiva, e de adotar todas as medidas necessárias para assegurar sua aplicação efetiva. As sanções previstas devem ser efetivas, proporcionadas e dissuasivas.

No seguimento destas iniciativas legislativas, e reconhecendo a necessidade de reforçar a segurança e resiliência digital ao nível dos produtos e componentes tecnológicos que sustentam o ecossistema digital europeu, a UE aprovou o Regulamento (UE) 2024/2847,

[47] Ver Anexo Setores, subsetores e categorias de entidades, do Regulamento (UE) 2022/2557 do Parlamento Europeu e do Conselho.

de 23 de outubro, relativo aos requisitos horizontais de cibersegurança dos produtos digitais. Também conhecido como o Regulamento de Ciber-Resiliência (*Cyber Resilience Act* - CRA), este diploma tem como objetivo mitigar as vulnerabilidades associadas a produtos com elementos digitais, estabelecendo requisitos essenciais para o seu desenvolvimento seguro. O CRA visa assegurar que apenas os produtos de *hardware* e *software* com um nível reduzido de vulnerabilidades sejam disponibilizados no mercado europeu e que os fabricantes integrem a segurança como um princípio fundamental ao longo de todo o ciclo de vida do produto, desde a conceção até à sua utilização e manutenção (PLMJ, 2024).

Este regulamento abrange uma ampla variedade de produtos com elementos digitais, incluindo os componentes *hardware*, *software* e soluções integradas, desde que possuam conetividade, direta ou indireta, com dispositivos ou redes. Entre estes incluem-se, nomeadamente, *smartphones*, *tablets*, dispositivos IOT, equipamentos de rede e segurança (como *firewalls* e *routers*), e dispositivos de computação periférica (ML, 2024).

O CRA prevê ainda um regime de sanções para as entidades que violem os seus requisitos, cabendo a responsabilidade pela sua aplicação às autoridades nacionais de fiscalização. Com este novo ato legislativo, a UE dá mais um passo no sentido de construir um mercado único digital mais seguro, coerente e resiliente, protegendo utilizadores, empresas, instituições e infraestruturas críticas contra vulnerabilidades e ameaças digitais.

Na sequência do esforço europeu para melhorar a segurança e resiliência da sua economia e sociedade, cada vez mais digitalizadas, a UE aprovou, em 2024, o Regulamento (UE) 2025/38, de 19 de dezembro, que cria medidas destinadas a reforçar a solidariedade e as capacidades da União para detetar, preparar e dar resposta a ciberameaças e incidentes de cibersegurança.

Também conhecido como o Regulamento de Cibersolidariedade (*Cyber Solidarity Act* – CSA), este regulamento tem como principal finalidade criar um quadro comum de resposta a ciberameaças, garantindo que os EM trabalham em conjunto para proteger as redes e sistemas de informação essenciais. Neste contexto, este ato legislativo tem como

principais objetivos reforçar a deteção precoce de ciberameaças, melhorar a coordenação da resposta a ciberameaças entre os EM, criar respostas mais eficazes a ataques de grande escala e tornar as infraestruturas digitais mais resilientes (UE, 2025d).

Para cumprir os seus objetivos, o regulamento prevê três medidas essenciais, nomeadamente, a criação de um Sistema Europeu de Alerta em matéria de Cibersegurança, a criação de um Mecanismo de Emergência em matéria de Cibersegurança e de uma Reserva de Cibersegurança da UE, e a criação de um Mecanismo Europeu de Análise de Incidentes de Cibersegurança (UE, 2025d). O cumprimento destes objetivos vai permitir uma maior cooperação e partilha de informações entre os EM, uma reação mais rápida e eficaz a incidentes de cibersegurança em grande escala, reduzir os riscos de ataques e do seu impacto nas infraestruturas críticas, e reforçar a confiança nos sistemas digitais (UE, 2025d).

O CSA centra-se menos nas obrigações individuais das entidades e mais no reforço da capacidade coletiva da UE para prevenir, detetar e responder a incidentes cibernéticos de grande escala, promovendo uma cooperação transfronteiriça e a solidariedade digital europeia.

A consolidação do quadro europeu de cibersegurança é o resultado da evolução legislativa progressiva, fruto da crescente importância da proteção do ciberespaço para a segurança, a economia e os direitos fundamentais.

Em conjunto, estes instrumentos legislativos refletem a estratégia integrada da UE, orientada para a proteção dos cidadãos e das organizações, para reforçar a resiliência das infraestruturas críticas, para promover a confiança no mercado único digital e para garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União.

1.5. Evolução das ciberameaças e ciberataques

A crescente dependência das TIC, principalmente das tecnologias digitais, tornou-se um elemento estrutural das sociedades e economias contemporâneas, promovendo a interligação entre instituições públicas, empresas e cidadãos a nível intersectorial e

transfronteiriço. Este processo de TD tem sido acompanhado por uma evolução constante da frequência, complexidade e do impacto dos ciberataques, transformando-os numa das principais ameaças à segurança digital, à estabilidade económica e à proteção dos direitos fundamentais dos cidadãos europeus, designadamente os direitos à privacidade, à proteção de dados pessoais, à segurança das redes e sistemas de informação e ao pleno exercício das liberdades fundamentais no ciberespaço (UE, 2024a e UE, 2025d).

Neste subcapítulo, faz-se a análise dos principais tipos de ciberameaças e ciberataques, e da sua evolução nos últimos anos, quer no contexto europeu como nacional, com especial destaque para os incidentes que tiveram maior impacto. Esta caracterização constitui um passo importante para compreender a situação atual relativamente às ciberameaças que, sendo novas ou recorrentes, têm maior ou menor impacto no ciberespaço da União e em Portugal.

1.5.1. Contexto nacional

Em Portugal, o panorama da cibersegurança tem se revelado cada vez mais complexo e exigente, refletindo o aumento exponencial dos ataques cibernéticos, cada vez mais sofisticados. Este contexto resulta da progressiva digitalização dos setores público e privado, aliada à hiperconectividade entre infraestruturas críticas e serviços essenciais. Este cenário, juntamente com multiplicação dos vetores de ataque e com a diversificação dos atores envolvidos, tem contribuído para o alargamento da área de ciberameaças, expondo as vulnerabilidades e os respetivos riscos para a economia, segurança nacional e para os direitos fundamentais dos cidadãos (CNCS, 2025c).

De acordo com o CNCS, o CERT.PT tem registado nos últimos anos um elevado número de incidentes no País. Entre as principais tipologias de incidentes mais frequentes em 2024 destacam-se as campanhas de *phishing e smishing*, diversas formas de engenharia social, o *ransomware,* a exploração de vulnerabilidades, os ataques de negação de serviços distribuída (*Distributed Denial of Service* – DDoS) e o a violação de contas (Figura 7).

Fig. 7 - Principais ciberameaças mais relevantes em Portugal 2024 – TOP 5[48]

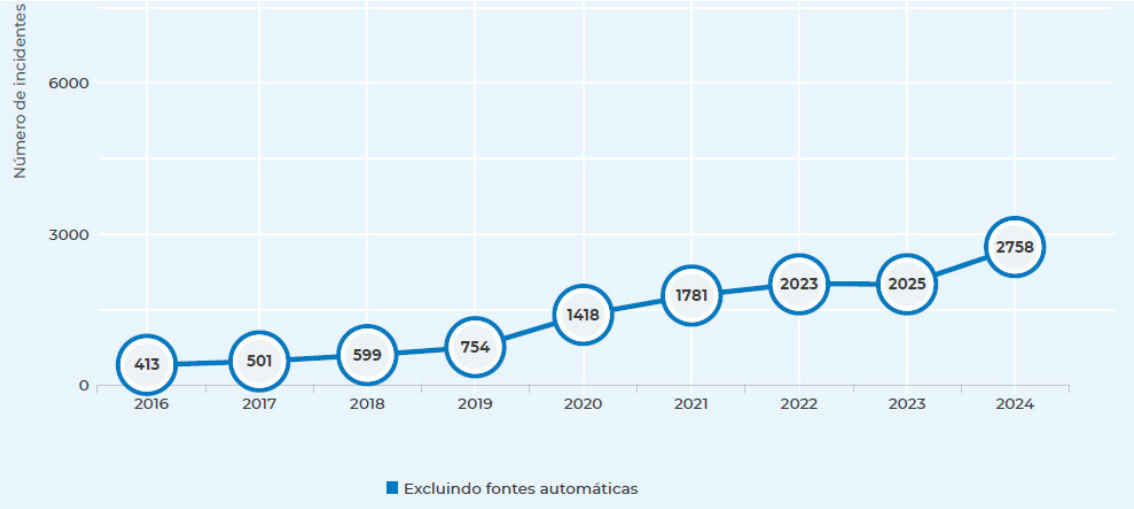
Fonte: CNCS, Relatórios 2020-2025

Os Relatórios de Cibersegurança em Portugal – Riscos e Conflitos, do CNCS (doravante designados por Relatórios 2020-2025) identificaram como principais ciberameaças em 2024 o *phishing* e *smishing*, a engenharia social e burlas *online* e o *ransomware*. Este relatório identificou ainda a exploração de vulnerabilidades, os ataques DDoS, a violação de contas, o código malicioso, a exfiltração de dados, a ciberespionagem e a tentativa de *login* como ciberameaças mais frequentes. Estas ameaças são, em grande parte, a consequência da intensificação da digitalização das atividades económicas e sociais e da consequente exposição acrescida dos sistemas de informação e suas vulnerabilidades, que resultam num risco relevante para a segurança das redes e dos sistemas de informação.

De acordo com o CERT.PT, em 2024 registou-se um aumento de 36% no número de incidentes no espaço digital nacional face ao ano de 2023 (Figura 8). Este crescimento enquadra-se na tendência de subida contínua observada desde 2016, que corresponde a um incremento médio anual de cerca de 29%. Esta trajetória foi interrompida em 2020, ano em que se verificou um aumento excecional de 88%, associado aos efeitos da pandemia da Covid-19, e em 2022, período no qual se registou um acréscimo residual de 0.1% relativamente ao ano anterior. Ainda em 2024, verificou-se que 78% dos incidentes envolveram entidades privadas, confirmando a predominância deste setor nos registos reportados pelo CNCS desde 2020 (CNCS, Relatórios 2020-2025).

[48] Ordenação estabelecida com base em cálculo que considera a redundância entre fontes, a abrangência de cada fonte e o potencial impacto de cada ciberameaça.

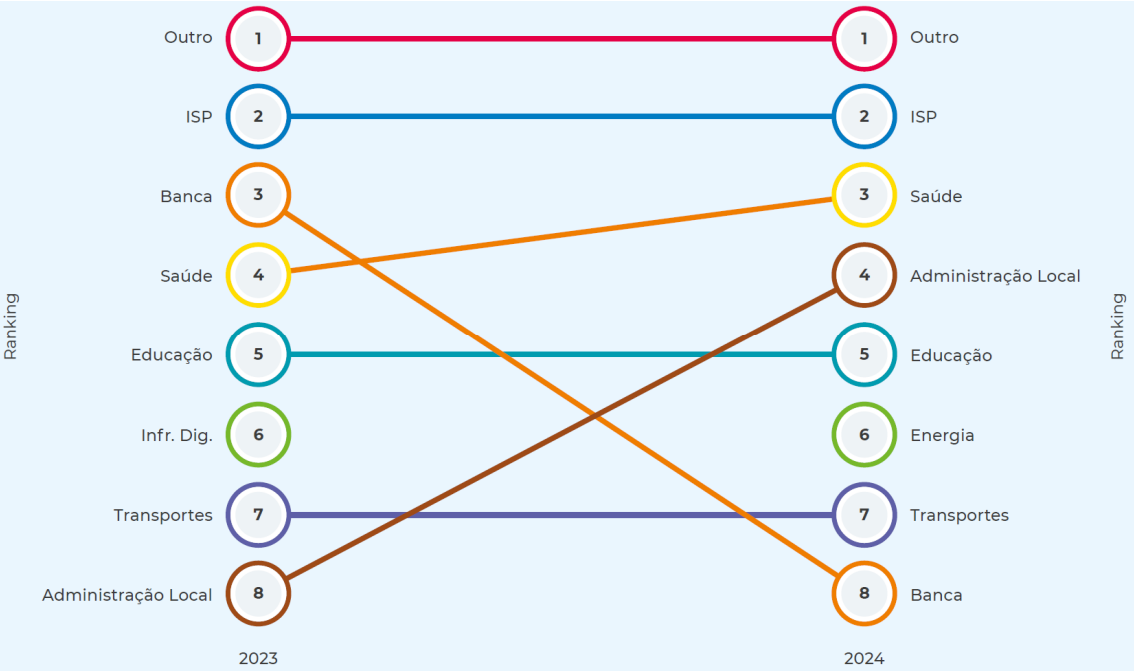
Fig. 8 - Número de incidentes registados pelo CERT.PT



Fonte: CNCS, Relatórios 2020-2025

Do ponto de vista setorial, os Relatórios 2020-2025 destacam que o setor dos prestadores de serviços de internet (*Internet Service Providers* – ISP) manteve o maior volume de incidentes em 2024, apesar de uma redução de 53% face ao ano anterior (Figura 9).

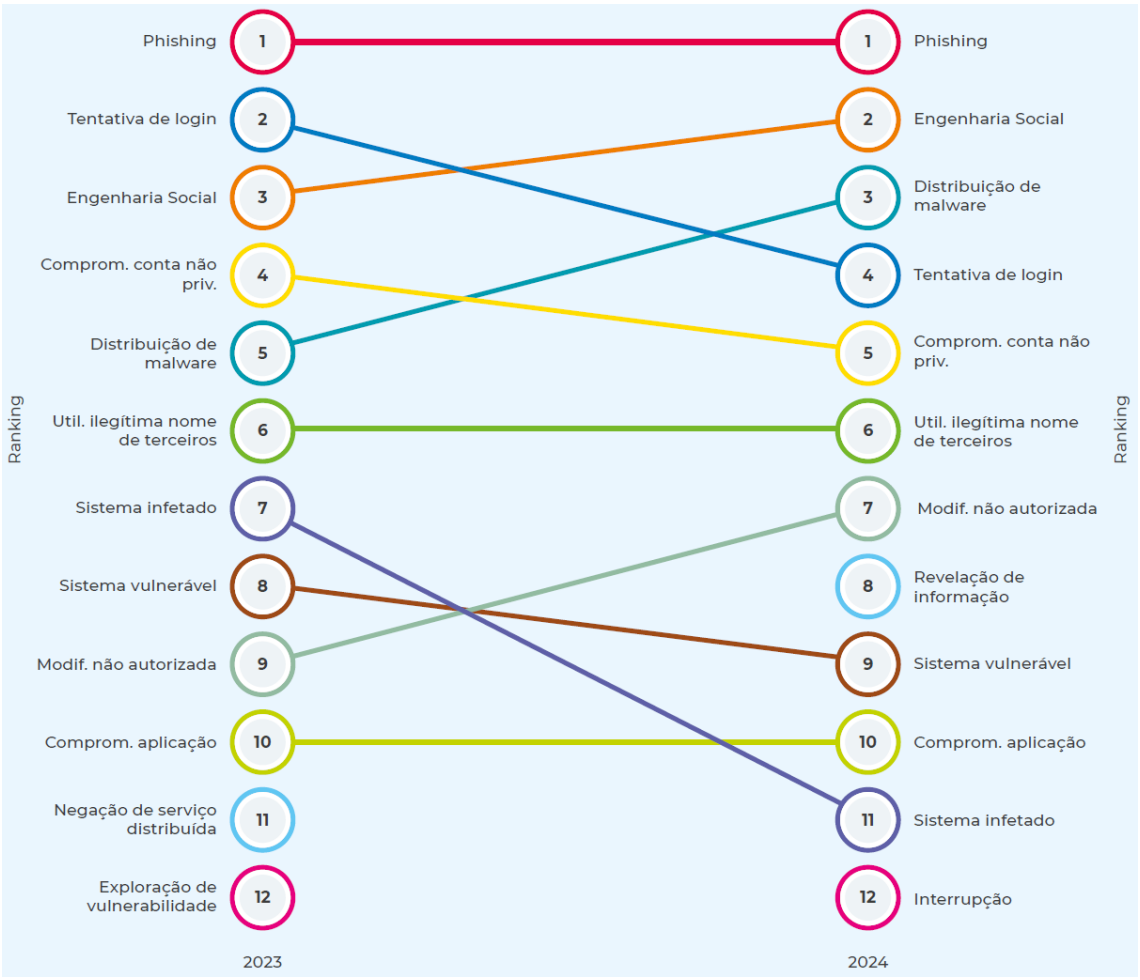
Fig. 9 - Variação no ranking de setor/área governativa com mais incidentes registados, relativamente a 2023 e 2024



Fonte: CNCS, Relatórios 2020-2025

No que se refere à tipologia de incidentes, o *phishing* representou 28,67% do total de ocorrências registadas pelo CERT.PT em 2024, correspondendo a um aumento de 13% face a 2023 (Figura 10).

Fig. 10 - Variação no ranking de tipologia com mais incidentes registados, relativamente a 2023 e 2024



Fonte: CNCS, Relatórios 2020-2025

A engenharia social foi a segunda tipologia mais prevalente, com 27,97% incidentes registados. Dentro desta categoria, as técnicas de *vishing*, *CEO fraud*, "Olá Pai…Olá Mãe" e *sextortion* registaram aumentos significativos de 136%, 164%, 326% e 158% respetivamente. Estas tendências confirmam a predominância persistente, desde 2018, das categorias de *phishing*, engenharia social e distribuição de malware no ciberespaço nacional (CNCS, Relatórios 2020-2025).Os Relatórios 2020-2025 destacam ainda que a

distribuição de *malware* duplicou em 2024, relativamente a 2023, representando 8,99% dos incidentes registado. Verificou-se, também, um aumento de 37% nos casos de violação de contas e 58% nas situações de modificação não autorizada. Em sentido inverso, observaram-se reduções significativas nas tentativas de login (-42%), bem como nos incidentes relacionados com sistemas infetados (-66%) e sistemas vulneráveis (-42%).

A análise da distribuição dos incidentes por setores revela uma certa heterogeneidade, observando-se que tipologias como engenharia social, o *phishing* e sistemas vulneráveis afetam transversalmente a maioria dos setores. Em contrataste, incidentes como sabotagem, perda de dados ou negação de serviço incidem em áreas específicas, nomeadamente administração local e regional, transportes, economia e ISP. Durante o ano de 2024 a distribuição de *malware* incidiu de forma particular sobre os setores da educação, ciência e administração local, enquanto que a engenharia social e *phishing* registaram maior incidência nos setores da saúde, energia e ensino superior, mantendo-se a banca entre os mais visados. Por fim, as tentativas de *login* concentraram-se sobretudo nos setores dos ISP e das infraestruturas digitais (CNCS, Relatórios 2020-2025).

Um dos impactos mais relevantes dos incidentes de cibersegurança manifesta-se ao nível da proteção de dados, uma vez que estes eventos podem representar riscos para os direitos e liberdades dos titulares. Em 2024, a Comissão Nacional de Proteção de Dados (CNPD) registou 331 notificações de violação de dados pessoais, o que representa uma inversão da tendência de crescimento observada desde 2019 (Figura 11).

Fig. 11 - Número de notificações à CNPD de violação de daados pessoais, de 2018 a 2024

Fonte: CNCS, Relatórios 2020-2025

A maioria destes incidentes afetou os princípios de confidencialidade, integridade e disponibilidade, destacando-se a confidencialidade como a dimensão mais comprometida, com 70,32% dos incidentes reportados à CNPD (CNCS, Relatórios 2020-2025).

Importa salientar que o setor privado foi o mais afetado pelas violações de dados pessoais em 2024, concentrando 77% das notificações, enquanto que o setor público registou 23%. Comparativamente a 2023, observou-se um aumento da proporção de notificações provenientes de entidades privadas (74%), o que corresponde a uma redução relativa das notificações provenientes de entidades públicas (CNCS, Relatórios 2020-2025).

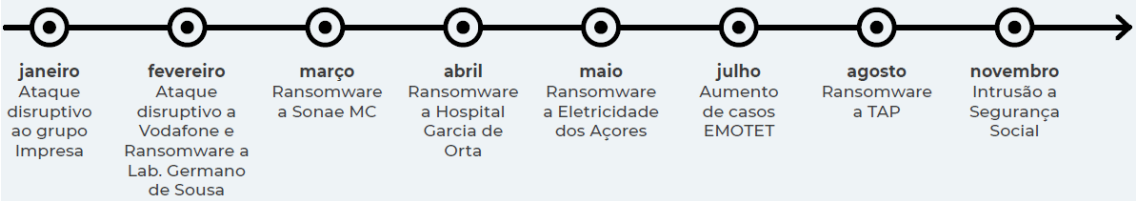
A análise dos vários tipos de incidentes e dos diversos setores abrangidos, permite compreender melhor o contexto em que atuam os diferentes agentes de ameaça no panorama nacional. Torna-se, assim, pertinente identificar os principais atores responsáveis pelas principais ameaças referidas anteriormente, cuja atuação contribui de forma decisiva para o aumento e diversificação dos incidentes registados em Portugal.

De acordo com os relatórios de cibersegurança do CNCS, os principais agentes de ameaça identificados no contexto nacional entre 2020 e 2025, são os cibercriminosos, os agentes estatais, os hacktivistas e os *insiders* (negligentes). Os cibercriminosos evidenciam-se pela sua atuação orientada para a obtenção de ganhos económicos ou financeiros, podendo operar de forma autónoma ou com o apoio de um agente estatal. Já os atores estatais, que se caracterizam pela sofisticação técnica e operacional, beneficiando dos recursos e capacidades de um Estado, atuam com fins estratégicos ou políticos, frequentemente associados a operações de ciberespionagem e cibersabotagem. Por sua vez, os hacktivistas atuam por motivos ideológicos, sem procurar ganhos económicos, financeiros ou reputacionais, embora a exposição mediática constitua um elemento importante para a afirmação das suas causas. Por último, o *insider* negligente representa um tipo de agente interno que, por comportamentos negligentes, pode comprometer a cibersegurança das redes e sistemas de informação da própria organização (CNCS, Relatórios 2020-2025).

A identificação destes atores de ameaça permite contextualizar e compreender melhor a natureza dos incidentes cibernéticos em Portugal nos últimos anos. Neste domínio, destaca-se a vaga de ataque cibernéticos ocorrida entre 2022 e 2024, que teve como objetivo várias instituições públicas e privadas, provocando a interrupção temporária de serviços essenciais e a exfiltração de dados sensíveis.

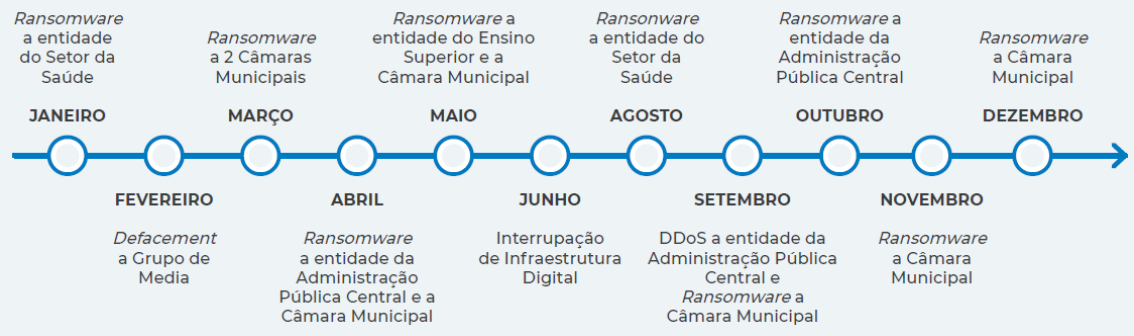
No passado recente, os incidentes mais relevantes em Portugal estiveram essencialmente associados à utilização de código malicioso, com particular destaque para o *ransomware* (Figuras 12, 13 e 14), sendo os casos mais notórios os dirigidos à Sonae MC, à Vodafone, ao Hospital Garcia da Horta, à Eletricidade dos Açores, à TAP e a várias entidades públicas locais e centrais.

Fig. 12 - Cronologia de ataques no ciberespaço com impacto elevado em Portugal, 2022[49]



Fonte: CNCS, Relatórios 2020-2025

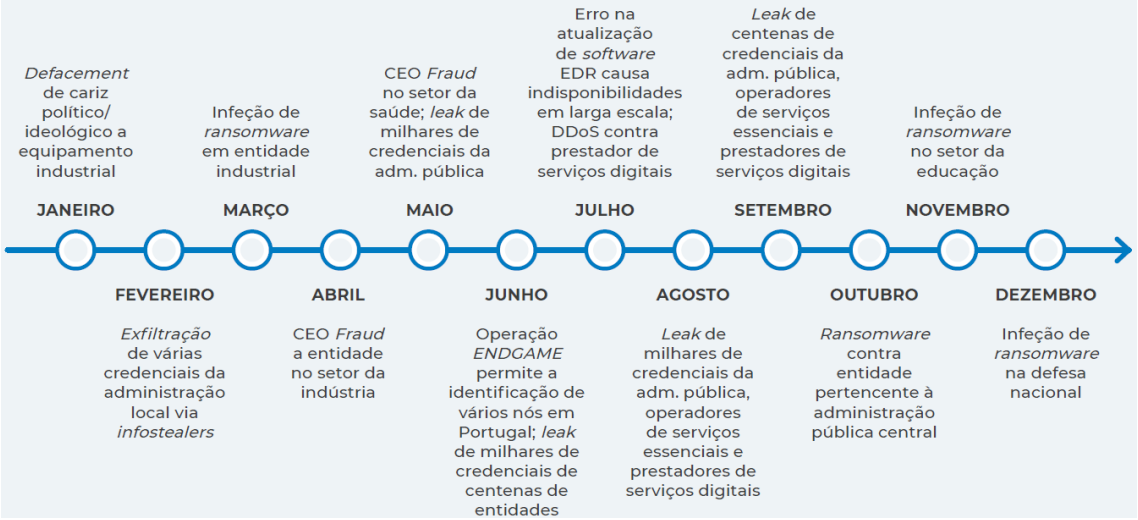
Fig. 13 - Cronologia de ataques no ciberespaço com impacto elevado em Portugal, 2023[50]



Fonte: CNCS, Relatórios 2020-2025

[49] e [50] Consideram-se como ataques no ciberespaço com impacto elevado os incidentes com efeitos relevantes nos serviços e infraestruturas e/ou com visibilidade social, cuja investigação já tenha revelado conclusões suficientes para serem descritos.

Fig. 14 - Cronologia dos incidentes e eventos no ciberespaço mais relevantes em Portugal, 2024[51]



Fonte: CNCS, Relatórios 2020-2025

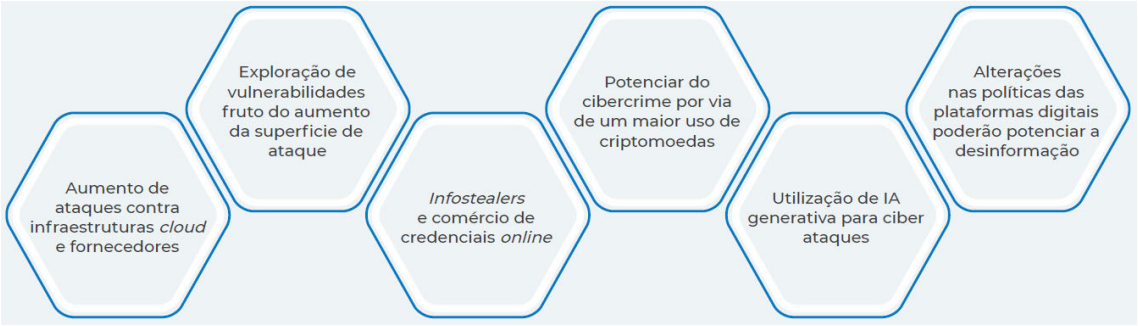
A análise dos tipos de ataque e dos setores afetados permite concluir que, independentemente da dimensão ou natureza das organizações, todas estão potencialmente expostas a ataques disruptivos, capazes de paralisar não apenas as respetivas organizações, mas também as entidades e serviços que delas dependem.

Em suma, de acordo com os Relatórios 2020-2025, o risco de uma entidade sofrer um incidente de cibersegurança no espaço digital aumentou em 2024 e irá continuar a aumentar nos próximos anos, sendo o *phishing* e o *smishing*, apontados como os principais tipos de ameaças, seguidos do *ransomware* e da exploração de vulnerabilidades. As técnicas de engenharia social e o *phishing* consolidam-se como os vetores de ataque mais recorrentes em Portugal, refletindo a crescente exploração do fator humano, enquanto o setor privado permanece como o principal alvo das ciberameaças. De acordo com os Relatórios, os cibercriminosos continuaram a ser considerados os principais agentes de ameaça, enquanto a introdução e massificação de tecnologias digitais emergentes – como a IA, a computação na nuvem e a automação avançada – nos

[51] A relevância de um incidente ou evento é avaliada com base no seu impacto, pelo seu carácter inovador, vitimologia e, conhecendo-se, natureza do atacante e por isso apenas pode ser avaliada em casos cuja investigação já tenha revelado conclusões suficientes.

ataques cibernéticos, irá contribuir para aumentar a complexidade e eficácia dos ataques, ampliando a sua velocidade, alcance, e capacidade de dissimulação, tornando cada vez mais difícil o sucesso do combate às ciberameaças.

Fig. 15 - Tendências para o futuro próximo



Fonte: CNCS, Relatórios 2020-2025

De acordo com os dados analisados, o panorama nacional de cibersegurança confirma uma tendência de crescimento e diversificação das ciberameaças, inserida num contexto de transformação digital acelerada. Embora os incidentes registados incluam setores não abrangidos pela Diretiva NIS2, observa-se uma forte correspondência entre os principais setores alvo e aqueles incluídos no seu âmbito de aplicação. Este panorama reforça a importância e necessidade da adoção da NIS2 por parte das entidades abrangidas.

1.5.2. Contexto europeu

A nível europeu, o panorama das ciberameaças tem se tornado progressivamente mais complexo e interligado, refletindo a crescente sofisticação, frequência e impacto dos ciberataques no espaço digital da União. A TD dos setores dos transportes, energia, finanças, telecomunicações e administração pública, só para citar alguns, tem criado um ecossistema digital cada vez mais interconectado e vulnerável. Este cenário é o resultado da evolução da TD e da crescente interdependência entre infraestruturas críticas, serviços essenciais e cadeias de abastecimento, aumentando desta forma a superfície de exposição a ciberameaças (ENISA, 2025a).

De acordo com os Relatórios ENISA *Threat Landscape* 2021-2025 (ETL 2021-2025), a UE enfrenta um crescimento significativo da quantidade, diversidade e complexidade de

ameaças cibernéticas, com destaque para o predomínio de ataques de *phishing*, engenharia social e *ransomware*, assim como a exploração de vulnerabilidades (Figura 16).

Fig. 16 - Principais ameaças na Europa, em 2024

Fonte: ENISA, ETL 2021-2025

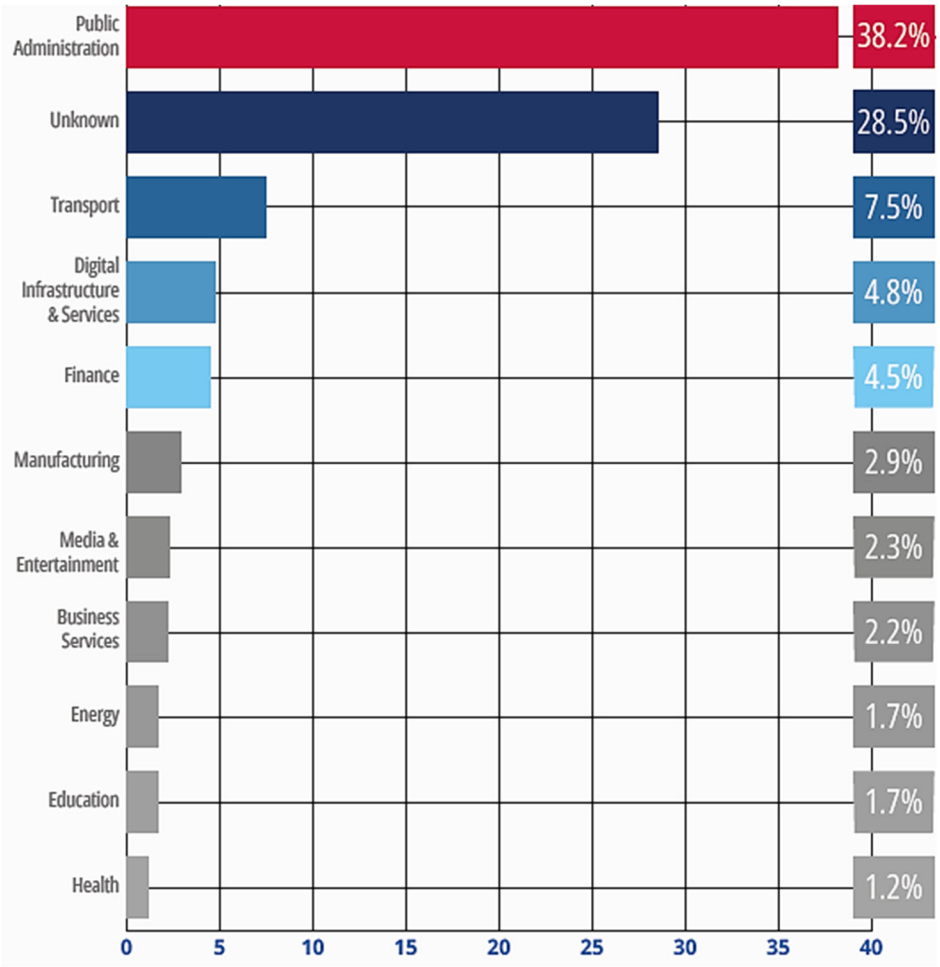
Os ataques DDoS têm registado igualmente um crescimento expressivo, em particular devido à atividade de grupos de hacktivistas motivados por fatores políticos ou ideológicos. Estes incidentes têm afetado sobretudo entidades públicas, instituições financeiras e operadores de serviços digitais, provocando interrupções na continuidade dos serviços prestados por estas entidades e, nalguns casos, a violação de dados sensíveis (ENISA, 2025a).

Este cenário de ameaças tem-se mantido relativamente estável nos últimos anos, continuando e criar impactos significativos na disponibilidade dos serviços e na proteção de dados. De acordo com os relatórios da ENISA (ETL 2021-2025), as principais tipologias de ameaças permanecem consistentes, destacando-se o *ransomware*, o *malware*, a engenharia social (com destaque para o *phishing*) e as ameaças direcionadas aos dados. A natureza persistente destas ameaças reflete-se de forma distinta nos

diferentes setores de atividade, revelando padrões específicos de incidentes e vulnerabilidades que afetam, em maior ou menor grau, as infraestruturas críticas, os serviços essenciais e as entidades públicas e privadas em toda a UE.

De acordo com o ETL 2025, os principais ciberataques corridos no período em análise tiveram como principal alvo a administração pública, representando cerca de 38,2% dos incidentes registados no espaço digital da União (Figura 17). Seguem-se os setores dos transportes (7,5%), das infraestruturas e serviços digitais (4,8%) e o setor financeiro/banca (4,5%), ambos fundamentais para o normal funcionamento das atividades económicas e sociais na UE.

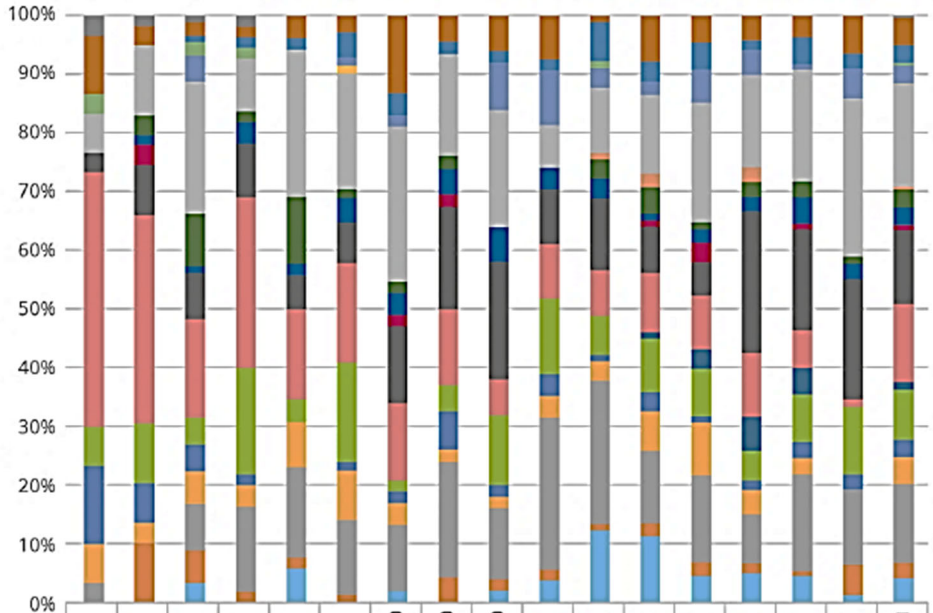
Fig. 17 - Incidentes registados por setor na Europa, 2025



Fonte: ENISA, ETL 2021-2025

Este cenário tem-se mantido relativamente estável nos últimos anos, destacando-se, contudo, o aumento significativo do registo de incidentes no setor dos transportes – que, em 2021, não figurava entre os quatro setores mais visados –, em contraste com a redução progressiva no setor da saúde, que nesse mesmo ano encontrava-se entre os quatro principais setores mais afetados (ETL 2021-2025) (Figura 18).

Fig. 18 - Evolução dos incidentes observados na Europa, em função do setor afetado, em 2020 e 2021



	4/20	5/20	6/20	7/20	8/20	9/20	10/20	11/20	12/20	1/21	2/21	3/21	4/21	5/21	6/21	7/21	Total
Water utilities	1	1	1	1													4
Transport	3	2	2	1	2	2	7	2	3	4	1	7	4	5	4	5	54
Targeted individuals			1	1	1	3	2	1	1	1	6	3	4	2	5	2	33
Space	1		2	1							1						5
Software supply chain			4			1	1		4	5	3	2	5	5	1	4	35
Semiconductor						1											1
Public administration/ Government	2	7	20	5	13	14	14	8	10	4	10	12	18	19	21	21	198
Postal & Courier Services											1	2		3			6
Military		2	8	1	6	1	1	1			3	4	1	3	3	1	35
Media/Entertainment		1	1	2	1	3	2	2	3	2	3	1	2	3	5	2	33
Legal		2					1	1				1	3		1		9
Healthcare/Medical	1	5	7	5	3	5	7	8	10	5	11	7	5	29	19	16	143
General public	13	21	15	16	8	12	7	6	3	5	7	9	8	13	7	1	151
Food												1	3	7	5		16
Finance/Banking	2	6	4	10	2	12	1	2	6	7	6	8	7	6	9	9	97
Energy	4	4	4	1		1	1	3	1	2	1	3	1	2	3	2	33
Education/Academic	2	2	5	2	4	6	2	1	1	2	3	6	8	5	3		52
Digital Service Providers	1		7	8	8	9	6	9	6	14	22	11	13	10	18	10	152
Construction		6	5	1	1	1		2	1	1	1	2	2	2	1	4	30
All Sectors			3		3		1		1	2	11	10	4	6	5	1	47

Fonte: ENISA, ETL 2021-2025

A análise das técnicas e vetores de intrusão apresentadas no ETL 2025 revela uma crescente sofisticação e diversificação das estratégias utilizadas pelos atacantes, centradas sobretudo na exploração de vulnerabilidades e do fator humano como principais pontos de entrada para comprometer os sistemas e infraestruturas digitais. Segundo a ENISA (2025a), cerca de 21% dos incidentes estiveram associados à exploração de vulnerabilidades, enquanto os ataques de *phishing* continuam a ser o vetor de intrusão mais recorrente no ciberespaço europeu, representando aproximadamente 60% dos casos observados. Paralelamente, destaca-se o aumento do recurso a *infostealers* para o roubo de credenciais e dados sensíveis.

A crescente eficácia e disseminação dos ataques de *phishing* tem sido amplamente potenciada pelo fenómeno do *phishing-as-a-service* (PhaaS), identificado pela ENISA (ETL 2025) como um dos principais catalisadores deste tipo de ataques. Este modelo de serviço tem permitido que agentes de ameaça com reduzida capacidade técnica executem campanhas de *phishing* complexas, contribuindo para o alargamento deste tipo de incidentes a todos os setores de atividade da UE.

De acordo com a ENISA (ETL 2025), os principais atores de ameaça no ciberespaço europeu são os atores estatais, os cibercriminosos e os hacktivistas, cada um atuando com motivações e objetivos diferentes. As guerras na Ucrânia e em Gaza alteraram significativamente o panorama de ameaças no espaço digital europeu, com o aumento de ataques por hacktivistas ou patrocinados por Estados, às infraestruturas críticas dos EM (ENISA, 2025a).

Os grupos de hacktivistas destacam-se pelo elevado número de incidentes que lhes são atribuídos, recorrendo especialmente a ataques DDoS, para expressar as suas causas ideológicas ou políticas. Exemplos recentes incluem perturbações temporárias em portais e infraestruturas aeroportuárias em Milão (dezembro de 2024). Por sua vez, os grupos de cibercriminosos são responsáveis pelos incidentes de maior impacto económico e operacional, em particular pela realização de campanhas de *ransomware* que causam disrupção significativa nas organizações atingidas. Neste contexto, foram reportadas recentemente (setembro de 2025) ataques aos aeroportos de Bruxelas, *Heathrow* e

Berlim[52], com o objetivo de criar o caos operacional. Já os grupos alinhados com os Estados focam a sua atividade em operações de cibersabotagem e ciberespionagem para obter informação estratégica e o comprometimento das infraestruturas críticas, como foi o caso do ataque ao setor energético da Dinamarca em maio de 2023, considerado o maior ataque contra infraestruturas críticas do país[53].

Importa salientar que, embora os incidentes registados incluam também setores e entidades fora do âmbito da Diretiva NIS2, os quatro principais setores atingidos pelos ciberataques no espaço europeu– administração pública, transportes, infraestruturas e serviços digitais, e finanças – integram o conjunto de setores abrangidos pela Diretiva. Este facto confirma a relevância e necessidade da adoção efetiva das medidas previstas na NIS2 por estas entidades, uma vez que representam 53,7% do total de incidentes registados no espaço europeu (ENISA, 2025).

Do ponto de vista geral, o cenário europeu de cibersegurança caracteriza-se por uma crescente complexidade e interligação entre as diversas tipologias de ameaças, os setores de atividade e os agentes envolvidos. Prevê-se que as ameaças provenientes de cibercriminosos e de atores estatais continuem a afetar, de forma significativa, as entidades públicas e privadas no espaço europeu, recorrendo a técnicas como o *phishing*, o *ransomware* e a *infostealers*.

A disseminação dos modelos de ataque baseados em serviços (*as-a-service*), nomeadamente o *phishing-as-a*-service e o *ransomware-as-a*-service, é potenciada pela integração das tecnologias digitais emergente, como a IA. Estas tecnologias potenciam o desenvolvimento de campanhas mais rápidas, eficazes e sofisticadas, tornando o combate às ameaças cibernéticas um desafio cada vez mais exigente.

[52] https://www.govtech.com/blogs/lohrmann-on-cybersecurity/cyber-incidents-take-off-europes-airports-join-a-growing-list

[53] https://sektorcert.dk/wp-content/uploads/2023/11/SektorCERT-The-attack-against-Danish-critical-infrastructure-TLP-CLEAR.pdf

1.6. Síntese da Revisão da Literatura

A revisão da literatura possibilitou entender a relação entre a TD, a evolução tecnológica, a SI e a cibersegurança, assim como a evolução das políticas e estratégias europeias e nacionais na área da cibersegurança. Verificou-se também que as TIC são o motor da rápida TD da economia e sociedade europeias e nacionais, alterando significativamente o funcionamento das organizações e dos Estados. Esta rápida TD tem vindo a criar novas oportunidades, mas também cria riscos e vulnerabilidades associados ao ciberespaço.

Este capítulo permitiu compreender que a SI, a proteção de dados e a cibersegurança, embora interligadas, apresentam âmbitos e finalidades diferentes. Demonstrou que a cibersegurança tornou-se fundamental na TD, assumindo um papel importante na preservação da confiança e continuidade operacional das organizações.

No contexto europeu, a revisão demonstrou que a UE tem vindo a desenvolver progressivamente o seu quadro normativo em matéria de cibersegurança, através da adoção de atos legislativos com o objetivo de melhorar o funcionamento do mercado interno, elevando o nível de cibersegurança dos seus EM. Do ponto de vista nacional, verificou-se que Portugal tem acompanhado a evolução europeia, seja através da adoção das políticas europeias, seja pelo desenvolvimento de estratégias nacionais.

A análise efetuada evidenciou ainda a correlação entre a digitalização da economia e sociedade, e o aumento da frequência e complexidade dos ciberataques, nomeadamente, através de *ransomware*, *phishing* ou ataques DDoS. Esta crescente interdependência tem colocado grandes desafios às organizações públicas e privadas, o que comprova a importância deste estudo.

2. Diretiva (UE) 2022/2555 – NIS2

A UE baseia-se no Estado de Direito, o que significa que todas as suas medidas têm por fundamento os Tratados aprovados pelos EM. Estes Tratados definem os objetivos, regras e o funcionamento da UE e constituem o direito primário de toda a legislação da União. Os atos legislativos que decorrem dos princípios e objetivos consagrados nos Tratados constituem direito derivado, que inclui três atos jurídicos vinculativos – regulamentos, diretivas e decisões – e dois atos jurídicos não vinculativos – recomendações e pareceres. Desta forma, os EM conseguem distinguir o que é de cumprimento obrigatório e o que constitui apenas diretrizes de orientação dentro da legislação da UE.

Neste contexto, sendo a Diretiva NIS2 um ato jurídico vinculativo, significa que é de implementação obrigatória por todos os EM, sendo da sua responsabilidade a forma como a vão aplicar. Todos os EM são obrigados a adotar medidas para incorporar a Diretiva no direito nacional, a fim de atingir os objetivos nela definidos. Importar referir que a transposição de uma diretiva para o direito nacional deverá estar concluída, geralmente, no prazo de dois anos após a sua adoção. A sua não transposição dentro do prazo estabelecido pode dar início a um processo por infração.

A necessidade de implementação da Diretiva NIS2 surge no contexto da rápida TD e no consequente aumento dos riscos para a cibersegurança que tornam as sociedades mais vulneráveis a ciberameaças. Para mitigar esses riscos é necessário implementar um conjunto de medidas para reforçar a cibersegurança dentro da UE, de modo a proteger as redes e os sistemas de informação de ciberameaças.

Neste enquadramento, é imperativo compreender o papel da Diretiva NIS2 no reforço da cibersegurança e na promoção de uma resposta coordenada entre os EM face às ameaças no ciberespaço europeu. A análise que se segue, baseia-se principalmente na Diretiva (UE) 2022/2555 e na documentação emitida pelo CNCS, enquanto autoridade nacional competente nesta matéria, não substituindo nem dispensando a consulta das publicações originais.

A Diretiva (UE) 2016/1148 foi a primeira medida legislativa transversal a toda a UE com o objetivo de alcançar um elevado nível comum de segurança das redes e dos sistemas de

informação na União, por forma a melhorar o funcionamento do seu mercado interno. Esta Diretiva tinha como objetivo:

> desenvolver as capacidades de cibersegurança em toda a União, atenuar as ameaças aos sistemas de rede e informação utilizados para prestar serviços essenciais em setores-chave e garantir a continuidade de tais serviços em face de incidentes, contribuindo assim para a segurança da União e para o eficaz funcionamento da sua economia e sociedade (UE, 2022b).

Em Portugal, a NIS foi transposta para a lei portuguesa em 2018, estabelecendo o Regime Jurídico da Segurança do Ciberespaço. Esta Lei estabeleceu a estrutura nacional para a cibersegurança, designadamente, o CNCS como a entidade responsável por supervisionar as entidades abrangidas na implementação desta Diretiva, e o CERT.PT, como a entidade responsável pela coordenação operacional na resposta a incidentes de cibersegurança em território nacional.

No entanto, apesar dos progressos alcançados, as medidas previstas na NIS revelaram-se insuficientes perante o crescimento da quantidade, dimensão, sofisticação, frequência e impacto dos incidentes de cibersegurança no espaço digital da União (Schmitz-Berndt, 2023). A própria UE identificou divergências na aplicação da Diretiva pelos EM, nomeadamente na interpretação do seu âmbito, na aplicação das obrigações em matéria de segurança, na notificação de incidentes e na aplicação das disposições da Diretiva em matéria de supervisão e execução (UE, 2022b).

Face a este cenário, intensificado pela crise da pandemia COVID-19, a avaliação da Diretiva NIS, inicialmente prevista para maio de 2021, foi antecipada para dezembro de 2020 (UE, 2020). Desta revisão, resulta a aprovação da Diretiva (EU) 2022/20555, em dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, e que revoga a sua antecessora.

A NIS2 entrou em vigor ao nível da UE a 16 de janeiro de 2023, sendo que os EM tinham até 17 de outubro de 2024 para fazer a transposição para o seu direito nacional. Contudo,

a 7 de maio de 2025, apenas 8 EM tinham transporto a Diretiva para as respetivas legislações nacionais (UE, 2025e). Em Portugal, foi aprovada Lei n.º 59/2025, de 22 de outubro, que autoriza o Governo a transpor a NIS2.

A Diretiva NIS2 baseia-se, principalmente, na diretiva anterior, e alarga o seu âmbito para reforçar e fortalecer as medidas de cibersegurança com o intuito de proteger as infraestruturas críticas em toda a UE. Apesar do foco desta Diretiva estar no combate às ciberameaças, ela também abrange outros cenários de risco, nomeadamente, incidentes com origem em atos negligentes, falhas na implementação de medidas de segurança adequadas, falta de manutenção de sistemas críticos, erros humanos ou falta de práticas de gestão dos riscos.

Neste contexto, para obter uma visão clara do papel da Diretiva NIS2 no reforço do quadro europeu de cibersegurança, é fundamental compreender a Diretiva, nomeadamente, quais os seus principais objetivos, como se distingue da sua antecessora e quais os seus principais requisitos.

A NIS2 pretende atingir os mesmos objetivos que a sua antecessora, principalmente (CNCS, 2025a):

- Exigir que os EM garantam um elevado nível de cibersegurança;
- Reforçar a cooperação europeia entre as autoridades competentes pela cibersegurança;
- Exigir que os principais operadores dos sectores-chave da nossa sociedade adotem as medidas de segurança necessárias e notifiquem às autoridades competentes qualquer incidente que tenha um impacto significativo na prestação dos seus serviços.

Esta Diretiva pretende, entre outros objetivos, eliminar as divergências existentes na aplicação dos requisitos da NIS entre os EM, contribuindo para uma maior harmonização através da definição de regras mínimas relativas ao funcionamento de um quadro regulamentar coordenado[54]. Ao alargar o seu âmbito de aplicação, a NIS2 procurar

[54] NIS2, artigo 5.º

responder aos desafios já reportados anteriormente e que se encontram explanados na própria diretiva[55].

Para uma melhor compreensão do alcance destas alterações e a forma como a NIS2 pretende ultrapassar as limitações da sua antecessora, importa analisar as principais diferenças e inovações introduzidas face à NIS, quer ao nível do seu âmbito de aplicação, quer ao nível das obrigações impostas às entidades abrangidas.

As principais diferenças e novidades introduzidas pela nova Diretiva em relação à anterior centram-se na ampliação do seu âmbito de aplicação, na estruturação dos setores abrangidos, na categorização das entidades abrangidas, e no reforço das obrigações e responsabilidades dessas entidades. A NIS2 passa, assim, a incluir mais entidades, diferenciando estas entre essenciais ou importantes, de acordo com a relevância nos setores onde estão inseridas ou com o tipo de serviço que prestam, bem como a sua dimensão[56].

Esta Diretiva introduz também uma maior precisão e um reforço das medidas de gestão dos riscos de cibersegurança, reconhecendo a importância da proteção das cadeias de abastecimento e a definição de regras mais detalhadas, específicas e otimizadas para o reporte de incidentes de cibersegurança[57]. Adicionalmente, a Diretiva NIS2 reforça os poderes de supervisão das autoridades competentes – no caso português será o CNCS – e estabelece um quadro sancionatório harmonizado a nível europeu, mais robusto e com coimas mais elevadas[58].

Importa ainda destacar a introdução da responsabilidade direta das pessoas singulares que desempenham funções de direção nas entidades abrangidas, bem como a importância da sua formação em cibersegurança[59].

[55] NIS2, Considerando 3.
[56] NIS2, artigo 3.º
[57] NIS2, artigos 21.º, 22.º, 23.º e 30.º
[58] NIS2, artigos 31.º a 37.º
[59] NIS2, artigos 20.º e 32.º

A Diretiva estabelece, igualmente, um conjunto de requisitos fundamentais destinados a assegurar um elevado nível comum de cibersegurança na União, impondo às entidades abrangidas a necessidade de rever, criar, estabelecer e/ou melhorar:

- Gestão dos riscos de cibersegurança e medidas técnicas, operacionais e organizativas;
- Notificação de incidentes de cibersegurança;
- Continuidade das atividades e gestão de crises;
- Segurança da cadeia de abastecimento e das relações com fornecedores diretos;
- Práticas básicas de ciber-higiene e formação em cibersegurança;
- Responsabilidade da gestão e governação das entidades;
- Supervisão, execução e regime sancionatório.

De forma geral, a Diretiva NIS2 estabelece um conjunto de requisitos destinados a reforçar a resiliência das redes e sistemas de informação das organizações públicas e privadas, promovendo uma abordagem integrada à gestão da cibersegurança. Ao exigir que as entidades abrangidas adotem medidas técnicas, operacionais e organizativas, práticas eficazes de gestão dos riscos e mecanismos de resposta a incidentes, esta Diretiva contribui para a consolidação de um elevado nível de cibersegurança em toda a União.

Tendo em conta as alterações introduzidas e o alargamento substancial do âmbito de aplicação da NIS2, considera-se importante analisar quais as entidades que passam a estar abrangidas pela Diretiva de acordo com os critérios definidos.

Nos termos dos artigos 2.º e 3.º, a NIS2 aplica-se a entidades públicas ou privadas, pertencentes a um dos tipos identificados nos anexos I e II da própria Diretiva, e que se enquadrem na definição de médias empresas ou que excedam os limiares destas (Figura 19).

Fig. 19 - Grandes e PME*

Micro empresa	Pequena empresa	Média empresa	Grande emrpesa
emprega menos de 10 pessoas e o volume de negócios anual ou balanço total anual não excede 2 milhões de euros.	emprega entre 11 e 50 pessoas e o volume de negócios anual ou balanço total anual não excede 10 milhões de euros.	emprega entre 51 a 250 pessoas; o volume de negócios anual não excede 50 milhões de euros ou o balanço total anual não excede 43 milhões de euros.	empresa masi de 250 pessoas; o volume de negócios anual excede 50 milhões de euros ou o balanço total anual excede 43 milhões de euros.
*Recomendação 2003/361/CE, da Comissão			

Fonte: elaboração própria, 2025

As entidades abrangidas são classificadas em entidades essenciais (setores de importância crítica) e entidades importantes (outros setores críticos), de acordo com o artigo 3.º, refletindo a medida em que são fundamentais no que concerne ao seu setor ou ao tipo de serviço que prestam (Figura 20).

Fig. 20 - Setores/serviços abrangidos pela NIS2

Essenciais	Importantes
Energia	Serviços postais e de estafeta
Transportes	Gestão de resíduos
Setor Bancário	Produção, fabrico e distribuição de produtos químicos
Infraestruturas do mercado financeiro	Produção, transformação e distribuição de produtos alimentares
Saúde	Indústria transformadora
Água potável	Prestadores de serviços digitais
Águas resíduais	Investigação
Infraestruturas digitais	
Gestão de serviços TIC (entre empresas)	
Administração pública	
Espaço	

Fonte: elaboração própria, 2025

Todavia, a Diretiva aplica-se a determinados prestadores de serviços considerados essenciais, independentemente da sua dimensão, nomeadamente, fornecedores de redes públicas de comunicações eletrónicas ou prestadores de serviços de comunicações eletrónicas acessíveis ao público, prestadores de serviços de confiança ou entidades responsáveis por registos de nomes de domínio e sistemas de nomes de domínio.

Adicionalmente, a Diretiva NIS2 abrange ainda entidades cuja atividade seja considerada crítica por cada EM. Estas entidades são legíveis se desempenharem funções essenciais para manutenção de funções societais ou económicas, para a segurança, proteção ou saúde

públicas, ou que possam gerar riscos sistémicos significativos, especialmente com impacto transfronteiriço.

A aplicação da Diretiva estende-se ainda a entidades públicas, mediante tipificação por cada EM, que prestem serviços críticos e cuja interrupção teria impacto relevante nas atividades sociais e económicas da União, bem como às entidades críticas identificadas pela Diretiva (UE) 2022/2557.

Estão excluídas do âmbito da Diretiva NIS2 as entidades que exerçam atividades nos domínios da defesa, da segurança nacional, da segurança pública, da defesa ou da aplicação de lei, incluindo a prevenção, investigação, deteção e repressão de infrações penais.

Conhecido o âmbito de aplicação da Diretiva e as entidades abrangidas, importa analisar as medidas de gestão dos riscos de cibersegurança que estas entidades devem adotar, com vista a garantir um elevado nível comum de cibersegurança na União.

De acordo com o artigo 21.º, as entidades abrangidas devem tomar medidas abrangentes, de carácter técnico, operacional e organizativo, para garantir a proteção dos sistemas de rede e informação. Estas devem ser adequadas e proporcionadas para gerir os riscos que afetam a segurança dos seus sistemas, assim como prevenir ou reduzir o impacto de incidentes, em ambientes físicos ou digitais, nas suas operações ou de terceiros.

Estas medidas devem ainda assegurar um nível de segurança ajustado ao risco, tendo em consideração a evolução tecnológica e, se aplicável, as normas europeias e internacionais pertinentes, assim como aos custos de implementação. Ao avaliarem a proporcionalidade das medidas a adotar, as entidades essenciais e importantes devem medir o seu grau de exposição ao risco, a probabilidade de um incidente ocorrer e qual a gravidade do seu impacto social e económico.

Estas medidas devem, no mínimo, contemplar os seguintes domínios:

- Políticas de análise de riscos e de segurança dos sistemas de informação;
- Tratamento de incidentes;

- Continuidade das atividades, como a gestão de cópias de segurança e a recuperação de desastres, e gestão de crises;
- Segurança da cadeia de abastecimento, incluindo aspetos de segurança respeitantes às relações entre cada entidade e os respetivos fornecedores ou prestadores de serviços diretos;
- Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e informação, incluindo o tratamento e a divulgação de vulnerabilidades;
- Políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;
- Práticas básicas de ciber-higiene e formação em cibersegurança;
- Políticas e procedimentos relativos à utilização de criptografia e, se for caso disso, de cifragem;
- Segurança dos recursos humanos, políticas seguidas em matéria de controlo do acesso e gestão de ativos;
- Utilização de soluções de autenticação multifator ou de autenticação contínua, comunicações seguras de voz, vídeo e texto e sistemas seguros de comunicações de emergência no seio da entidade, se for caso disso.

A Diretiva NIS2 introduz ainda medidas especificas para as entidades dos setores das infraestruturas digitais, da gestão de serviços TIC e da prestação de serviços digitais, refletindo a necessidade de uma abordagem diferente em função da criticidade e tipo de serviços prestados por essas entidades[60]. Os requisitos técnicos e metodológicos das medidas de gestão dos riscos de cibersegurança a adotar por estas entidades, constam no Regulamento de Execução da Diretiva (UE) 2022/2555, de 17 de outubro de 2024 (UE, 2024).

Esta Diretiva atribui maior ênfase à segurança da cadeia de abastecimento, não só porque um ataque a uma empresa terá impacto nas suas operações isoladamente, como também pode ter um efeito em cascata, afetando outras entidades das quais são fornecedoras. Neste contexto, a NIS2 confere uma importância acrescida neste domínio, relativamente

[60] NIS2, artigo 21.º

às medidas de segurança da cadeia de abastecimento, incluindo os aspetos associados às relações entre cada entidade e os seus fornecedores ou prestadores de serviços diretos. Assim, as entidades devem avaliar a adequação das medidas a adotar tendo em consideração as vulnerabilidades específicas, a qualidade global dos produtos, as práticas de cibersegurança e os procedimentos de desenvolvimento seguro dos seus fornecedores ou prestadores de serviços.

Embora as micro e pequenas empresas não estejam diretamente cobertas pela NIS2 (à exceção das entidades referenciadas nos artigos 2.º e 3.º), se fizerem parte da cadeia de abastecimento das entidades essenciais e importantes, estas entidades têm a responsabilidade de garantir a cibersegurança entre os seus fornecedores.

Em Portugal, o CNCS disponibiliza o QNRCS, que constitui um guia de cibersegurança, com a indicação de um conjunto de medidas que abrangem todos os aspetos da gestão dos riscos de cibersegurança a implementar pelas entidades essenciais e importantes. Este organismo disponibiliza também o Guia para a Gestão dos riscos em matérias de SI e cibersegurança. Este guia é um referencial que visa estabelecer uma abordagem coerente e sistematizada ao processo de identificação, análise, avaliação e tratamento dos riscos de cibersegurança. O objetivo deste documento é orientar as entidades na implementação de um processo de gestão dos riscos ao nível organizacional.

Após a definição dos requisitos técnicos e metodológicos das medidas de gestão dos riscos de cibersegurança, a Diretiva NIS2 estabelece igualmente obrigações de reporte de incidentes significativos[61], assegurando que as autoridades competentes, nomeadamente a CSIRT respetiva, dispõem da informação atempada para avaliar o eventual impacto transfronteiriço do incidente.

De acordo com o artigo 23.º, as entidades abrangidas pela Diretiva são obrigadas a notificar as autoridades, sem demora injustificada, qualquer incidente de cibersegurança que tenha um impacto significativo na prestação dos seus serviços. No caso de ocorrer um incidente significativo, as entidades afetadas devem comunicar um alerta rápido no

[61] NIS2, artigo 23.º

prazo de 24 horas, depois de terem tomado conhecimento do incidente, indicando se este foi causado por um ato ilícito ou malicioso ou se pode ter um impacto transfronteiriço. Posteriormente, 72 horas depois, as entidades devem apresentar uma notificação com a avaliação inicial da gravidade e do impacto do incidente, acompanhada dos indicadores de exposição a riscos, se aplicável. A pedido da CSIRT, ou da autoridade competente, poderá ainda haver lugar a um relatório intercalar para atualização da informação importante. Por último, no prazo máximo de um mês após a notificação, as entidades terão de enviar um relatório final com a descrição pormenorizada do incidente e da sua gravidade, com o tipo de ameaça ou causa provável, com as medidas de remediação aplicadas e em curso e a descrição do impacto transfronteiriço, se aplicável.

Em Portugal, atualmente, as entidades que devem ser notificadas em caso de um incidente significativo estão definidas no Regime Jurídico da Segurança do Ciberespaço – o CNCS e as autoridades setoriais competentes – e que será atualizado com a transposição da Diretiva (UE) 2022/2555).

De forma a criar condições para estimular o cumprimento rigoroso dos requisitos da Diretiva NIS2, a UE inclui um quadro sancionatório como mecanismo de incentivo à conformidade que visa assegurar a implementação efetiva das medidas de cibersegurança por parte das entidades abrangidas. Neste âmbito, os artigos 32.º e 33.º incubem os EM a adotar medidas de supervisão ou de execução necessárias para garantir o cumprimento da Diretiva. Estas medidas devem ser eficazes, proporcionadas e dissuasivas, tendo em conta as circunstâncias individuais de cada entidade.

No caso de haver incumprimento das obrigações previstas nos artigos 21.º ou 23.º, por parte das entidades, o artigo 34.º determina o seguinte regime sancionatório:

- entidades essenciais: coimas "num montante máximo não inferior a 10 000 000,00€ ou num montante máximo não inferior a 2 % do volume de negócios anual a nível mundial, no exercício financeiro anterior, da empresa a que a entidade essencial pertence, consoante o montante que for mais elevado";
- entidades importantes: coimas "num montante máximo não inferior a 7 000 000,00€ ou num montante máximo não inferior a 1,4 % do volume de

> negócios anual a nível mundial, no exercício financeiro anterior, da empresa a que a entidade importante pertence, consoante o montante que for mais elevado".

A presente Diretiva prevê ainda um regime diferente no caso de se tratar de entidades da administração pública, cabendo aos EM adotar as regras para determinar se e em que medida podem ser aplicadas coimas.

Entre as principais inovações da Diretiva NIS2, destaca-se a responsabilização dos membros dos órgãos de direção, ou qualquer pessoa singular responsável com poder de representação, das entidades essenciais e importantes, evidenciado nos artigos 20.º e 32.º. Estes artigos estabelecem que estes responsáveis devem aprovar as medidas de gestão dos riscos de cibersegurança, supervisionar a sua aplicação e, em caso de infrações cometidas pelas suas entidades, podem ser responsabilizados.

O artigo 20.º estabelece ainda que os membros dos órgãos de direção sejam obrigados a frequentar ações de formação de cibersegurança, e incentiva as entidades essenciais e importantes a fornecer ações de formação semelhantes aos seus funcionários, promovendo uma cultura de ciber-higiene dentro das organizações. Esta sensibilização para a cibersegurança e ciber-higiene são fundamentais para garantir um elevado nível comum de cibersegurança na UE.

Em termos gerais, a análise da Diretiva NIS2, evidencia um reforço significativo do quadro europeu de cibersegurança, consolidando os avanços introduzidos pela sua antecessora. A própria designação da Diretiva traduz esta mudança de paradigma, passando de "segurança das redes e da informação" (NIS) para "cibersegurança" (NIS2).

A nova Diretiva é a resposta da UE ao aumento da complexidade e frequência das ameaças digitais, e à necessidade de promover uma abordagem harmonizada à cibersegurança e de aumentar a maturidade cibernética em toda a União. Para alcançar esses objetivos foi necessário aumentar o âmbito de aplicação, introduzir medidas técnicas, operacionais e organizativas mais robustas e reforçar as obrigações de reporte de incidentes, o estabelecimento de mecanismos de supervisão mais rigorosos e a implementação de um quadro sancionatório dissuasivo.

A Diretiva NIS2 representa um passo histórico na consolidação da resiliência digital europeia, contribuindo para a segurança da União e para o eficaz funcionamento da sua economia e sociedade.

3. Avaliação de resultados dos inquéritos e entrevistas

Considerando os objetivos do presente estudo e a problemática identificada, optou-se pela adoção de uma metodologia mista, combinando a revisão da literatura, a pesquisa quantitativa e a pesquisa qualitativa. Neste capítulo, pretende-se apresentar a análise dos dados obtidos, através dos inquéritos e entrevistas, realizados a profissionais das áreas das TIC e cibersegurança. O objetivo desta análise é avaliar o nível de maturidade das organizações em matéria de cibersegurança e identificar os principais desafios associados à implementação da Diretiva NIS2.

3.1. Pesquisa quantitativa (inquéritos)

A pesquisa quantitativa baseia-se na recolha de dados observáveis e mensuráveis, permitindo quantificar fenómenos e generalizar os resultados obtidos a partir de uma amostra (Freixo, 2011; Reis, 2010; Malhotra, 2004, citado por Gouveia, 2012). Neste contexto, optou-se pela realização de um inquérito estruturado, composto por questões fechadas, dirigido a profissionais das áreas das TIC e cibersegurança, cujo tratamento estatístico permitiu analisar as respostas de forma sistemática e comparável. Esta abordagem permitiu a recolha de dados quantificáveis, facilitando a subsequente análise estatística.

A investigação decorreu em quatro etapas: conceção do questionário, envio e acompanhamento das respostas, recolha e tratamento dos dados e, por fim, análise dos resultados obtidos.

Não sendo viável inquirir a totalidade das organizações abrangidas pela NIS2, optou-se por enviar o questionário ao maior número possível de profissionais, com o objetivo de aumentar a representatividade da amostra e reforçar a fiabilidade das análises estatísticas. Foi assegurada a todos os participantes a confidencialidade das respostas e o uso exclusivo dos dados para fins estritamente académicos no âmbito desta investigação.

O questionário foi elaborado e disponibilizado na plataforma *Google Forms*, sendo o convite à participação enviado por correio eletrónico e através da plataforma *LinkedIn*, de modo a maximizar a taxa de resposta. No total foram enviados mais de 200 emails com o

link de acesso ao questionário, que foi igualmente divulgado em três publicações no *LinkedIn*. A recolha de dados decorreu entre abril e setembro de 2025, tendo sido obtidas 30 respostas válidas.

Na sua elaboração, procurou-se garantir que as informações recolhidas permitissem alcançar o objetivo central desta pesquisa – avaliar o nível de maturidade das organizações em matéria de cibersegurança. Neste sentido, o inquérito foi construído com base na ferramenta *Cybercheckup*[62], do CNCS, fundamentada no QNRCS 2019 e no QACC 2020.

As questões, de carácter padronizado e apresentadas na mesma ordem a todos os participantes, pretenderam assegurar a fiabilidade, consistência e validade das respostas obtidas, possibilitando aferir o estado das organizações em termos de cibersegurança.

A escolha pela ferramenta *Cibercheckup* justifica-se pela sua relevância e adequação ao contexto nacional, enquanto instrumento de referência para autoavaliação das capacidades de cibersegurança das organizações. O modelo considera três níveis de capacidade – Inicial (1), Intermédio (2) e Avançado (3) – definidos no QACC 2020. Cada nível inclui as práticas propostas para atingir o objetivo definido e as evidências necessárias para verificar a implementação efetiva das medidas de segurança (Figura 21).

Fig. 21 - Níveis de capacidade definidos pelo QACC 2020

Níveis de Capacidade	Descrição	Evidências
1 – Inicial	Medidas de segurança básicas que poderiam ser implementadas para alcançar o objetivo de segurança, nomeadamente em iniciativas *ad-hoc*, por iniciativas isoladas e pouco formais.	Evidência de implementação das medidas de nível Inicial.
2 – Intermédio	Medidas de segurança que atendem à maioria dos casos e necessidades para atingir os objetivos de segurança da informação. As medidas são atingidas formalmente.	Evidência de implementação das medidas de nível Intermédio.
3 – Avançado	Medidas de segurança avançadas que envolvem a monitorização contínua dos controlos, avaliação e revisão recorrentes, levando em consideração alterações, incidentes, testes e exercícios, para melhoria proativa das mesmas.	Evidência de implementação das medidas de nível Avançado.

Fonte: CNCS, 2020

[62] https://cibercheckup.cncs.gov.pt/

Para atingir o nível máximo (3), as organizações devem implementar as medidas esplanadas nos níveis anteriores.

Importa sublinhar que a determinação dos níveis de capacidade é realizada de forma independente para cada objetivo de segurança podendo, dentro de um mesmo objetivo, coexistir dimensões com diferentes níveis de capacidade. Ou seja, esta ferramenta permite às organizações avaliar os diferentes níveis de maturidade, quer entre os objetivos de segurança, quer entre os componentes que integram cada um desses objetivos.

Após a revisão da literatura e considerando o fenómeno a estudar, o questionário foi estruturado em sete partes: introdução, identificação do setor de atividade da organização e cinco grupos de questões correspondentes às capacidades fundamentais de cibersegurança – Identificar, Proteger, Detetar, Responder e Recuperar (Figura 22). O questionário completo encontra-se no Anexo I.

Fig. 22 - Objetivos da cibersegurança

Fonte: CNCS, 2019

Os dados recolhidos foram submetidos a tratamento estatístico utilizando o *software Statistical Package for the Social Sciences* (SPSS). Foi realizada uma análise estatística descritiva com o objetivo de caracterizar o comportamento das variáveis em estudo.

Concluída a descrição dos procedimentos metodológicos, apresenta-se, de seguida, a análise dos dados recolhidos e dos principais resultados obtidos a partir dos inquéritos realizados. A análise dos resultados está estruturada segundo as dimensões

correspondentes às áreas avaliadas no inquérito, com o propósito de identificar as principais tendências e padrões nas respostas. Esta abordagem permitiu aferir o nível de maturidade em cibersegurança das organizações participantes, com base nos cinco domínios definidos no QNRCS 2019.

Com o objetivo de contextualizar o enquadramento organizacional das entidades que participaram no inquérito, precede-se à apresentação da distribuição das respostas por setor de atividade. No total, responderam 30 organizações, 26 das quais pertencem a diferentes setores abrangidos pela Diretiva NIS2. Seis das respostas obtidas dizem respeito a entidades que não estão abrangidas pela Diretiva, e estão identificadas como "Outros".

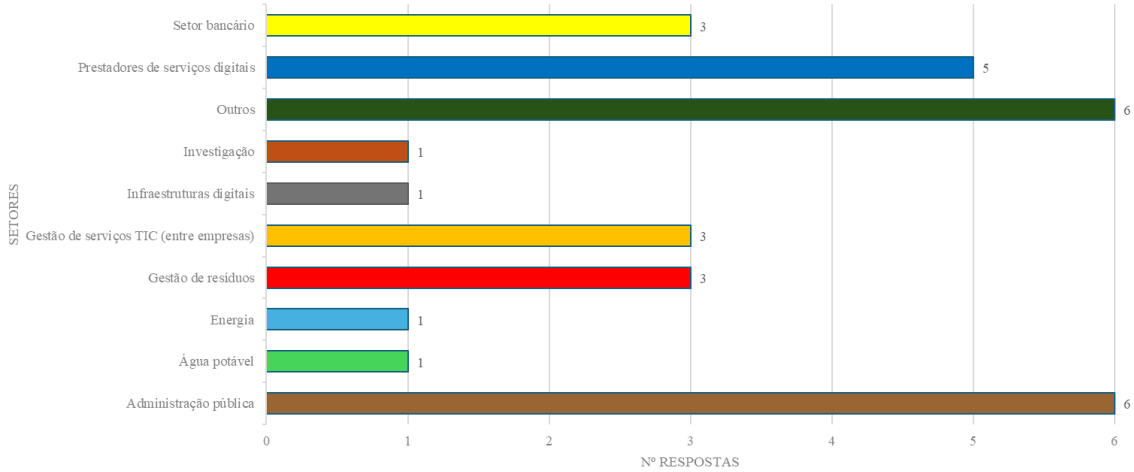
A análise da distribuição setorial evidencia que a Administração Pública e o grupo "Outros" registaram a maior percentagem de respostas, representando cada um 20% do total. Seguem-se as entidades Prestadoras de serviços digitais, com 16,7%, e os setores da Gestão de resíduos, Serviços TIC entre empresas e a Banca, cada um com 10%. Já os setores da Energia, Água potável, Infraestruturas digitais e Investigação registaram uma participação residual (3,3%), correspondendo a cada um apenas uma resposta (Figuras 23 e 24).

Fig. 23 - Distribuição das respostas por setor de atividade (%) – tabela

Setor de atividade	Qtd.	%
Administração pública	6	20
Água potável	1	3,3
Energia	1	3,3
Gestão de resíduos	3	10
Gestão de serviços TIC (entre empresas)	3	10
Infraestruturas digitais	1	3,3
Investigação	1	3,3
Outros	6	20
Prestadores de serviços digitais	5	16,7
Setor bancário	3	10
Total	30	100

Fonte: elaboração própria, 2025

Fig. 24 - Distribuição das respostas por setor de atividade – gráfico



Fonte: elaboração própria, 2025

Esta distribuição revela uma amostra diversificada, que abrange quer organizações públicas como privadas, permitindo analisar o nível de maturidade em cibersegurança em diferentes contextos setoriais em Portugal.

Importar referir que, embora a amostra inclua entidades de diferentes setores de atividade, o número de respostas obtidas foi relativamente reduzido. Esta limitada taxa de participação poderá estar associada à complexidade e sensibilidade do tema, bem como ao possível receio das entidades em partilhar informação detalhada sobre o seu nível de maturidade em cibersegurança, ainda que tenha sido garantida a total confidencialidade das respostas.

De acordo com a análise da tabela “Objetivos da cibersegurança” é possível constatar que o nível de maturidade das organizações varia entre os diferentes objetivos definidos no QNRCS 2019, com evidente tendência para valores intermédios. Verifica-se, igualmente, uma forte presença de respostas classificadas como “Não sabe/Não aplicável” (entre 29,0% e 37,9%). Este tipo de resposta pode indicar lacunas no conhecimento interno sobre a implementação (ou falta) de determinadas medidas de cibersegurança (Figura 25).

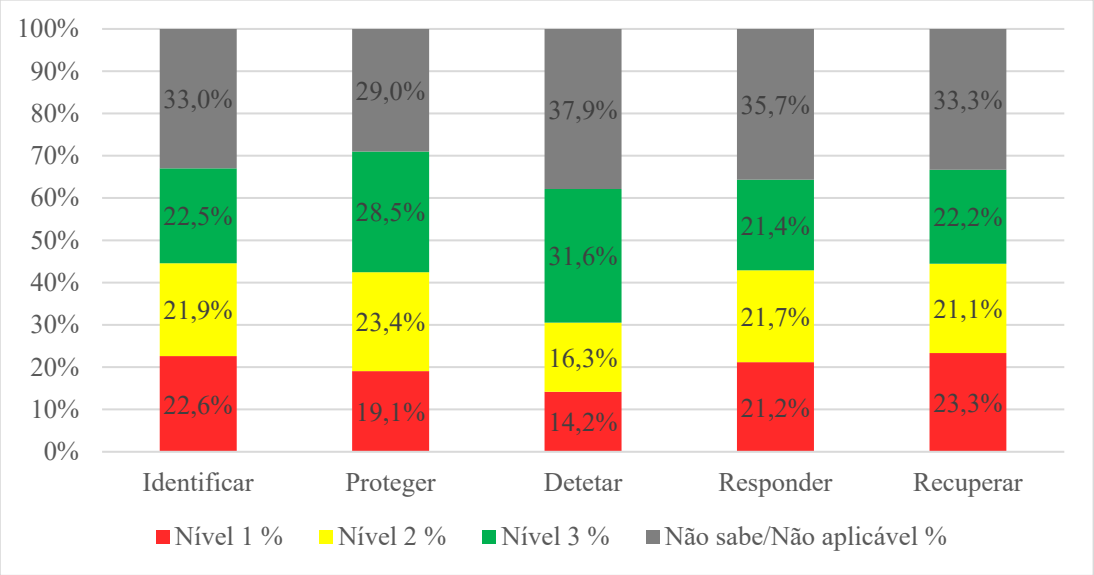
Fig. 25 - Objetivos da cibersegurança – nível médio de maturidade (%) – tabela

Medidas	Nível 1	Nível 2	Nível 3	Não sabe/Não aplicável
Identificar	22,6%	21,9%	22,5%	33,0%
Proteger	19,1%	23,4%	28,5%	29,0%
Detetar	14,2%	16,3%	31,6%	37,9%
Responder	21,2%	21,7%	21,4%	35,7%
Recuperar	23,3%	21,1%	22,2%	33,3%

Fonte: elaboração própria, 2025

De forma geral, observa-se uma distribuição equilibrada entre os níveis 1, 2 e 3, ainda que com diferenças entre objetivos (Figura 26).

Fig. 26 - Objetivos da cibersegurança – nível médio de maturidade (%) – gráfico



Fonte: elaboração própria, 2025

A dimensão "Proteger" destaca-se com o maior nível de maturidade, concentrando 28,5% das respostas no nível 3 (avançado) e 23,4% das respostas no nível 2 (intermédio), apresentando simultaneamente a percentagem mais baixa de "Não sabe/Não aplicável" (29,0%). Este resultado sugere que as organizações têm investido em medidas preventivas, como controlo de acessos, segmentação de redes, gestão de vulnerabilidades e políticas de backup (QNRCS 2019). O objetivo "Detetar" destaca-se como o segundo domínio com o maior nível de maturidade, concentrando 31,6% das respostas no nível 3,

e 16,3% e 14,2% das respostas nos níveis 2 e 1, respetivamente. No entanto, regista também a maior proporção de "Não sabe/Não aplicável" (37,9%). Esta análise permite concluir que existe uma assimetria no nível de maturidade em cibersegurança entre organizações na dimensão "Detetar".

As dimensões "Identificar", "Responder" e "Recuperar" revelam um padrão semelhante, com distribuições muito próximas entre os três níveis de maturidade (entre 21,1% e 23,3%), e percentagens elevadas de respostas "Não sabe/Não aplicável" (entre os 33,0% e os 35,7%). Estes resultados indicam que práticas como a identificação de ativos, gestão dos riscos, assim como as práticas associadas à resposta e recuperação face a incidentes, ainda se encontra em fase de consolidação e com níveis de maturidade relativamente baixos (QNRCS 2019).

A análise da tabela "Objetivos da cibersegurança" evidencia, assim, uma maior maturidade das organizações nas capacidades de proteção e deteção, associadas porventura a medidas tecnológicas e operacionais mais tangíveis, enquanto as dimensões de identificação, resposta e recuperação permanecem menos desenvolvidas.

A justificação deste panorama poderá estar relacionada com uma postura mais reativa e centrada na proteção técnica das redes e sistemas de informação, em detrimento da adoção de medidas de gestão dos riscos de cibersegurança, nomeadamente, políticas de análise dos riscos e de segurança dos sistemas de informação, sistemas de recuperação de desastres, gestão de incidentes, aspetos reforçados pela Diretiva NIS2.

De seguida, serão apresentados os resultados da análise do nível de maturidade em cibersegurança por setor de atividade (Figura 28), interpretada de acordo com os intervalos de classificação definidos na Figura 27.

Fig. 27 - Intervalo de classificação dos níveis de maturidade em cibersegurança

Intervalo de valores	Interpretação
1,00 – 1,99	Nível Inicial
2,00 – 2,49	Nível Intermédio
2,50 – 3,00	Nível Avançado

Fonte: elaboração própria, 2025

Fig. 28 - Nível médio de maturidade, por setor de atividade – tabela

Setor	Média Maturidade	Nível Maturidade
Administração pública	1,67	Nível Inicial
Água potável	1,88	Nível Inicial
Energia	2,92	Nível Avançado
Gestão de resíduos	1,45	Nível Inicial
Gestão de serviços TIC (entre empresas)	2,01	Nível Intermédio
Infraestruturas digitais	2,95	Nível Avançado
Investigação	1,38	Nível Inicial
Outros	1,56	Nível Inicial
Prestadores de serviços digitais	2,24	Nível Intermédio
Setor bancário	2,57	Nível Avançado
Total Geral	**1,93**	**Nível Inicial**

Fonte: elaboração própria, 2025

Estes intervalos, definidos no QACC 2020, demonstram que uma organização pode posicionar-se em níveis de capacidade distintos para um mesmo objetivo de segurança. Esta análise abrange tanto as entidades incluídas no âmbito de aplicação da Diretiva NIS2, como aquelas não abrangidas, identificadas na tabela pelo grupo "Outros".

De forma global, a amostra apresenta um nível médio de maturidade de 1,93%, o que corresponde a um nível inicial. Este resultado significa que a maioria das organizações inquiridas encontram-se numa fase preliminar de implementação de medidas de cibersegurança.

A tabela evidencia diferenças significativas no nível de maturidade em cibersegurança entre os setores de atividade, com destaque para os setores da Energia (2,92), Infraestruturas Digitais (2,95) e setor Bancário (2,57), que atingem níveis avançados de maturidade, acima de 2,5. Estes resultados podem ser justificados com o facto destes setores serem abrangidos por regulamentação própria na área da segurança da informação[63], tradicionalmente sujeitos a controlos de conformidade mais rigorosos. Sendo setores mais expostos a ciberataques, estas entidades tendem a reforçar os seus

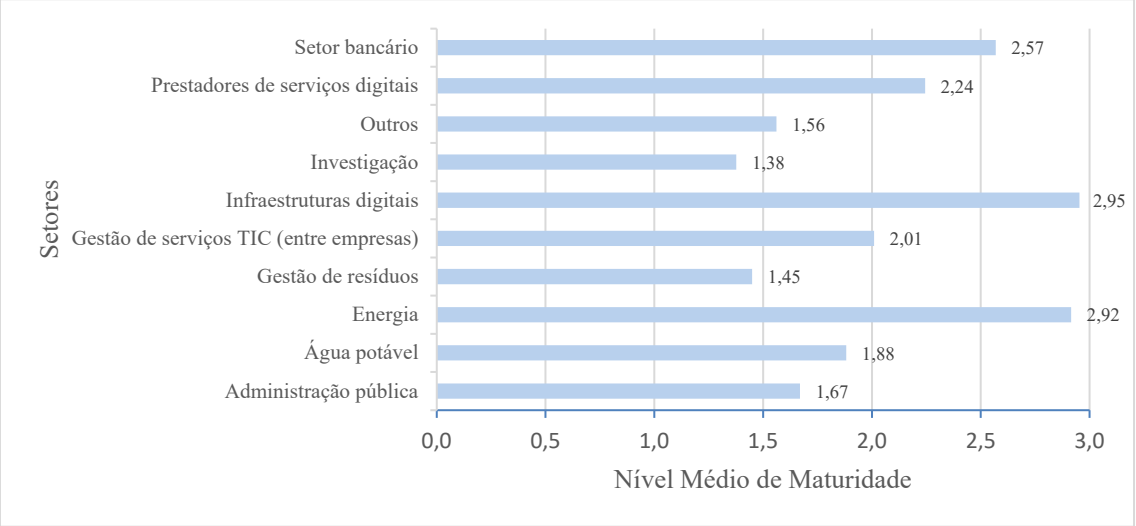
[63] Decreto-Lei n.º 15/2022; Regulamento (UE) 2022/2554; Lei n.º 46/2018.

sistemas de identificação, proteção, deteção e resposta a incidentes, assim como os sistemas de recuperação.

Os setores de Gestão de serviços TIC (ente empresas) e os Prestadores de serviços digitais apresentam níveis intermédios de maturidade em cibersegurança (2,01 e 2,24, respetivamente). Apesar destas entidades terem implementados sistemas e práticas de segurança, é necessário apostar em políticas organizacionais, processos de resposta e recuperação de incidentes, medidas essenciais para atingir o nível avançado (QNRCS 2019).

Em contraste, a Administração Pública (1,67), Água potável (1,88), Gestão de Resíduos (1,45), Investigação (1,38) e o grupo "Outros" apresentam níveis de maturidade baixos (inicial). Este grupo de setores representa a maior parte da amostra e revela que muitas organizações – incluindo várias entidades abrangidas pela Diretiva NIS2 – ainda se encontram num estado inicial de maturidade em cibersegurança (Figura 29).

Fig. 29 - Nível médio de maturidade, por setor de atividade - gráfico



Fonte: elaboração própria, 2025

Quanto às entidades classificadas como "Outros", o facto de estas não serem abrangidas pela Diretiva, pode ajudar a explicar o nível de maturidade mais baixo, dada a menor pressão regulatória e ausência de obrigações legais na área da SI.

No global, os resultados evidenciam uma clara assimetria na maturidade em cibersegurança entre setores, onde as áreas mais críticas e reguladas (energia, infraestruturas digitais e setor bancário) apresentam um nível avançado, enquanto setores com menos pressão regulatória demonstram a necessidade de reforçar as suas capacidades de cibersegurança. Estes resultados sugerem que a exposição a requisitos regulatórios e a dependência tecnológica podem influenciar positivamente o grau de implementação de medidas de cibersegurança nas organizações.

Estes resultados reforçam a importância da Diretiva NIS2 enquanto instrumento de harmonização e garante de um elevado nível comum de cibersegurança, incentivando as organizações – especialmente as de menor maturidade – a adotar medidas para reforçar as suas capacidades de cibersegurança, sejam elas abrangidas, ou não, pela Diretiva.

A análise quantitativa permitiu evidenciar um baixo nível de maturidade média em cibersegurança nas organizações inquiridas, com maior robustez nas dimensões de proteção e deteção e maior fragilidade nas dimensões de identificação, resposta e recuperação. A existência de diferenças significativas entre setores de atividade reforça a importância de políticas que garantam a harmonização e reforço das capacidades de cibersegurança, tal como preconizado pela Diretiva NIS2.

3.2. Pesquisa qualitativa (entrevistas)

A pesquisa qualitativa baseia-se, neste caso, numa metodologia estruturada, conduzida através de entrevistas compostas por um conjunto de questões aplicadas a todos os entrevistados, na mesma ordem e formulação. Este tipo de abordagem pretende compreender e interpretar o fenómeno em estudo, mais do que o medi-lo ou avaliá-lo. A investigação qualitativa procura, assim, observar, descrever e interpretar o contexto tal como se apresenta, sem procurar controlá-lo (Freixo, 2011; Reis, 2010; Malhotra, 2004, citado por Gouveia, 2012).

A opção por este tipo de pesquisa surgiu com o intuito de complementar a análise quantitativa e de aprofundar a compreensão sobre o grau de preparação das organizações

em relação à Diretiva NIS2. Esta fase da investigação baseou-se na realização de entrevistas estruturadas a profissionais das áreas de TIC e cibersegurança.

As entrevistas foram desenvolvidas à volta de quatro eixos principais:

1. Conhecimento e adoção da Diretiva NIS2;
2. Implementação dos requisitos;
3. Desafios enfrentados;
4. Impactos nos processos organizacionais, técnicos e operacionais.

Este planeamento permitiu explorar o nível de conhecimento das organizações sobre os requisitos da Diretiva, o estado de implementação das medidas de conformidade, as dificuldades encontradas, assim como as alterações introduzidas na governação, infraestrutura técnica e processos internos.

A investigação qualitativa pretendeu captar as perceções e experiências dos profissionais relativamente à aplicação dos requisitos da NIS2, permitindo identificar tendências, boas práticas e dificuldades comuns em contexto organizacional. As entrevistas constituíram, assim, um complemento essencial à pesquisa quantitativa, contribuindo para uma visão mais completa e holística da maturidade e capacidade de adaptação das entidades às exigências da Diretiva.

As entrevistas foram realizadas entre os meses de setembro e outubro de 2025, aplicadas a um conjunto de cinco participantes com experiência reconhecida nas áreas de cibersegurança e conformidade, com o objetivo de obter uma perspetiva diversificada sobre a aplicação da Diretiva NIS2 em Portugal.

O painel incluiu profissionais de diferentes setores de atividade: um professor universitário e especialista em cibersegurança, com experiência académica e científica na área (entrevistado 1); um consultor da empresa Hito, especialista em governação, gestão dos riscos e conformidade (entrevistado 2); um consultor da empresa de auditoria Ernest & Young, com atuação no domínio da conformidade, cibersegurança e gestão dos riscos (entrevistado 3); um colaborador do CNCS, enquanto consultor especialista em cibersegurança (entrevistado 4); e um representante da empresa Prologin, especializada

em produtos e serviços de cibersegurança e sistemas de informação (entrevistado 5). Esta diversidade permitiu incluir diferentes perspetivas setoriais, assegurando uma análise abrangente do nível de maturidade e dos desafios enfrentados pelas organizações. Importa referir que as respostas dadas pela Enerst & Young, refletem a experiência global da empresa no acompanhamento de clientes no âmbito de conformidade com regulação em cibersegurança.

As entrevistas seguiram um guião estruturado, composto por um conjunto fixo de questões idênticas para todos os participantes, de acordo com os quatro temas referidos anteriormente. As entrevistas foram realizadas de forma síncrona (presencial e online) e assíncrona (por correio eletrónico) mediante consentimento informado dos participantes. Cada entrevista síncrona teve uma duração média entre 40 e 60 minutos.

Os dados recolhidos foram submetidos a uma análise de conteúdo, com o objetivo de identificar padrões, convergências e divergências nas perceções dos entrevistados. Este método permitiu interpretar qualitativamente as opiniões e experiências relatadas, contribuindo para uma compreensão dos principais desafios, práticas e níveis de maturidade das entidades portuguesas quanto à implementação da NIS2.

Concluída a descrição da metodologia adotada, procede-se à apresentação e análise dos resultados obtidos. Esta análise pretende interpretar, de forma abreviada, as principais perceções dos participantes sobre o estado de implementação da Diretiva, destacando o nível de conhecimento e adoção, as dificuldades técnicas e organizacionais identificadas, bem como os impactos observados nos processos internos das organizações. Com base nos objetivos definidos, a análise que se segue está organizada de acordo com os quatro temas previstos para as entrevistas, para facilitar a compreensão das perceções dos entrevistados relativamente a cada um deles.

No que respeita ao conhecimento e adoção da Diretiva NIS2, todos os entrevistados reconheceram a importância da Diretiva e a sua relevância para o reforço da cibersegurança. Todavia, o nível de conhecimento e grau de adoção variam consoante o setor e maturidade de cada entidade.

De acordo com as entrevistas, algumas organizações já apresentam um conhecimento consolidado da Diretiva, estando em execução medidas concretas para a implementação dos seus requisitos. É o caso do entrevistado 1, que refere que "a organização tem pleno conhecimento da Diretiva NIS2 e dos seus requisitos". Por outro lado, o entrevistado 2 alega que muitas das organizações ainda se encontram numa fase inicial de implementação da Diretiva, nomeadamente na interpretação dos requisitos e na definição de planos de ação ("muitas organizações já têm consciência da NIS2, mas ainda estão numa fase de interpretação e planeamento").

Na abordagem a esta tema, foi também evidenciada a falta de conhecimento da Diretiva e as suas implicações, por parte das PME, com o entrevistado 3 a afirmar que "as pequenas e médias empresas parecem de alguma forma desprevenidas com o alargamento da abrangência". Em contraste, em entidades com níveis mais elevados de maturidade, como a do entrevistado 5, a adoção da NIS 2 encontra-se num estado bastante avançado ("a organização já se encontra numa fase muito avançada do processo de implementação […] estimando-se que cerca de 95% das ações necessárias estejam concluídas"). O entrevistado 4 sublinha, contudo, a importância da criação de "mecanismos de flexibilidade proporcional", que permitam às organizações de menor dimensão ajustar as exigências da Diretiva às suas capacidades "de modo a não comprometer a sua viabilidade operacional".

De forma global, conclui-se que, apesar do conhecimento generalizado da Diretiva NIS2, a sua implementação ainda é muito escassa, condicionada pelo grau de maturidade em cibersegurança e contexto setorial das organizações.

Relativamente à implementação dos requisitos da Diretiva, as entrevistas revelam diferenças entre as entidades observadas, refletindo diferentes níveis de maturidade. Se por um lado existem organizações com "projetos estruturados (…) com planeamento faseado", com implementação de "gestão de vulnerabilidades" e de "gestão de incidentes" (entrevistado 1), por outro, as áreas com maior progresso são as de "governação (…) e plano de continuidade do negócio" (entrevistado 2). No entanto, persistem desafios significativos, com o entrevistado 3 a identificar a "gestão de terceiros" como um desafio claro para organizações abrangidas pela NIS2, visto que "até ao momento não estavam

abrangidas por uma regulamentação de SI baseada em *standards* de referência". O entrevistado 4 acrescenta que, embora existam avanços significativos, persistem como principais desafios a "contratação e retenção de técnicos especializados em cibersegurança" e a dificuldade das organizações "em compreender e operacionalizar as exigências da NIS2, sobretudo nas áreas de gestão dos riscos, deteção de incidentes e mecanismos de notificação". Por último, o entrevistado 5 realça como principal dificuldade a "vertente organizacional, particularmente ao nível processual e documental", como uma das áreas mais complexas, devido à necessidade de "formalizar procedimentos e atualizar políticas internas".

Quanto aos desafios enfrentados, as dificuldades identificadas distribuem-se principalmente em três áreas: recursos (técnicos, financeiros e humanos), gestão da cadeia de abastecimento e gestão organizacional. A carência de financiamento e de recursos humanos especializados é transversal às organizações ("falta de recursos humanos e financeiros" – entrevistado 3 – e "limitações orçamentais, especialmente em PME", juntamente com a "falta de formação" – entrevistado 2). O entrevistado 1 realça estes desafios, tendo em consideração o investimento financeiro "considerável" que foi necessário fazer, "especialmente em *licensing* de ferramentas especializadas e formação das equipas". Já anteriormente, o entrevistado 4 tinha referido a "dificuldade relacionada com a contratação e retenção de técnicos especializados em cibersegurança" na organização, como um dos principais desafios. Foram ainda destacados desafios relacionados com a complexidade técnica e integração de várias ferramentas e de diferentes fornecedores (entrevistados 1, 2 e 3).

A gestão da cadeia de abastecimento surge como uma preocupação recorrente por causa da diferença do nível de maturidade dos fornecedores (entrevistado 2) e na dificuldade das organizações em gerir esta cadeia (entrevistado 3). O entrevistado 4 defende ainda que que as entidades que não estejam diretamente abrangidas pela Diretiva, e sejam fornecedores das organizações incluídas, é "recomendável que os contratos celebrados com essas organizações incluam cláusulas e evidências relacionadas com boas práticas de cibersegurança, assegurando, assim, um mínimo de conformidade e mitigação dos riscos".

Um dos principais desafios identificados nas entrevistas refere-se à gestão organizacional, nomeadamente, as mudanças culturais e organizativas (entrevistados 1 e 2). Esta perceção é complementada pela análise do entrevistado 5, que indicou como principal obstáculo a "dimensão burocrática associada ao cumprimento das exigências formais" da Diretiva, nomeadamente, "a necessidade de produzir, organizar e validar um volume significativo de documentação e evidencias processuais".

Por último, quanto aos impactos da NIS2 nos processos organizacionais, técnicos e operacionais das organizações, as entrevistas permitiram apurar um impacto estrutural e positivo na maturidade organizacional. No entanto, este impacto também aumentou a complexidade administrativa inerente à implementação de medidas regulamentares.

Durante as entrevistas, ficou evidente o reforço da governação e formalização de políticas de SI nas organizações. O entrevistado 1 referiu a criação de um "Comité de Cibersegurança" e a revisão das "políticas de gestão dos riscos", como ações para o reforço da governação e formalização de políticas de SI. De forma complementar, o entrevistado 2 destacou a necessidade de "rever políticas, redefinir papéis e reforçar a governação de cibersegurança", evidenciando a necessidade de consolidação das práticas internas. O entrevistado 3 observou igualmente uma reestruturação nos "modelos de governo" das organizações com o objetivo de "garantir a integração da SI nos processos fundamentais" internos. Na mesma linha de entendimento, o entrevistado 4 identificou "uma mudança estrutural significativa (…) com as chefias de topo (…) a ter uma responsabilidade acrescida na governação". Por fim, o entrevistado 5 destacou que os processos internos encontram-se agora mais "estruturados e documentados", com a introdução de "mecanismos de monitorização, controlo e reporte", que permitem uma gestão mais eficaz das práticas de cibersegurança.

Três dos entrevistados (1, 2 e 4) realçam a importância das organizações encontrarem um modelo de financiamento sustentável de modo a garantir, a médio e longo prazo, a conformidade, e melhoria contínua, com a NIS2. Partilhando a mesma ideia, o entrevistado 3 identifica as "pequenas e médias empresas no setor privado", como as organizações com maiores dificuldades.

De um modo geral, as entrevistas permitiram evidenciar, de forma transversal, que as organizações encontram-se numa fase de transição entre a consciencialização e a implementação da Diretiva NIS2. As entidades reconhecem a importância da nova Diretiva para garantir um elevado nível comum de segurança das redes e da informação, mas assumem que a concretização prática das medidas necessárias enfrenta limitações de recursos técnicos, financeiros e humanos. Verificou-se que as organizações com um nível de maturidade mais avançado (por exemplo, a organização do entrevistado 5), com sistemas de SI certificados ou equipas internas de cibersegurança dedicadas, encaram a NIS2 como uma oportunidade de reforço da governação e da resiliência operacional. As restantes entidades manifestam preocupação quanto aos recursos e carga administrativa necessária para garantirem a conformidade.

Após a análise dos dados obtidos e a apresentação dos resultados daí subsequentes, torna-se importante apresentar uma reflexão das principais conclusões. O recurso aos inquéritos e entrevistas possibilitou uma compreensão global e aprofundada do grau de maturidade em matéria de cibersegurança das organizações em Portugal, assim como o seu nível de preparação face à implementação da Diretiva NIS2.

A análise quantitativa revelou que a maturidade média das entidades inquiridas encontra-se maioritariamente num nível inicial. Foi ainda possível verificar uma elevada assimetria entre setores de atividade, com destaque para os mais críticos e com maior regulação, que apresentam níveis de maturidade superiores (avançado). Por outro lado, os setores menos críticos e sem regulação específica, apresentam níveis inferiores de maturidade.

Estes resultados mostram que, apesar da consciencialização dos riscos associados à cibersegurança, a generalidade das organizações ainda não consolidou e formalizou as medidas necessárias destinadas a garantir a resiliência e segurança das suas redes e da informação.

Relativamente à análise qualitativa, esta permitiu complementar e contextualizar os resultados obtidos através dos inquéritos, comprovando que as organizações portuguesas ainda se encontram, na sua maioria, numa fase inicial, entre a consciencialização e a implementação dos requisitos da Diretiva NIS2. Também foi possível verificar, através

das entrevistas, que a adoção dos requisitos da Diretiva permanece desigual por culpa de fatores estruturais como a falta de recursos humanos especializados, limitações financeiras e dificuldade da adaptação dos processos internos às novas exigências.

As entrevistas revelaram ainda que as organizações com maior maturidade cibernética encaram esta norma como uma oportunidade de reforço da governação, da gestão dos riscos e da resiliência operacional. Em contrapartida, há entidades que enfrentam dificuldades na formalização de políticas e processos internos com vista a melhorar a sua maturidade em cibersegurança.

A articulação entre os resultados quantitativos e qualitativos corroboram a existência de um panorama heterogéneo, caracterizado por melhorias pontuais, mas ainda longe do objetivo da Diretiva NIS2: garantir um elevado nível comum de segurança das redes e da informação em toda a União.

Concluída a análise integrada dos resultados obtidos, importa refletir sobre as principais limitações que poderão ter condicionado os resultados da presente investigação.

Apesar da relevância dos dados alcançados para os objetivos desde estudo, a análise quantitativa e qualitativa apresenta um conjunto de limitações que importa reconhecer.

Em primeiro lugar, a reduzida dimensão da amostra da investigação quantitativa – composta por apenas 30 respostas válidas – constitui uma condicionante à generalização dos resultados. A fraca taxa de participação, justificada em parte pela opção de algumas organizações em não participar devido à natureza sensível do tema da cibersegurança, resultou igualmente numa distribuição setorial desigual. Cumpre salientar que, apesar da Diretiva NIS2 abranger 18 setores de atividade, as respostas obtidas representam apenas 9 desses setores, correspondendo a 24 das 30 entidades participantes efetivamente abrangidas por esta Diretiva. Ficou a faltar também a identificação da dimensão das entidades inquiridas (PME ou grandes empresas) que permitiria explorar as diferenças de maturidade de acordo com esta caraterística. Por outro lado, embora o *Cybercheckup* seja uma ferramenta oficial disponibilizada pelo CNCS, o seu carácter extenso poderá ter contribuído também para a reduzida taxa de participação.

No âmbito da investigação qualitativa, importa referir o possível enviesamento das respostas e interpretações individuais, decorrente da subjetividade inerente às perceções dos entrevistados. Acresce ainda que, a natureza sensível do tema, poderá ter condicionado o nível de detalhe das respostas partilhadas, devido à necessidade de preservar a confidencialidade da informação das respetivas organizações.

Com base nos resultados obtidos, e nas limitações identificadas ao longo desta investigação, considera-se relevante definir um conjunto de linhas futuras de investigação, que contribuam para aprofundar o conhecimento do nível de maturidade em cibersegurança das organizações, bem como sobre o processo de implementação da Diretiva NIS2 em Portugal.

No âmbito da investigação quantitativa, recomenda-se a ampliação da amostra, de forma a assegurar uma maior representatividade e abrangência dos diferentes setores de atividade. Esta expansão permitirá realizar análises estatísticas mais robustas e comparáveis. Tal como referido anteriormente, será relevante incluir organizações de distintas dimensões, de modo a possibilitar uma análise mais detalhada dos diferentes níveis de maturidade alcançados.

Considera-se, ainda, importante a adoção de uma ferramenta alternativa de avaliação da maturidade em cibersegurança, em complemento ao *Cybercheckup* do CNCS, como por exemplo, a *CyberFundamentals Framework* (*CyFun*)[64], desenvolvida na Bélgica. Esta ferramenta distingue-se do *Cybercheckup* por permitir determinar níveis de maturidade diferentes dentro de cada objetivo de cibersegurança. Adicionalmente, o *CyFun* baseia-se em normas internacionais reconhecidas, como o *NIST,* as ISO/IEC 27001/27002 e os *CIS Controls,* o que lhe confere uma base metodológica sólida, harmonizada e assente em boas práticas globalmente validadas.

No que respeita à análise qualitativa, recomenda-se a utilização de s*oftware* de apoio à análise de dados qualitativos (como NVivo[65]), com vista a reforçar a fiabilidade, a consistência e a sistematização da análise de conteúdo das entrevistas. A aplicação deste

[64] https://cyfun.eu/en
[65] https://nvivo.de/en/

tipo de ferramentas permitirá identificar, de forma mais rigorosa, padrões, relações e temas recorrentes nas perceções dos participantes.

Por último, face aos desafios evidenciados pelas análises quantitativa e qualitativa, quer ao nível de maturidade em cibersegurança, quer na implementação das medidas previstas na Diretiva NIS2, o presente estudo revela-se de particular importância ao propor uma metodologia acessível e orientada para apoiar as entidades na adoção eficaz dos requisitos exigidos.

4. Proposta de metodologia para implementar a NIS2

A Diretiva NIS2 estabelece medidas destinadas a garantir um elevado nível comum de cibersegurança na UE. Este instrumento jurídico representa muito mais do que um simples exercício de conformidade regulamentar, constitui a oportunidade estratégica para as entidades essenciais e importantes, bem como aquelas que, embora não estejam diretamente abrangidas pela Diretiva, pretendem reforçar as suas medidas de cibersegurança. A sua implementação reforça a resiliência das redes e sistemas de informação das organizações e contribui para o aumento da confiança e credibilidade junto dos seus clientes, parceiros e partes interessadas.

Neste contexto, torna-se pertinente a apresentação de uma proposta de metodologia prática e adaptável para a implementação da Diretiva NIS2 em organizações de diferentes setores e dimensões, quer estejam diretamente sujeitas às suas obrigações, quer procurem, voluntariamente, elevar o seu nível de cibersegurança. Pretende-se, assim, fomentar o desenvolvimento ou o reforço das medidas de cibersegurança, de forma a aumentar a resiliência organizacional e a capacidade de proteção contra ciberameaças.

De acordo com um estudo da IDC (*International Data Corporation*), realizado em 2024, 47% das empresas portuguesas inquiridas apresentam pouco ou nenhum conhecimento sobre a Diretiva NIS2. O estudo revela ainda que 38% das organizações estão a par das medidas recomendadas para a gestão de risco, embora admitam não as conhecer em profundidade. Adicionalmente, 60% das emprestas não têm a sua administração envolvida no tema da Diretiva NIS2 ao nível da conformidade, fator que poderá explicar os níveis gerais de falta de preparação identificados.

A metodologia proposta neste estudo está especialmente direcionada para a realidade das PME, que representam a maioria do tecido empresarial em Portugal e que, frequentemente, não dispõe de recursos – financeiros, humanos ou técnicos – para implementar medidas avançadas de cibersegurança (CNCS, 2022b).

Reconhecendo estas limitações, esta metodologia oferece uma abordagem prática, proporcional e acessível, que permite às organizações cumprir os requisitos principais da Diretiva NIS2. Para garantir uma implementação eficaz e ajustada à realidade das PME,

a metodologia proposta está organizada em várias fases interdependentes. Esta abordagem visa ajudar as organizações no percurso para a conformidade, desde a compreensão do enquadramento legal até à adoção das medidas técnicas, operacionais e organizativas adequadas aos requisitos da Diretiva.

4.1. Enquadramento e avaliação da aplicabilidade

A primeira fase desta metodologia centra-se na compreensão do enquadramento da Diretiva e na avaliação da sua aplicabilidade. É uma etapa chave, que permitirá às organizações entenderem o contexto legal, bem como identificar os objetivos, o âmbito e as principais obrigações decorrentes da Diretiva NIS2. Nesta fase, procede-se à análise do setor de atividade, da dimensão e da relevância das organizações, com o objetivo de determinar se estas se enquadram na categoria de entidade essencial ou importante. Este enquadramento jurídico é crucial para verificar se as entidades estão abrangidas pela Diretiva e para avaliar o impacto esperado na sua estrutura organizacional e tecnológica, assim como nos seus processos internos.

Durante esta etapa é fundamental que as entidades compreendam os principais requisitos da Diretiva, uma vez que estes constituem a base para a definição das práticas de cibersegurança a implementar. A Diretiva NIS2 estabelece obrigações claras, incluindo práticas de gestão dos riscos, exigências relacionadas com a segurança da cadeia de abastecimento e procedimentos claros para a resposta e notificação de incidentes. Realça ainda a importância da governação e responsabilidade ao nível da gestão de topo, e incrementa um regime de supervisão e sanções rigoroso, cujo desconhecimento pode resultar em consequências legais e reputacionais significativas para as entidades abrangidas. Torna-se, assim, importante compreender estes requisitos para garantir uma implementação eficaz, coerente e alinhada com as obrigações legais.

Para um melhor enquadramento nacional, é essencial consultar a Lei n.º 59/2025, que autoriza o Governo a transpor a Diretiva (UE) 2022/2555 e que estabelecerá o novo Regime Jurídico da Cibersegurança. Por outro lado, conforme o setor de atividade, deve ser analisada a relação entre a Diretiva NIS2 e outros instrumentos legislativos europeus

complementares, como o Regulamento DORA ou o *Cyber Resilience Act*, de forma a compreender todas as obrigações aplicáveis e potenciais sobreposições regulatórias.

A avaliação inicial constitui, assim, a base para o desenvolvimento de uma estratégia de conformidade proporcional, eficiente e adequada à realidade das organizações.

4.2. Avaliação de capacidades de cibersegurança

Concluído o enquadramento normativo e identificadas as obrigações aplicáveis, será necessário efetuar um diagnóstico inicial da maturidade em cibersegurança. Esta avaliação é fundamental para as organizações compreenderem o estado atual em termos de capacidades, processos, recursos e nível de proteção existente. Este diagnóstico permitirá identificar os pontos fortes e fracos das redes e sistemas de informação das entidades, com impacto na conformidade com a Diretiva NIS2.

Recomenda-se a utilização de referenciais e normas para esta avaliação, nomeadamente a framework de avaliação do *NIST Cybersecurity Framework* (NIST CSF), para garantir um alinhamento com as melhores práticas reconhecidas internacionalmente. Estes *standards* permitem às organizações definir uma base estruturada para a identificação de lacunas e de ações de melhoria contínua.

O objetivo do diagnóstico é avaliar, para cada um dos objetivos da cibersegurança previstos no QNRCS 2019, o seu nível da maturidade: Identificar, Proteger, Detetar, Responder e Recuperar.

A avaliação do objetivo "Identificar" assenta na "compreensão do contexto da organização, dos ativos que suportam os processos críticos da atividade da organização e dos riscos associados relevantes" (CNCS, 2019). Após esta avaliação, é desejável que a entidade consiga definir e priorizar os seus recursos e investimentos de acordo com os seus objetivos gerais e com a sua estratégia de gestão dos riscos.

O objetivo "Proteger" avalia a "implementação de medidas destinadas a proteger os processos organizativos e os ativos da organização, independentemente da sua natureza

tecnológica" (CNCS, 2019). Pretende-se que as organizações definam medidas orientadas à sua proteção nas três dimensões: Pessoas, Processos e Tecnologia.

A avaliação do objetivo "Detetar" assenta na "definição e implementação de medidas destinadas a identificar, de forma atempada, os incidentes" (CNCS, 2019), que possam impactar a segurança das redes e dos sistemas de informação.

Já com a avaliação do objetivo "Responder", pretende-se definir e implementar "medidas de ação apropriadas, em caso de deteção de um incidente" (CNCS, 2019), de forma a reduzir os seus potenciais efeitos adversos nas redes e sistemas de informação das organizações.

Por último, "Recuperar" compreende a "definição e implementação de atividades que visam a gestão de planos e medidas de recuperação dos processos e serviços afetados por um incidente de cibersegurança" (CNCS, 2019). As medidas associadas a este objetivo visam reforçar a resiliência das organizações, assegurando que, em caso de ocorrer um incidente, estas sejam capazes de acionar os mecanismos necessários para reestabelecerem a sua atividade.

A avaliação do grau de maturidade em cada objetivo da cibersegurança irá permitir priorizar ações proporcionais de acordo com o risco associado, evitando investimentos desnecessários e pôr em causa as atividades da organização. Esta avaliação irá contribuir com informação objetiva sobre a maturidade em cibersegurança, que deverá ser utilizada pela administração/direção para suporte à tomada de decisão, nomeadamente, na definição de uma estratégia sustentável para a aplicabilidade dos requisitos da Diretiva NIS2.

Esta análise pode ser efetuada por terceiros ou pelas próprias entidades, através de ferramentas de autoavaliação, como a ferramenta portuguesa *CiberCheckup* (do CNCS) ou a *CyberFundamentals Framework (CyFun)* belga. Existem ainda outras ferramentas que poderão ser utilizadas, como a *ENISA Cybersecurity Maturity Assessment Tool*. Esta autoavaliação possibilita mapear os requisitos da Diretiva com o estado atual das organizações, demonstrando em que áreas são necessárias melhorias ou alterações.

Após a autoavaliação do nível de maturidade em cibersegurança, as entidades devem realizar uma análise de lacunas ("*gap analysis*"), com o objetivo de comparar o estado atual das capacidades existentes com os requisitos exigidos pela Diretiva. Este processo permitirá identificar, de forma clara, os controlos e processos inexistentes ou insuficientemente desenvolvidos, distinguindo os requisitos críticos e obrigatórios das práticas recomendadas. Esta análise irá ainda permitir detetar as áreas que necessitam de melhoria e definir um conjunto de ações proporcionais, servindo de base para a elaboração de um plano de implementação faseado, realista e alinhado com o perfil de risco da organização.

4.3. Definir políticas, responsabilidades e estrutura de governação

Após a avaliação da maturidade em cibersegurança e análise de lacunas, é necessário definir a estrutura organizacional que irá liderar, enquadrar e supervisionar a implementação das medidas de cibersegurança. Nesta fase, serão definidas políticas, responsabilidades e mecanismos de governação que suportam a gestão dos riscos de cibersegurança.

As organizações sem estratégia de segurança implementada devem iniciar a definição e formalização das políticas e responsabilidades internas, que enquadrem a operacionalização das ações previstas. Considera-se, assim, fundamental a elaboração de uma estratégia de segurança da informação assente em políticas simples e ajustadas à realidade das organizações, que contribuam para a proteção dos sistemas e dos dados, e para a gestão dos riscos. Estas políticas deverão apoiar a capacidade de identificar, proteger, detetar e responder aos riscos que ameaçam a SI, bem como recuperar de incidentes que possam comprometer a continuidade das atividades.

Neste sentido, recomenda-se a criação de uma Política de Segurança da Informação, que estabeleça os princípios gerais de proteção, gestão do risco, cumprimento legal, resposta a incidentes, melhoria contínua e promoção de uma cultura de cibersegurança. Em complemento, recomenda-se a definição de uma Política de Utilização Aceitável de Ativos de Informação e de uma Política de Gestão de Identidades e Acessos, que

clarifiquem regras e responsabilidades dos utilizadores e os controlos de acesso aos sistemas.

Para concretizar as políticas recomendadas, é necessário que os processos que as sustentam se traduzam em ações práticas, através de controlos simples e adequados ao contexto das organizações. Adicionalmente, devem ser estabelecidos planos operacionais que definam o que fazer em caso de incidentes, como assegurar a continuidade da atividade e como recuperar o normal funcionamento.

Para executar a estratégia de SI apresentada, e de forma a apoiar o aumento do nível de maturidade em cibersegurança e o cumprimento dos requisitos da Diretiva NIS2, recomenda-se a elaboração de uma matriz que identifique a articulação entre as políticas, os controlos e os planos operacionais adotados, de acordo com os principais referenciais: ISO/IEC 27001, ISO/IEC 27002, NIST 2.0, CIS Controls v8 e QNRCS 2019 (Figura 30).

Fig. 30 - Exemplo de uma matriz de articulação entre as políticas, processos/procedimentos e os planos

Nível	Objetivo	Exemplos	Responsabilidade
Políticas (Governação)	Definir princípios e orientações, de acordo com as especificidades e as necessidades da organização	Política de Segurança da Informação; Política de Utilização Aceitável de Ativos de Informação; Política de Gestão de Identidades e Acessos; Política de Gestão de Risco	Gestão de topo; Responsável pela Segurança da Informação
Processos/Procedimentos (Implementação)	Estabelecer processos e procedimentos claros para executar	Processos: Gestão dos Riscos; Gestão de Incidentes; Gestão de Vulnerabilidades; Gestão de Acessos; Gestão de Ativos; Procedimentos: criação/remoção de contas; revisão de privilégios; aplicação de *patchs* e atualizações; monitorização de eventos; execução de *backups* ; implementação de MFA	Equipas técnicas; Predadores de Serviços; Responsável pela Segurança da Informação; Responsávceis Operacionais
Planos (Operação e Continuidade)	Definir procedimentos para resposta, recuperação e comunicação, em caso de incidente grave	Plano de Resposta a Incidentes; Plano de Recuperação de Desastres; Plano de Continuidade de Negócio; Plano de Comunicação de Incidentes	Equipas operacionais; Equipa de gestão de incidentes; Equipa de Comunicação; Responsável pela Segurança da Informação

Fonte: elaboração própria, 2025

Para uma operacionalização desta matriz é necessária uma estrutura de governação clara, com responsabilidades bem definidas nas organizações. A implementação de políticas de segurança da informação pressupõe, numa fase inicial, a nomeação formal de um responsável pela SI, frequentemente designado *Chief Information Security Officer* (CISO), ou função equivalente. Esta designação é essencial para definir competências e responsabilidades, garantir liderança e coordenação das iniciativas de segurança e assegurar a ligação entre a estratégia definida pela Administração e a execução

operacional das medidas. Compete ao responsável pela SI orientar, implementar, manter e supervisionar as políticas de segurança, promovendo a sua melhoria contínua.

Paralelamente, torna-se indispensável a definição clara dos papéis e responsabilidades de todos os intervenientes, assegurando que cada utilizador compreende o seu contributo para a SI. A Diretiva NIS2 reforça esta necessidade, ao atribuir responsabilidades explícitas aos órgãos de gestão, exigindo uma postura ativa na aprovação e monitorização das medidas de gestão dos riscos de cibersegurança. Só uma governação sólida garante os recursos necessários para a implementação dos processos de SI.

Para apoiar as organizações na definição de funções e responsabilidades de cada interveniente, recomenda-se a adoção de uma matriz RACI (*Responsible, Accountable, Consulted, Informed*) (Figura 31). Note-se que a matriz apresentada é um exemplo simplificado, devendo ser adaptada ao contexto, dimensão, estrutura organizacional, recursos e às necessidades e particularidades de cada organização.

Esta matriz permite estabelecer, delimitar e formalizar as funções que cada elemento tem na implementação das medidas, melhorando a comunicação e tomada de decisão.

Fig. 31 - Exemplo de uma matriz RACI

Tarefa/Processo	Responsible (Executa)	Accountable (Aprova)	Consulted (Apoio técnico/funcional)	Informed (Comunicado)
Aprovação da Política de Segurança da Informação	Responsável da Segurança da Informação (CISO)	Administração / Direção	Serviços Jurídicos; TI	Todos os colaboradores
Gestão de Acessos	Equipa de TIC	Responsável da Segurança da Informação (CISO)	Recursos Humanos; Responsáveis de departamentos	Utilizadores afetados
Resposta a Incidentes	Equipa de Resposta a Incidentes	Responsável da Segurança da Informação (CISO)	Equipa de TIC; Serviços jurídicos; Comunicação	Administração / Direção e utilizadores afetados
Manutenção do Plano de Continuidade	Equipa de TIC	Administração / Direção; Responsável da Segurança da Informação (CISO)	Donos dos Processos	Toda a organização

Fonte: elaboração própria, 2025

Desta forma, a metodologia proposta reforça a necessidade de adoção de políticas, processos, procedimentos e planos operacionais simples, que devem ser complementados por mecanismos de governação claros, liderados pelos órgãos de gestão das organizações,

conforme previsto na Diretiva. Estes devem aprovar as medidas de gestão dos riscos de cibersegurança e supervisionar a sua aplicação.

A adoção de políticas e atribuição de responsabilidades não se limita a um requisito administrativo, mas sim ao desenvolvimento da estrutura governativa da cibersegurança. De acordo com os principais referencias internacionais – ISO/IEC 27001:2022, NIST 2.0 – sem uma governação forte, sem liderança ou responsabilização, os processos e os controlos técnicos perdem eficácia e não é assegurada a melhoria contínua. A governação funciona como o eixo central da cibersegurança, definindo as prioridades e assegurando a sustentabilidade das medidas de segurança adotadas.

As políticas de segurança, e os documentos que as complementam, não implicam necessariamente processos de certificação. No entanto, a sua definição deve ser baseada em normativos de referência, tais como a família das ISO/IEC 27000, o NIST, o CIS *Controls* ou o QNRCS.

Para as organizações mais maduras em termos de cibersegurança, aconselha-se a implementação de um Sistema de Gestão de Segurança da Informação, com base nas normas internacionais reconhecidas, como a ISSO/IEC 27001, que estabelece os princípios gerais que devem ser aplicados aos ativos de suporte, nomeadamente servidores, sistemas de informação, redes, infraestruturas, entre outros.

No âmbito da Diretiva NIS2, a implementação de uma estratégia de segurança da informação irá, assim, permitir a garantia da confidencialidade, integridade e disponibilidade dos sistemas de informação e dos dados. Esta abordagem implica a implementação de um sistema de gestão dos riscos, a identificação e mitigação de ameaças e vulnerabilidades, e o cumprimento dos requisitos legais aplicáveis em matéria de cibersegurança. Adicionalmente, a estratégia de segurança da informação deve incluir a definição de processos de deteção, gestão e resposta a incidentes, bem como a promoção da melhoria continua através de avaliações regulares, auditorias internas e revisões periódicas.

A implementação de uma estratégia de SI constitui um passo fundamental para garantir a segurança das redes e da informação e, consequentemente, para reforçar nível de cibersegurança das organizações.

Após definir as políticas e responsabilidades, é necessário assegurar que esta estratégia se traduz em práticas concretas, através da implementação de controlos técnicos, operacionais e organizativos adequados.

4.4. Implementar medidas de gestão dos riscos

No seguimento da análise de lacunas e identificação das necessidades de melhoria face aos requisitos da Diretiva NIS2, o passo seguinte consiste em estabelecer um processo sistemático e estruturado com a priorização das medidas a implementar com base no risco e contexto organizacional[66]. A inexistência deste instrumento pode resultar em decisões baseadas maioritariamente em critérios *ad-hoc* ou perceções subjetivas, o que dificulta a justificação, a rastreabilidade e o alinhamento com os objetivos estratégicos das organizações.

Com o intuito de reforçar a aplicabilidade prática da metodologia proposta, propõe-se a integração de uma matriz de prioridades que irá permitir às organizações avaliar cada medida identificada de acordo o seu impacto e esforço necessário para a sua aplicação (Figura 32).

Fig. 32 – Exemplo de uma matriz de prioridades

Impacto/Esforço	Baixo	Médio	Elevado
Elevado	Implementação imediata	Prioridade elevada	Avaliar riscos de cibersegurança e não conformidade
Médio	Prioridade moderada	Programar a médio prazo	Considerar apenas se alinhada com estratégia da organização
Baixo	Implementar apenas se integrado noutras iniciativas	Prioridade baixa	Programar a longo prazo

Fonte: elaboração própria, 2025

[66] ISO/IEC 27005:2022, NIST CSF 2.0, CIS Controls v8 e QNRCS

Entende-se como impacto, o contributo esperado da medida para a redução do risco e para o cumprimento dos requisitos de conformidade aplicáveis, enquanto o esforço reflete os recursos financeiros, técnicos e humanos necessários para a sua implementação, incluindo o tempo de execução.

A matriz de prioridades é um instrumento simples e replicável que irá permitir às organizações identificarem as medidas mais importantes, ou seja, aquelas que poderão proporcionar um ganho significativo com um esforço de implementação reduzido ou moderado.

A priorização das medidas garante uma implementação mais objetiva, transparente e ajustável à realidade organizacional. Este processo terá um impacto muito grande na otimização dos recursos, principalmente em organizações com capacidades limitadas, permitindo uma implementação faseada das medidas de cibersegurança, alinhada com o nível de risco de cada organização. Este processo de priorização permite ainda aumentar a aplicabilidade da metodologia e reforçar a sua adoção, principalmente em entidades com uma baixa maturidade em cibersegurança.

Para garantir que as medidas adotadas estão alinhas e priorizadas com os objetivos estratégicos das organizações, recomenda-se a integração deste processo no modelo de Gestão de Riscos Empresarial (*Enterprise Risk Management* – ERM) existente ou, no caso de não haver, a criação de um. O ERM está vocacionado para identificar e gerir os riscos de uma empresa, proporcionando benefícios significativos quando comparado a estratégias isoladas de gestão dos riscos. Este instrumento permite uma visão transversal dos riscos, considerando não apenas o impacto técnico, mas também os efeitos operacionais, financeiros, legais e reputacionais. Com a aplicação do ERM, a cibersegurança deixar de ser vista como um tema exclusivamente tecnológico, passando a ser reconhecida como um risco organizacional e estratégico. Este alinhamento permite às organizações tomar decisões de investimento mais consistentes, de acordo com as prioridades, garantindo a sustentabilidade e melhoria contínua das medidas de gestão dos riscos adotadas.

Deste modo, concluída a fase de definição de prioridades, inicia-se a fase de implementação faseada das medidas. Esta fase é muito importante, pois traduz a transposição prática da Diretiva NIS2 para a realidade das organizações. Nesta etapa, as organizações vão implementar as medidas de gestão dos riscos de acordo com as prioridades definidas anteriormente. Estas devem começar por iniciativas de elevado impacto na segurança das redes e da informação, e de baixo custo, para obter melhorias imediatas, em vez de tentar cumprir todos os requisitos previstos na Diretiva NIS2. Estas medidas devem ser proporcionais à complexidade, dimensão e grau de exposição aos riscos das organizações. Assim, as entidades críticas e com maior dependência tecnológica – entidades essenciais – deverão adotar mecanismos mais robustos, enquanto que as entidades menos críticas – entidades importantes – deverão adotar medidas mais simples, desde que eficazes.

Para apoiar a implementação destas medidas, as organizações podem recorrer às diretrizes e boas práticas presentes nas normas e referenciais nacionais e internacionais reconhecidos, como a ISO/IEC 27001, o NIST, os CIS *Controlos*, as orientações da ENISA e o QNRCS. Estes referenciais fornecem orientações práticas, exemplos de evidências e mapeamentos que facilitam a correspondência entre os requisitos da Diretiva NIS2 e as boas práticas de segurança da informação. Importa referir que o mapeamento efetuado por estes referenciais não implica o cumprimento automático dos requisitos da Diretiva, mas funcionam como instrumentos que servem como ferramentas de alinhamento com a conformidade.

As medidas a implementar devem abranger as três dimensões fundamentais dos sistemas de informação – processos, pessoas e tecnologia – e contemplar as seguintes medidas de gestão dos riscos de cibersegurança exigidos na Diretiva:

- política de segurança dos sistemas de rede e de informação;
- política de gestão dos riscos;
- gestão de incidentes;
- continuidade de negócio e gestão de crises;
- segurança da cadeia de fornecimento;

- segurança na aquisição, desenvolvimento e manutenção de sistemas de rede e de informação;
- políticas e procedimentos para avaliar a eficácia das medidas;
- práticas básicas de higiene digital e formação em segurança;
- procedimentos relativos à utilização de criptografia e cifragem;
- segurança de recursos humanos;
- controlo de acessos;
- gestão de ativos;
- utilização de autenticação multifator (MFA) e comunicações seguras;
- segurança ambiental e física.

A conformidade com a Diretiva NIS2 não se limite às atividades internas das organizações por ela abrangidas. Importa salientar que uma das medidas com maior impacto nacional é a imposição de obrigações aos fornecedores críticos, de forma a salvaguardar que a segurança dos sistemas e da informação seja tratada em toda a cadeia de abastecimento. Esta nova abordagem, que não existia na Diretiva NIS, introduz desafios adicionais para as organizações, na medida em que irá implicar a revisão dos processos de seleção e contratação de fornecedores, de modo a assegurar a proteção das redes e da informação contra ciberameaças que possam surgir por via destes parceiros. Na prática, significa que as entidades essenciais e importantes têm de estender as obrigações aos seus fornecedores, mesmo que não sejam entidades abrangidas pela Diretiva NIS2, uma vez que estas constituem uma extensão dos seus serviços.

Tendo em consideração a amplitude e complexidade dos requisitos previstos na Diretiva, optou-se por não identificar, neste estudo, os processos específicos associados à implementação de cada medida prevista, uma vez que tal exercício implicaria um nível de especificidade operacional que varia consoante o contexto, setor e maturidade de cada organização. No entanto, como base de orientação, e sem necessidade de recorrer a certificações, recomenda-se que estas medidas sejam alinhadas com referências reconhecidos, como as ISO/IEC 22301, 27001, 27002, 27005, o NIST 2.0, os CIS Controls v8 e o QNRCS 2019.

4.5. Elaborar planos de resposta a incidentes e continuidade do negócio

Após a implementação das medidas técnicas, operacionais e organizativas, torna-se necessário garantir que as organizações estão preparadas para responderem de forma eficaz a incidentes de segurança e a interrupções das suas operações. Para tal, é indispensável a elaboração de Planos de Resposta a Incidentes (PRI) e de Continuidade do Negócio (PCN), que assegurarem a resiliência operacional e a recuperação dos processos críticos das organizações. Estes planos devem ser claros, simples e fáceis de seguir e implementar, ajustados à dimensão e realidade das organizações. O PRI deve estabelecer procedimentos claros e bem documentados para detetar, analisar, conter, mitigar e recuperar de incidentes de segurança. Deve ainda definir os papéis e responsabilidades, garantindo uma resposta rápida, eficaz e coordenada.

A resposta a incidentes deve ser complementada por medidas de continuidade do negócio, que assegurem a manutenção, ou o restabelecimento rápido das atividades essenciais. Neste âmbito, as entidades devem desenvolver dois instrumentos fundamentais: o PCN, que define a estratégia e procedimentos para manter ou recuperar processos essenciais, e o Plano de Recuperação de Desastres (PRD), que estabelece ações específicas para restaurar sistemas e infraestruturas tecnológicas.

Estes planos devem identificar critérios de ativação e procedimentos operacionais, permitindo preparar as organizações para lidar com diferentes tipos de incidentes, incluindo ataques cibernéticos (ex.: *ransomware*, *phishing*, ataques DDoS), falhas de *hardware* ou *software*, erros humanos (intencionais ou acidentais), bem como eventos naturais ou acidentais (ex.: terramotos, inundações, incêndios).

A existência de um PCN e de PRD contribui para reduzir o tempo de recuperação, mitigar os impactos financeiros decorrentes da interrupção da atividade e diminuir os riscos legais e reputacionais associados a incidentes significativos.

Contudo, a eficácia destes planos depende da realização de testes periódicos e da sua atualização sempre que ocorram alterações organizacionais, tecnológicas ou processuais. Estes exercícios formais servem para assegurar que as equipas compreendem e conseguem executar os procedimentos definidos.

A implementação do PCN e do PRD pode ser orientada por referenciais reconhecidos, como a ISO/IEC 22301, que estabelece o sistema de gestão de continuidade do negócio, ou o NIST SP 800-34, que fornece orientações práticas para a recuperação de sistemas de informação.

Adicionalmente, importa assegurar o cumprimento das obrigações de reporte previstas na Diretiva NIS2, perante a ocorrência de incidentes significativos. Sempre que ocorra um incidente, as entidades abrangidas devem notificar, sem demora injustificada, a CSIRT, ou, quando aplicável, a autoridade competente. Considera-se um incidente significativo aquele que cause, ou possa vir a causar, graves perturbações operacionais, perdas financeiras significativas ou impactos substanciais sobre outras entidades ou indivíduos.

Assim, as entidades essenciais e importantes devem elaborar um plano formal de resposta a incidentes, que inclua procedimentos de notificação interna e externa, garantindo o cumprimento dos prazos e exigências definidos na Diretiva NIS2.

4.6. Monitorização e melhoria contínua

A implementação das medidas previstas na Diretiva NIS2 não deve ser entendida como um exercício pontual, orientada apenas para a conformidade, mas como um processo dinâmico e contínuo de gestão de cibersegurança. A monitorização e revisão sistemática das medidas adotadas constituem um requisito da Diretiva e visam garantir que estas se mantêm eficazes e alinhadas com o nível real de risco das organizações, assegurando a melhoria contínua da postura de cibersegurança e a resiliência operacional.

De forma a avaliar o grau de implementação da metodologia proposta, recomenda-se a utilização de indicadores de desempenho (*Key Performance Indicator* – KPI) focados no progresso (Figura 33). Através destes KPI será possível monitorizar as ações previstas, assegurando que as organizações evoluem no nível de maturidade de cibersegurança de forma estruturada e proporcional ao seu contexto.

Fig. 33 - Exemplo de KPI para monitorizar a implementação da metodologia proposta

Fase da Metodologia	Indicador (KPI)	Como é medido	Interpretação
Enquadramento e conformidade	KPI 1: Determinação do enquadramento legal concluída	Sim / Não	Verificar se a organização sabe se é essencial, importante ou fora de âmbito.
Diagnóstico de maturidade	KPI 2: Grau de conclusão da análise de lacunas	Nº áreas avaliadas / Nº total de áreas previstas	Garantir que a autoavaliação foi realizada integralmente.
Priorizar medidas	KPI 3: Matriz de prioridades aplicada	Sim / Não	Confirmar que existe priorização objetiva das ações.
Definição de políticas	KPI 4: Percentagem de políticas aprovadas pela gestão	Nº políticas aprovadas / Nº políticas previstas	Avaliar o comprometimento da administração.
Definição de responsabilidades	KPI 5: RACI formalmente adotada	Sim / Não	Verificar clareza de papéis e responsabilidades.

Fonte: elaboração própria, 2025

Os KPI a definir devem ser simples, mensuráveis, baseados em evidências documentais e permitir acompanhar a implementação da metodologia, garantindo que os requisitos da Diretiva NIS2 estão a ser gradualmente incorporados nas práticas da organização.

Paralelamente, deverão ser desenvolvidos KPI para monitorizar o avanço da implementação das medidas de gestão dos riscos de cibersegurança previstas, para assegurar que as entidades estão alinhadas com os requisitos da Diretiva (Figura 34).

Fig. 34 - Exemplo de KPI para monitorizar a implementação das medidas de gestão dos riscos de cibersegurança

Área	Indicador (KPI)	Como é medido	Interpretação
Governação	Percentagem de políticas aprovadas pela Administração	Nº de políticas aprovadas / Nº de políticas previstas	Verifica se a governação apoiou formalmente a estratégia
Responsabilidades	Existência de RACI formalmente adotada	Sim / Não	Clarifica papéis e evita lacunas de responsabilidade
Gestão do risco	Existência de análise de riscos	Sim / Não	Demonstra maturidade no processo de avaliação do risco
Controlo de acessos	Percentagem de contas com revisão periódica efetuada	Nº de contas revistas / Nº total de contas	Avalia o princípio do menor privilégio
Continuidade de negócio	Grau de implementação do PCN/PRD	Escala simples (Não iniciado / Em desenvolvimento / Concluído / Testado)	Avalia a progressão faseada
Formação	Percentagem de colaboradores sensibilizados	Nº formados / Nº total de colaboradores	Mede evolução da cultura de cibersegurança

Fonte: elaboração própria, 2025

A utilização de KPI na implementação desta metodologia permite avaliar o seu progresso de forma objetiva e garantir que as decisões tomadas durante a sua execução baseiam-se em dados concretos. A utilização destes instrumentos permitirá melhorar continuamente os processos, assegurando o alinhamento com os objetivos organizacionais.

Como reforço da proposta para a avaliação, monitorização e melhoria contínua da conformidade com os requisitos da Diretiva NIS2, recomenda-se a adoção de uma framework internacionalmente reconhecida. Apesar de existirem algumas recomendas, propõe-se a utilização da NIST 2.0 por reunir as três dimensões da monitorização – avaliação, controlo e melhoria contínua – permitindo uma governação estruturada e sustentada da segurança das redes e da informação. A utilização deste instrumento permite fornecer uma abordagem harmonizada no planeamento, implementação e avaliação contínua das medidas de cibersegurança, permitindo o acompanhamento da sua eficácia ao longo do tempo.

4.7. Formação e cultura de cibersegurança

No âmbito da Diretiva NIS2, a formação em cibersegurança não deve ser entendida como uma necessidade de cumprimento legal, mas como um elemento essencial para a resiliência, mitigação dos riscos e segurança das redes e da informação. Mais do que uma mera obrigação, a capacitação contínua dos colaboradores deve ser encarada como uma prática natural e inerente à cultura das próprias organizações.

Desta forma, é importante criar programas de formação e sensibilização sobre cibersegurança, com o objetivo de aumentar a consciencialização organizacional de todas as partes envolvidas.

A eficácia destes programas só é assegurada se estes forem contínuos e ajustados ao perfil e responsabilidades dos utilizadores. Deverá, ainda, ser garantida a integração destas campanhas nos processos internos das organizações, nomeadamente, no acolhimento de novos funcionários, na gestão de acessos e na revisão periódica de funções.

A obrigatoriedade de formação em cibersegurança está bem patente na Diretiva NIS2, com o reforço do papel da Administração na promoção ativa de uma cultura de

cibersegurança, devendo esta acautelar os recursos necessários parta a sua implementação.

Para estas iniciativas produzirem resultados sustentáveis é essencial avaliar o seu impacto através de KPI. Esta monitorização contínua permite identificar níveis de adesão, medir e evolução do comportamento organizacional face ao risco e ajustar conteúdos e formatos das ações de formação e sensibilização (Figura 35).

Fig. 35 - Exemplo de KPI para monitorizar formação em cibersegurança

Área avaliada	Indicador (KPI)	Como é medido	Interpretação
Participação	KPI 1: Percentagem de colaboradores que concluíram a formação obrigatória	Nº colaboradores formados / Nº total de colaboradores	Avalia o grau de cobertura da formação dentro da organização
Frequência	KPI 2: Frequência média de ações de formação em cibersegurança	Nº de ações de formação em cibersegurança realizadas por ano	Verifica se a formação é contínua e integrada no tempo, e não pontual ou reativa
Adequação por Função	KPI 3: Taxa de conclusão da formação específica por perfil de risco	Nº colaboradores críticos formados / Nº total de colaboradores críticos	Assegura que funções mais expostas ao risco recebem formação adequada
Eficácia	KPI 4: Taxa média respostas corretas em testes pós-formação	Pontuação média dos questionários pós-formação	Verifica se os conteúdos foram compreendidos de forma prática
Cultura Organizacional	KPI 5: Percentagem de incidentes associados a erro humano	Nº incidentes atribuídos a falha humana / Nº total de incidentes	Mede evolução da cultura e eficácia da sensibilização

Fonte: elaboração própria, 2025

Considerando que o fator humano figura entre as três principais ameaças à cibersegurança (ENISA, 2024), é fundamental que as organizações apostem em formação. Deste modo, é crucial que as organizações invistam não apenas em tecnologia – *software* e *hardware* – para garantir a SI, mas também na formação dos seus funcionários para reforçar a postura de cibersegurança das organizações e para mitigar os riscos associados ao comportamento humano.

Paralelamente, a formação em cibersegurança tem um impacto transformador nos colaboradores, promovendo comportamentos mais seguros, reduzindo as vulnerabilidades humanas e contribuindo de forma significativa para a ciber-resiliência organizacional.

4.8. Considerações finais

A metodologia proposta neste estudo procura oferecer um plano estruturado, progressivo e proporcional para a implementação da Diretiva NIS2, permitindo que as organizações com diferentes níveis de maturidade reforcem a sua resiliência e capacidade de gestão dos riscos de cibersegurança. A aplicação desta metodologia contribui, assim, para a promoção de um elevado nível de segurança das redes e dos sistemas de informação, bem como para o cumprimento das obrigações legais decorrentes da Diretiva.

Importa referir que esta abordagem não procede ao mapeamento exaustivo entre cada requisito da Diretiva e os controlos previstos nos referenciais reconhecidos (como a ISO/IEC 27001, o NIST 2.0, os CIS *Controls* ou o QNRCS 2019), uma vez que tal exercício requerer um nível de especificidade operacional ajustado ao setor, à dimensão organizacional, ao perfil de risco e ao nível de maturidade pré-existente de cada organização.

No entanto, considera-se que a metodologia apresentada constitui uma base orientadora robusta para apoiar as organizações na aplicação faseada e proporcional dos requisitos da Diretiva NIS2, promovendo a evolução contínua da maturidade em cibersegurança e contribuindo para o reforço da resiliência digital das organizações.

5. Conclusões

Vivemos hoje numa realidade profundamente dependente das TIC, com destaque para as digitais. As tecnologias emergentes como a IA, *big data*, IOT, computação na nuvem, ML, entre outras, têm impulsionado a TD das sociedades e organizações, transformando significativamente a forma como interagimos, comunicamos, acedemos à informação e trabalhamos. As tecnologias digitais têm tido um impacto relevante em áreas como a saúde, a educação, o turismo ou os transportes. É correto afirmar que a utilização das TIC promove o desenvolvimento das sociedades, ao mesmo tempo que melhoram a qualidade de vida das pessoas (Nevado-Peña, D., López-Ruiz, V., Alfaro-Navarro, J., 2019).

No entanto, a TD acarreta também novos desafios, sobretudo no que diz respeito à proteção e segurança dos sistemas de informação contra ciberameaças, que podem resultar em graves consequências, incluindo interrupção de atividades, perdas financeiras e danos reputacionais (Sharma, R., 2012).

Foi neste contexto de insegurança no espaço digital que a UE aprovou a Diretiva (UE) 2022/2555, com o objetivo de melhorar a segurança das redes e sistemas de informação no espaço europeu. O presente estudo surge como resposta a esta Diretiva, que tem como principal objetivo apresentar uma metodologia prática para a sua implementação.

Concluídas as fases desta investigação, serão apresentadas de seguida as conclusões, limitações à investigação e propostas de pesquisa futuras.

5.1. Conclusões da Investigação

A crescente dependência das tecnologias expõe as organizações a ciberameaças, cada vez mais frequentes e sofisticadas. A revisão da literatura evidencia que a TD e a evolução das TIC alteraram profundamente o funcionamento das sociedades e das organizações. Identificou-se, por um lado, o papel determinante destas tecnologias no desenvolvimento económico e social e, por outro, a contribuição para o surgimento de novos riscos e vulnerabilidades no ciberespaço.

A análise conceptual realizada permitiu esclarecer os conceitos de SI, proteção de dados e cibersegurança que, embora intimamente relacionados, possuem âmbitos e finalidades distintas, com destaque para a cibersegurança, o tema principal desta investigação.

Nos últimos anos, a UE tem vindo a consolidar o seu quadro jurídico com o objetivo de reforçar as capacidades de cibersegurança dos EM, por via da adoção de regulamentos e diretivas. Em resposta ao aumento da exposição da União às ciberameaças, foi aprovada a Diretiva NIS2, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança, substituindo a sua antecessora, a Diretiva 2016/1148.

No plano nacional, Portugal tem desenvolvido gradualmente a sua estratégia de cibersegurança, alinhando-a com as normas europeias, nomeadamente através da transposição e implementação da Diretiva NIS2, do RGPD, do Regulamento DORA, do Regulamento de Cibersolidariedade, entre outros instrumentos. Este enquadramento normativo evidencia o esforço conjunto, europeu e nacional, para reforçar a resiliência digital das organizações.

No entanto, os relatórios mais recentes da ENISA e CNCS sobre cibersegurança demonstram que a evolução tecnológica tem sido acompanhada por um aumento contínuo da frequência, sofisticação e impacto dos ciberataques, com especial incidência do *phishing*, na engenharia social, no *ransomware*, dos ataques DDoS e da exploração de vulnerabilidades.

Perante este cenário de ameaça crescente, e considerando que o objetivo desta investigação é desenvolver uma metodologia simples para apoiar as organizações na implementação da Diretiva NIS2, foi fundamental compreender os seus principais objetivos e requisitos. Importa salientar que a NIS2 é uma evolução da NIS, por esta não conseguir assegurar adequadamente a proteção das ameaças cibernéticas crescentes. Assim, a nova Diretiva estabelece requisitos mais rigorosos e promove um nível mais elevado de cibersegurança, abordando áreas como gestão dos riscos, monitorização, segurança da cadeia de fornecedores, notificação de incidentes e responsabilização dos órgãos de gestão. Adicionalmente, introduz um regime sancionatório, com o objetivo de

garantir o cumprimento das obrigações de cibersegurança por parte das entidades abrangidas.

Neste contexto, tornou-se essencial realizar uma avaliação do nível de maturidade e do grau preparação das organizações, de modo a permitir, numa etapa subsequente, desenvolver uma metodologia adequada para a implementação da NIS2. Esta avaliação assentou em duas abordagens distintas, mas complementares, combinando métodos quantitativos (inquéritos) e qualitativos (entrevistas). Através desta avaliação foi possível caracterizar tanto o nível de maturidade em cibersegurança, como o grau de preparação das organizações para o cumprimento dos requisitos da Diretiva NIS2.

Os resultados dos inquéritos demonstram uma heterogeneidade significativa das entidades avaliadas. Os setores mais regulados e críticos – como a energia, as infraestruturas digitais e o setor bancário – apresentam níveis de maturidade mais elevados, enquanto que os setores com menor pressão regulatória – como a administração pública, a gestão de resíduos e a investigação – revelam níveis de maturidade substancialmente inferiores. As entrevistas realizadas com especialistas em cibersegurança confirmam igualmente uma assimetria no grau de conhecimento sobre a NIS2, sendo maior em entidades com maturidade superior. Foi igualmente possível constatar que, apesar da Diretiva ter sido publicada em dezembro de 2022, a maioria das organizações ainda se encontra numa fase intermédia entre a consciencialização e a implementação desta norma. As entrevistas revelaram ainda que os principais desafios identificados pelas entidades incluem a falta de recursos humanos especializados, as limitações financeiras, a complexidade técnica e a diversidade da cadeia de fornecedores.

As análises conceptual, quantitativa e qualitativa serviram de base para o desenvolvimento de uma metodologia simples e adaptável, concebida para apoiar as organizações na transposição efetiva dos requisitos da NIS2, especialmente orientada para a realidade das PME. A metodologia foi estruturada em sete fases, organizadas de acordo com uma sequência lógica de execução. Importa salientar que a metodologia proposta constitui uma recomendação orientadora, sendo que, a implementação de cada etapa dependerá do nível de maturidade em que a organização se encontra.

Esta abordagem pretende garantir que a implementação da Diretiva seja proporcional e sustentável, garantindo que as entidades progridem de forma gradual, alinhando os investimentos necessários com o seu perfil de risco, dimensão e grau de maturidade.

Esta metodologia pretende ser um instrumento de apoio às organizações portuguesas na interpretação e implementação da Diretiva NIS2, contribuindo para aumentar o nível comum de cibersegurança a nível nacional.

5.2. Limitações associadas à investigação

Na elaboração deste estudo foram identificadas algumas limitações que importa reconhecer, embora nenhuma tenha comprometido o objetivo proposto.

A principal limitação está relacionada com a Lei n.º 59/2025, que autoriza o Governo a transpor a Diretiva (UE) 2022/2555 para o ordenamento jurídico nacional. No momento em que esta Lei foi aprovada, o estudo já estava praticamente concluído, inviabilizando a inclusão da respetiva análise, em particular no que respeita à concretização nacional das obrigações previstas pela NIS2.

Outra limitação prende-se com a enixistência de estudos sobre a aplicação da Diretiva NIS2 em PME, principalmente em Portugal. Tal deve-se à atualidade do tema e ao facto de muitos EM ainda não terem transposto a Diretiva.

Relativamente à avaliação do nível de maturidade em cibersegurança das organizações, a dimensão da amostra é relativamente reduzida, o que limita a generalização dos resultados a todo o universo de entidades abrangidas pela NIS2 em Portugal. Esta fraca adesão afetou igualmente a distribuição setorial, não sendo possível representar todos os 18 setores abrangidos, o que pode introduzir enviesamentos na leitura dos resultados.

Acresce que não foi possível identificar, de forma sistemática, a dimensão das organizações inquiridas, o que impossibilitou uma análise diferenciada da maturidade em função da dimensão organizacional. Esta limitação torna-se particularmente relevante neste estudo, dado que a Diretiva NIS2 utiliza este critério para definir o âmbito de aplicação.

Importa ainda referir o número reduzido de entrevistas realizadas. Apesar da qualidade e diversidade dos entrevistados, as perceções recolhidas refletem opiniões pessoais, suscetíveis de enviesamentos das respostas. A sensibilidade do tema poderá igualmente ter condicionado o nível de detalhe fornecido, com possíveis resultados desfasados da realidade.

Por fim, a metodologia proposta, ainda que seja fundamentada em literatura, referenciais reconhecidos e nos resultados empíricos obtidos, esta não foi objeto de aplicação nem de validação por especialistas. Assim, a sua eficácia prática e o respetivo impacto na evolução da maturidade em cibersegurança das organizações carecem de confirmação empírica futura.

Apesar das limitações não invalidarem os resultados obtidos, estas demonstram a necessidade de investigação complementar futura, com amostras maiores, análises mais granulares e validação prática da metodologia proposta.

5.3. Recomendações para futuras investigações

Tendo em consideração os resultados alcançados e as limitações identificadas ao longo do estudo, considera-se importante apresentar um conjunto de recomendações e de linhas de investigação futura. Estas sugestões poderão contribuir para aprofundar o conhecimento sobre a implementação da NIS2 e para reforçar a maturidade em cibersegurança das organizações nacionais.

A primeira recomendação refere-se à avaliação do nível de maturidade em cibersegurança através de questionários. Sugere-se que este instrumento seja atualizado de forma a incorporar todas as dimensões relevantes da cibersegurança, incluindo a dimensão organizacional e governação.

Para avaliar a eficácia da metodologia proposta, recomenda-se a aplicação em organizações de diferentes dimensões e setores para recolher contributos e, assim, ajustar e melhorar este instrumento.

Outra recomendação diz respeito ao estudo das alterações introduzidas na legislação portuguesa, na sequência da transposição da NIS2 através da Lei n.º 59/2025, e à revisão da metodologia de acordo com essas alterações. Só desta forma será possível assegurar o alinhamento da metodologia com o enquadramento jurídico nacional, permitindo uma melhor aplicabilidade nas organizações nacionais. Será também interessante aplicar este estudo num momento posterior à entrada em vigor do novo Regime Jurídico de Cibersegurança, de forma a avaliar o impacto efetivo da transposição da NIS2 na maturidade em cibersegurança das organizações e no funcionamento do mercado nacional.

Bibliografia

Admass, W., Munaye, Y., Diro, A. (2024). *Cyber security: State of the art, challenges and future directions. Cyber Security and Applications*. Volume 2.100031. ISSN 2772-9184. https://doi.org/10.1016/j.csa.2023.100031.

Alves, D. (2021). O papel fundamental da Cibersegurança na Proteção de Dados Pessoais. Anuário da Proteção de Dados. Observatório da Proteção de Dados Pessoais. CEDIS/NOVA School of Law

Amoo, O., et al. (2024). *GDPR's impact on cybersecurity: A review focusing on USA and European practices*. International Journal of Science and Research Archive. 11. 1338-1347. 10.30574/ijsra.2024.11.1.0220.

Andersson, A., Hedström, K., Karlsson, F. (2022). *Standardizing information security – a structurational analysis*. Information & Management. Volume 59, Issue 3. 103623. ISSN 0378-7206. https://doi.org/10.1016/j.im.2022.103623.

Andronache, A., & Althonayan, A. (2018) *Shifting From Information Security Towards A Cybersecurity Paradigm*. 10.1145/3285957.3285971.

Ashrapova U., Apsilyam M. (2025). *Cybersecurity in the Digital Economy: new challenges and solutions*. International Scientific-Electronic Journal "Pioneering Studies and Theories". Volume 1, nº2.

Assembleia da República (2025). Projeto de Lei n.º 580/XIII/2.ª (PEV). Nota Técnica, de 18 de dezembro. N.º 32, II Série A.

Assembleia da República (2025). Proposta de Lei n.º 50/XVI/1.ª, de 14 de fevereiro. Assembleia da República. nº 182, II Série A.

Awati, R., KirvanRahul, P., Pratt, A. (2025). *What is ICT (information and communications technology)?* Disponível online em: https://www.techtarget.com/searchcio/definition/ICT-information-and-communications-technology-or-technologies. Último acesso em 15-04-2025

Bambi, B., Oladele, M., Suleiman, P. (2025). *Brief History of the Development of Information and Communication Technology (ICT)*. Management Information System In Education. Education Dialogue Association (EDUDIA) and the Institute for Educational Planning and Administration (IEPA).

Banco de Portugal (2025). Comunicado do Banco de Portugal sobre o pacote legislativo relativo à resiliência operacional digital do setor financeiro (DORA). Disponível online em: https://www.bportugal.pt/comunicado/comunicado-do-banco-de-portugal-sobre-o-pacote-legislativo-relativo-resiliencia. Último acesso em 08-08-2025.

Bélanger, F., Crossler, R. (2011). *Privacy in the Digital Age: A Review of Information Privacy*. Research in Information Systems. MIS Quarterly, 35(4), 1017. https://doi.org/10.2307/41409971

Bitrián, P., Buil, I., Catalán, S., Merli, D. (2024). *Gamification in workforce training: Improving employees' self-efficacy and information security and data protection behaviours*. Journal of Business Research. Volume 179.114685. ISSN 0148-2963. https://doi.org/10.1016/j.jbusres.2024.114685.

Bojor, L., Petrache, T. & Cristescu, C. (2024). *Emerging Technologies in Conflict: The Impact of Starlink in the Russia – Ukraine War*. Land Forces Academy Review. 29. 185-194. 10.2478/raft-2024-0020.

Castells, M. (2010). *The Rise of the Network Society*. Vol. I of The information age: Economy, society, and culture. Wiley-Blackwell.

Castells, M. (2003). A Era da Informação: Economia, Sociedade e Cultura. Vol. II, O Poder da Identidade. Comunicação e Sociedade. 5. 168. 10.17231/comsoc.5(2004).1256.

Castells, M., Cardoso, G. (2006). A Sociedade em Rede Do Conhecimento à Ação Política - Manuel Castells & Gustavo Cardoso. Conferência promovida pelo

Presidente da República. 4 e 5 de março de 2005 | Centro Cultural de Belém. Imprensa Nacional - Casa da Moeda.

Castelo-Branco, I., Oliveira, T., Simões-Coelho, P., Portugal, J., Filipe, I. (2022). *Measuring the fourth industrial revolution through the Industry 4.0 lens: The relevance of resources, capabilities and the value chain*. Computers in Industry. Volume 138. ISSN 0166-3615. https://doi.org/10.1016/j.compind.2022.103639.

Ceko, E. (2024). *On relations between cyber security index and iso 27001 standard index in western balkan countries*. CRJ. 12-17. 10.59380/crj.vi1.5098

Center for Internet Security (2025). *CIS Critical Security Controls. v8.1*. Disponível online em: https://learn.cisecurity.org/cis-controls-download. Último acesso em 08-10-2025.

Colabianchi, S., Costantino, F., Nonino, F., Palombi, G. (2025). *Transforming threats into opportunities: The role of human factors in enhancing cybersecurity*. Journal of Innovation & Knowledge. Volume 10. ISSN 2444-569X. https://doi.org/10.1016/j.jik.2025.100695.

CNCS (2019). Quadro Nacional de Referência para a Cibersegurança. Centro Nacional de Cibersegurança.

CNCS (2020). Quadro de Avaliação de Capacidades de Cibersegurança. Versão 1.0. Centro Nacional de Cibersegurança.

CNCS (2020). Relatório de Cibersegurança em Portugal – Riscos e Conflitos. Centro Nacional de Cibersegurança.

CNCS (2020a). Relatório Cibersegurança em Portugal: Ética & Direito. Observatório de Cibersegurança.

CNCS (2021). Relatório de Cibersegurança em Portugal – Riscos e Conflitos. Centro Nacional de Cibersegurança.

CNCS (2022). Relatório de Cibersegurança em Portugal – Riscos e Conflitos. Centro Nacional de Cibersegurança.

CNCS (2022a). Guia para Gestão dos Riscos em matérias de Segurança da Informação e Cibersegurança. Centro Nacional de Cibersegurança. V1.1.

CNCS (2022b). PME e Cibersegurança em Portugal. Documento desenvolvido pelo Centro Nacional de Cibersegurança no âmbito da Aliança para a Cibersegurança.

CNCS (2023). Relatório de Cibersegurança em Portugal – Riscos e Conflitos. Centro Nacional de Cibersegurança.

CNCS (2024). Relatório de Cibersegurança em Portugal – Riscos e Conflitos. Centro Nacional de Cibersegurança.

CNCS (2025). O que é a cibersegurança. Disponível online em: https://www.cncs.gov.pt/pt/Diretiva-sri-2-nis-2/. Último acesso em 20-08-2025.

CNCS (2025). Coordenação da resposta a incidentes. Disponível online em: https://www.cncs.gov.pt/pt/certpt/coordenacao-da-resposta-a-incidentes/. Último acesso em 08-07-2025.

CNCS (2025). Matriz de Classificação de entidades Diretiva SRI 2.

CNCS (2025a). Diretiva SRI 2 (NIS2). Disponível online em: https://www.cncs.gov.pt/pt/Diretiva-sri-2-nis-2/. Último acesso em 08-07-2025.

CNCS (2025b). Sobre nós. Disponível online em: https://www.cncs.gov.pt/pt/sobre-nos/. Último acesso em 08-07-2025.

CNCS (2025c). Relatório de Cibersegurança em Portugal – Riscos e Conflitos. Centro Nacional de Cibersegurança.

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Management Review, 4(10): 13-21. https://timreview.ca/article/835

Decreto-Lei n.º 7/2004, de 7 de janeiro. Diário da República n.º 5/2004. I Série A.

Decreto-Lei n.º 69/2014, de 9 de maio. Diário da República n.º 89/2014. I Série.

Decreto-Lei n.º 136/2017, de 6 de novembro. Diário da República n.º 217/2017. I Série.

Decreto-Lei n.º 15/2022, de 14 de janeiro. Diário da República n.º 10/2022. Série I.

DGAE (2025). Política Empresarial. Disponível online em: https://www.dgae.gov.pt/servicos/politica-empresarial.aspx. Último acesso em 09-09-2025

ENISA (2020). *Main incidents in the EU and worldwide*. ENISA Threat Landscape 2020. Disponível online em: https://www.enisa.europa.eu/sites/default/files/publications/ETL2020%20-%20Incidents%20A4.pdf. Último acesso em 09-09-2025.

ENISA (2021). *ENISA Threat Landscape 2021*. Disponível online em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2021. Último acesso em 09-09-2025.

ENISA (2022). *ENISA Threat Landscape 2022.* Disponível online em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2022. Último acesso em 09-09-2025.

ENISA (2023). *ENISA threat landscape 2023*. Disponível online em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023. Último acesso em 09-09-2025.

ENISA (2024). *ENISA Threat Landscape 2024*. Disponível online em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024. Último acesso em 09-09-2025.

ENISA (2024). *ENISA threat landscape for DoS attacks*. Disponível online em: https://www.enisa.europa.eu/publications/dos-report. Último acesso em 09-09-2025.

ENISA (2024). *Foresight Cybersecurity Threats for 20230 – Update. Executive Summary*. Disponível online em: https://www.enisa.europa.eu/publications/foresight-cybersecurity-threats-for-2030-update-2024-executive-summary. Último acesso em 20-06-2025.

ENISA (2024a). *NIS Investments 2024*. Disponível online em: https://www.enisa.europa.eu/publications/nis-investments-2024. Último acesso em 09-06-2025.

ENISA (2025). Technical Implementation Guidance. Version 1.0. Luxembourg: Publications Office of the European Union.

ENISA (2025a). *ENISA Threat Landscape 2025*. Disponível online em: https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025. Último acesso em 09-09-2025.

Garibaldi, S., Deane, F. (2023). *Cyberspace as a fifth dimension of national security: trade measure exceptions*. Journal of International Trade Law and Policy. 22. 67-88. 10.1108/JITLP-01-2023-0004.

Gouveia, H. (2012). Das Beiras para o Centro. A imagem da região centro junto dos seus habitantes. Dissertação de Mestrado, IPAM – Instituto Português de Administração de Marketing. http://hdl.handle.net/10400.26/7471

Henman, F. (2022). *Digital Social Policy: Past, Present, Future*. Journal of Social Policy, 51, 535–550. doi:10.1017/S0047279422000162

High Table (2025). *ISO27001:2022 Annex A Controls – Control by Control.* Disponível online em: https://hightable.io/category/iso27001-annex-a-controls/. Último acesso em 05-10-2025.

IDC (2021). *Future of Industry Ecosystems: Shared Data and Insights.* Disponível online em: https://blogs.idc.com/2021/01/06/future-of-industry-ecosystems-shared-data-and-insights/ . Último acesso em 09-09-2025.

IDC (2024). *NIS2 Readiness: A Guide for Organizations in Europe*. InfoBrief, sponsored by Microsoft.

International Organization for Standardization & International Electrotechnical Commission (2018). ISO/IEC 27000:2018 – Information technology — Security techniques — Information security management systems — Overview and vocabulary (5th ed.). ISO.

International Organization for Standardization & International Electrotechnical Commission (2019). ISO/IEC 27701:2019 – Security techniques: Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management — Requirements and guidelines (1st ed.). ISO.

ISCTE (2022). Orientações aos investigadores sobre proteção de dados pessoais em atividades de investigação científica no ISCTE – Instituo Universitário de Lisboa.

Julião, R. (2003). Informação Geográfica e Cidadania. Lisboa: UNL/FCSH – Dep. de Geografia e Planeamento Regional. Lisboa.

Kraus, Sascha & Jones, Paul & Kailer, Norbert & Weinmann, Alexandra & Chaparro-Banegas, Nuria & Roig-Tierno, Norat. (2021). *Digital Transformation: An Overview of the Current State of the Art of Research. SAGE Open*. 11. 10.1177/21582440211047576.

Laberge, L., O'Toole, C., Schneider, J., Smaje, K. (2020). *How COVID-19 has pushed companies over the technology tipping point—and transformed business forever*. McKinsey Digital and Strategy & Corporate Finance Practices. McKinsey & Company.

Lei n.º 41/2004, de 18 de agosto. Diário da República nº 194/2004, I Série A.

Lei n.º 46/2012, de 29 de agosto. Diário da República nº 167/2012, I Série.

Lei n.º 46/2018, de 13 de agosto. Diário da República nº 155/2018, I Série.

Lei n.º 58/2019, de 8 de agosto. Diário da República nº 151/2019, I Série.

Lei n.º 59/2019, de 8 de agosto. Diário da República nº 151/2019, I Série.

Lei n.º 59/2025, de 22 de outubro. Diário da República n.º 204/2025, I Série.

Decreto-Lei n.º 15/2022, de 14 de janeiro, de 2022; Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022; Lei n.º 46/2018, de 13 de agosto de 2018.

Lember, V., Brandsen, T., & Tõnurist, P. (2019). *The potential impacts of digital technologies on co-production and co-creation*. Public Management Review, 21(11), 1665–1686. https://doi.org/10.1080/14719037.2019.1619807

McChesney, R. W. (2013). *Digital Disconnect: How Capitalism is Turning the Internet Against Democracy*. The New Press. https://doi.org/10.2307/jj.26193195

Madiega, T. (2022). *Russia's war on Ukraine: Digital issues (EPRS At a Glance*, PE 729.317). European Parliamentary Research Service.

Mansell, R. (2021). *Adjusting to the digital: Societal outcomes and consequences*. Research Policy. Volume 50, Issue 9. 104296. ISSN 0048-7333. https://doi.org/10.1016/j.respol.2021.104296.

Makhija, A. (2021). I*nformation Security Management Systems - Evolving Landscape & ISO 27001: An Empirical Study*. Journal of Accounting, Finance, Economics, and Social Sciences. 6. 9-17. 10.62458/jafess.160224.6(1)9-17.

Missão para a Sociedade da Informação (MSI) (1997). Livro Verde para a Sociedade da Informação em Portugal. MSI-MCT. Lisboa.

Mohsin, K. (2022). *Data Privacy and Cybersecurity* (December 11, 2022). http://dx.doi.org/10.2139/ssrn.4299439

Moloi, T., Marwala, T. (2023). *Technologies of the Fourth Industrial Revolution*. In book: Enterprise Risk Management in the Fourth Industrial Revolution. 10.1007/978-981-99-6307-2_3.

Morais Leitão (2024*). Legal Alert:* Regulamento de Ciber-Resiliência – Principais medidas. Disponível online em: https://www.mlgts.pt/pt/conhecimento/legal-alerts/Legal-Alert-Regulamento-de-Ciber-Resiliencia-Principais-medidas/25643/. Último acesso em 20-07-2025.

NATO (2022). *Cyber defence and the Russia-Ukraine war. North Atlantic Treaty Organization.* Disponível online em: https://www.nato.int/cps/en/natohq/topics_78170.htm. Último acesso em 09-09-2025

Nevado-Peña, D., López-Ruiz, V., Alfaro-Navarro, J. (2019). *Improving quality of life perception with ICT use and technological capacity in Europe, Technological Forecasting and Social Change*. Volume 148.119734. ISSN 0040-1625. https://doi.org/10.1016/j.techfore.2019.119734.

National Institute of Standards and Technology (2012). Guide for conducting risk assessments (NIST Special Publication 800-30 Rev. 1). U.S. Department of Commerce.

National Institute of Standards and Technology (2020). Security and Privacy Controls for Information Systems and Organizations. NIST Special Publication 800-53. Revision 5. https://doi.org/10.6028/NIST.SP.800-53r5

National Institute of Standards and Technology (2010). Contingency Planning Guide for Federal Information Systems. NIST Special Publication 800-34 Rev. 1.

PECB (2025). *ISO 22301 Societal Security Business Continuity Management Systems.* Disponível online em: https://pecb.com/en/whitepaper/iso-22301-societal-security-business-continuity-management-systems. Último acesso em 15-10-2025.

PLMJ. (2024). Cyber Resilience Act: Segurança Cibernética na Economia Digital. Transformative Legal Experts.

Reid, R. & van Niekerk, J. (2014). *From Information Security to Cyber Security Cultures Organizations to Societies*. Conference: Information Security South Africa (ISSA)At: Johannesburg, South Africa.

Resolução do Conselho de Ministros n.º 36/2015, de 12 de junho. Diário da República nº 113/2015, I Série

Resolução do Conselho de Ministros n.º 92/2019, de 5 de junho. Diário da República nº 108/2019, I Série

Resolução do Conselho de Ministros n.º 207/2024, de 30 de dezembro. Diário da República nº 252/2024, I Série.

Schmitz-Berndt, S. (2023). *Defining the reporting threshold for a cybersecurity incident under the NIS Directive and the NIS2 Directive*, Journal of Cybersecurity, Volume 9, Issue 1, 2023, tyad009, https://doi.org/10.1093/cybsec/tyad009

Sharma, R. (212). *Study of latest emerging trends on cyber security and its challenges to Society*. International Journal of Scientific & Engineering Research, Volume 3, Issue 6. ISSN 2229-5518

Silva, B (2001). A tecnologia é uma estratégia. In Paulo Dias &Varela de Freitas (org.). Atas da II Conferência Internacional Desafios 2001. Braga: Centro de Competência da Universidade do Minho do Projeto Nónio, pp. 839-859. (ISBN: 972-98456-1-1)

Sousa, H. (2012). Castells, M. (2002). A Era da Informação: Economia, Sociedade e Cultura, Vol. I, A Sociedade em Rede. Lisboa: Fundação Calouste Gulbenkian.

Sehgal, N. K., Sohoni, S., Xiong, Y., Fritz, D., Mulia, W., & Acken, J. M. (2011*). Invited Paper: A Cross Section of the Issues and Research Activities Related to Both Information Security and Cloud Computing*. IETE Technical Review, 28(4), 279–291. https://doi.org/10.4103/0256-4602.83549

Taherdoost, H. (2022). *Cybersecurity vs. Information Security. Procedia Computer Science.* Volume 215. Pages 483-487- ISSN 1877-0509. https://doi.org/10.1016/j.procs.2022.12.050.

Taherdoost, H., Sahibuddin, S. and Jalaliyoon, N. (2014). *Evaluation of Security Factors Effectingon Web-Based Service Adoption, Recent Advances*. In Telecommunications, Informatics and Educational Technologies, ISBN: 978-1-61804-262-0, Page: 117-123

UE (1994). A Via Europeia para a Sociedade da Informação. Plano de Ação. Comunicação da Comissão ao Concelho e ao Parlamento Europeu e ao Comité Económico e Social e ao Comité das regiões. Nº 247.

UE (1995). Diretiva (UE) 95/46 do Parlamento Europeu e do Conselho, de 24 de outubro. Jornal Oficial da União Europeia n.º L 281, de 23 de novembro de 1995.

UE (2001). Segurança das redes e da informação: Proposta de abordagem de uma política europeia. Comunicação da Comissão ao Concelho e ao Parlamento Europeu e ao Comité Económico e Social e ao Comité das regiões. Nº 298.

UE (2002). Diretiva (UE) 2002/21 do Parlamento Europeu e do Conselho, de 7 de março. Jornal Oficial da União Europeia n.º L 108, de 24 de abril de 2002.

UE (2002a). Diretiva (UE) 2002/58 do Parlamento Europeu e do Conselho, de 12 de julho. Jornal Oficial da União Europeia n.º L 201, de 31 de julho de 2002.

UE (2004). Regulamento (CE) 460/2004 do Parlamento Europeu e do Conselho, de 10 de março de 2004. Jornal Oficial da União Europeia n.º L 077, de 13 de março de 2004.

UE (2009). Diretiva (UE) 2009/136 do Parlamento Europeu e do Conselho, de 25 de novembro. Jornal Oficial da União Europeia n.º L 337/11, de 18 de dezembro de 2009.

UE (2013). Diretiva (UE) 2013/40 do Parlamento Europeu e do Conselho, de 12 de agosto. Jornal Oficial da União Europeia n.º L 218/8, de 14 de agosto de 2016.

UE (2013). Regulamento (UE) 526/2013 do Parlamento Europeu e do Conselho, de 21 de maio. Jornal Oficial da União Europeia n.º L 165/41, de 18 de junho de 2013.

UE (2013a). Estratégia da União Europeia para a cibersegurança: Um ciberespaço aberto, seguro e protegido. Comunicação conjunta ao Parlamento Europeu, ao Concelho, ao Comité Económico e Social e ao Comité das regiões. Nº 1.

UE (2016). Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 16 de julho. Jornal Oficial da União Europeia n.º L 194/1, de 19 de julho de 2016.

UE (2016a). Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril. Jornal Oficial da União Europeia n.º L 119/1, de 4 de maio de 2016.

UE (2016b). Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho, de 27 de abril. Jornal Oficial da União Europeia n.º L 119/89, de 4 maio de 2016.

UE (2019). Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril. Jornal Oficial da União Europeia n.º L 151/15, de 7 de junho de 2019.

UE (2020). Proposta de Diretiva do Parlamento Europeu e do Conselho, de 16 de dezembro. Comunicação n.º 823, de 16 de dezembro de 2020.

UE (2022a). Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro. Jornal Oficial da União Europeia n.º L 333/1, de 27 de dezembro de 2022.

UE (2022b). Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro. Jornal Oficial da União Europeia n.º L 333/80, de 27 de dezembro de 2022.

UE (2022c). Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro. Jornal Oficial da União Europeia n.º L 333/164, de 27 de dezembro de 2022.

UE (2023). *Joint communication on the EU policy on cyber defence. European Commission.* Disponível online em: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=JOIN%3A2022%3A49%3AFIN. Último acesso em 09-09-2025.

UE (2024). Regulamento de Execução (UE) 2024/2690 da Comissão, de 17 de outubro. Jornal Oficial da União Europeia Série L, de 18 de outubro de 2024.

UE (2024a). Regulamento (UE) 2024/2847 do Parlamento Europeu e do Conselho, de 23 de outubro. Jornal Oficial da União Europeia Série L, de 20 de novembro de 2024.

EU (2025). O direito primário da União Europeia. Disponível online em: https://eur-lex.europa.eu/PT/legal-content/summary/the-european-union-s-primary-law.html. Último acesso em 05-09-2025.

UE (2025). Micro, pequenas e médias empresas: definição e âmbito de aplicação. Disponível online em: https://eur-lex.europa.eu/PT/legal-content/summary/micro-small-and-medium-sized-enterprises-definition-and-scope.html. Último acesso em 05-09-2025.

UE (2025a). Cibersegurança da UE: estratégia e principais políticas. Disponível online em: https://www.consilium.europa.eu/pt/policies/cybersecurity/timeline-cybersecurity/. Último acesso em 09-09-2025.

UE (2025b). Iniciativa Internet de próxima geração. Disponível online em: https://digital-strategy.ec.europa.eu/pt/policies/next-generation-internet-initiative. Último acesso em 09-09-2025.

UE (2025c). Um futuro digital para a Europa. Disponível online em: https://www.consilium.europa.eu/pt/policies/a-digital-future-for-europe/. Último acesso em 09-09-2025.

UE (2025d). Regulamento (UE) 2025/38 do Parlamento Europeu e do Conselho, de 19 de dezembro. Jornal Oficial da União Europeia Série L, de 15 de janeiro de 2025.

UE (2025e). Transposição da Diretiva SRI 2 nos países da EU. Disponível online em: https://digital-strategy.ec.europa.eu/pt/policies/nis-transposition. Último acesso em 09-09-2025.

Vieira de Almeida (2023). Digital Operational Resilience Act (DORA). Comunicações, Proteção de Dados & Tecnologia. VdA Expertise.

W. Alec Cram & Jonathan Yuan (2023). *Out with the old, in with the new: examining national cybersecurity strategy changes over time.* Journal of Cyber Policy, 8:1, 26-47, DOI: 10.1080/23738871.2023.2238712

Wang, G. & Wendy. (2019). *Measuring information security and cybersecurity on private cloud computing.* Journal of Theoretical and Applied Information Technology, 96, 156-168.

Anexos

Anexo I – Questionário (perguntas)

Questionário sobre Cibersegurança

Este questionário visa aferir o estado da organização em termos de cibersegurança, considerando o Quadro Nacional de Referência para a Cibersegurança e o Quadro de Avaliação de Capacidades Mínimas em Cibersegurança, do Centro Nacional de Cibersegurança.

* Indica uma pergunta obrigatória

Em que nível se encontra a sua organização na implementação das capacidades de cibersegurança?

1. **Setor de atividade a que pertence a sua organização?** *

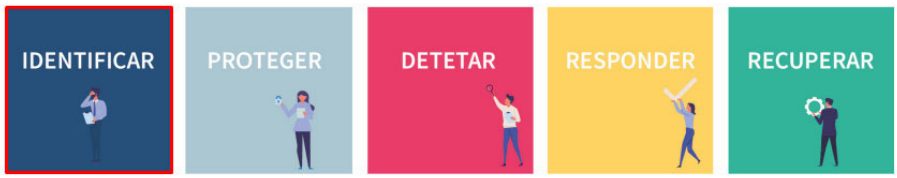
Nota: setores de importância crítica e setores críticos, de acordo com a NIS2 (Anexos I e II)

Marcar apenas uma oval.

- ◯ 1. Energia
- ◯ 2. Transportes
- ◯ 3. Setor bancário
- ◯ 4. Infraestruturas do mercado financeiro
- ◯ 5. Saúde
- ◯ 6. Água potável
- ◯ 7. Águas residuais
- ◯ 8. Infraestruturas digitais
- ◯ 9. Gestão de serviços TIC (entre empresas)
- ◯ 10. Administração pública
- ◯ 11. Espaço (empresas que apoiam prestação de serviços espaciais)
- ◯ 12. Serviços postais e de estafeta
- ◯ 13. Gestão de resíduos
- ◯ 14. Produção, fabrico e distribuição de produtos químicos
- ◯ 15. Produção, transformação e distribuição de produtos alimentares
- ◯ 16. Indústria transformadora
- ◯ 17. Prestadores de serviços digitais
- ◯ 18. Investigação
- ◯ 19. Outros

CAPACIDADE DE IDENTIFICAR

Compreensão do contexto da organização, dos ativos que suportam os processos críticos da atividade da organização e dos riscos associados relevantes. Esta compreensão permite que a organização consiga definir e priorizar os seus recursos e investimentos, de acordo com os seus objetivos gerais e com a sua estratégia de gestão do risco (CNCS, 2020).
(Selecione a opção em que melhor se enquadra à sua organização)



2. **1. Os dispositivos físicos, redes e sistemas de informação da sua organização encontram-se inventariados?** *

Marcar apenas uma oval.

- ◯ 1. Existem registos em ficheiros isolados e de forma ad hoc
- ◯ 2. Encontram-se registados em ferramenta de gestão de ativos físicos
- ◯ 3. Existem processos e ferramentas para a descoberta automática
- ◯ 4. Não sabe/Não aplicável

3. **2. As aplicações e plataformas de software são inventariadas?** *

Marcar apenas uma oval.

- ◯ 1. Existem registos em ficheiros isolados com informações sobre sistemas
- ◯ 2. São registados em ferramenta de gestão de ativos de software
- ◯ 3. Existe um sistema de descoberta automática (novos sistemas e alterações)
- ◯ 4. Não sabe/Não aplicável

4. **3. As redes e fluxos de dados são mapeados?** *

Marcar apenas uma oval.

- ◯ 1. Existem registos das redes e respetivas zonas
- ◯ 2. O registo é ao nível do IP e inclui fluxos de comunicações
- ◯ 3. Existem processos e ferramentas para o mapeamento automático de ativos de rede
- ◯ 4. Não sabe/Não aplicável

5. **4. As redes e sistemas de informação externos encontram-se identificados e catalogados?** *

Marcar apenas uma oval.

- ◯ 1. Os ativos localizados externamente são identificados de forma ad hoc
- ◯ 2. Os ativos localizados externamente possuem dados completos de identificação
- ◯ 3. Existem processos e ferramentas para mapeamento automático de ativos localizados externamente
- ◯ 4. Não sabe/Não aplicável

6. **5. Os ativos necessários para a prestação de bens e serviços encontram-se classificados?** *

Marcar apenas uma oval.

- ◯ 1. Os ativos encontram-se classificados de forma ad hoc
- ◯ 2. Existem métodos de classificação dos ativos por criticidade e valor percebido bem como uma política de classificação consoante a sua importância percebida para o negócio
- ◯ 3. A classificação dos ativos é revista em períodos regulares e o nível da classificação dos ativos influencia na seleção dos controlos de segurança aplicados
- ◯ 4. Não sabe/Não aplicável

7. **6. A missão, visão, valores, estratégias e objetivos encontram-se definidos e comunicados?** *

Marcar apenas uma oval.

- ◯ 1. A missão, visão, valores e objetivos estratégicos estão definidos através de contrato ou estatuto
- ◯ 2. A política de segurança da informação faz referência à missão, visão, objetivos e valores
- ◯ 3. Existem ações de sensibilização das partes interessadas quanto às políticas de segurança, missão e objetivo da organização
- ◯ 4. Não sabe/Não aplicável

8. **7. Os ativos críticos estão identificados?** *

Marcar apenas uma oval.

- ◯ 1. Existem registos dos ativos críticos em ficheiros isolados e ad hoc
- ◯ 2. Existe uma política de classificação de ativos conforme a sua criticidade e são registados e classificados em ferramenta própria
- ◯ 3. Existem processos e ferramentas para descoberta automática de ativos críticos
- ◯ 4. Não sabe/Não aplicável

9. **8. Os requisitos de resiliência para a prestação de serviços críticos estão definidos?** *

Marcar apenas uma oval.

- ◯ 1. Existe documentação dos requisitos mínimos de infraestrutura, de forma ad hoc
- ◯ 2. Existe um Plano de Continuidade de Negócio e é validado experimentalmente em períodos regulares
- ◯ 3. Existe a capacidade para operação imediata em localização alternativa
- ◯ 4. Não sabe/Não aplicável

10. **9. A política de segurança da informação está definida e comunicada?** *

Marcar apenas uma oval.

- ◯ 1. Existe uma política de segurança estabelecida e divulgada internamente
- ◯ 2. Os colaboradores são informados e participam em ações de sensibilização sobre a existência da política e os seus termos
- ◯ 3. A política é revista periodicamente e é mantida num sistema eletrónico de registo e armazenamento de políticas
- ◯ 4. Não sabe/Não aplicável

11. **10. Os requisitos legais e regulamentares para a cibersegurança são cumpridos?** *

Marcar apenas uma oval.

- ◯ 1. Existe internamente conhecimento informal sobre leis e regulamentações aplicáveis
- ◯ 2. As leis e regulamentações aplicáveis estão identificadas na política de segurança
- ◯ 3. É efetuada uma revisão regular das leis e regulamentações aplicáveis
- ◯ 4. Não sabe/Não aplicável

12. **11. As vulnerabilidades dos ativos encontram-se identificadas?** *

Marcar apenas uma oval.

- ◯ 1. As vulnerabilidades dos ativos são detetadas de forma ad hoc e sem processo de tratamento formal
- ◯ 2. As vulnerabilidades dos ativos são detetadas, tipificadas e tratadas por processos especializados
- ◯ 3. Existe sistema de descoberta automática de vulnerabilidades dos ativos
- ◯ 4. Não sabe/Não aplicável

13. **12. A organização partilha informações sobre ameaças em grupos de interesse?** *

Marcar apenas uma oval.

- ◯ 1. São apenas mantidos contactos informais com grupos de interesse
- ◯ 2. Existe um responsável identificado para comunicar sobre ameaças e temas de segurança da informação com grupos de interesse, seguindo um processo formal
- ◯ 3. Existe sistema de coleta e tratamento de comunicação de ameaças integrado no processo de gestão de vulnerabilidades
- ◯ 4. Não sabe/Não aplicável

14. **13. As ameaças internas e externas são identificadas e classificadas?** *

Marcar apenas uma oval.

- ◯ 1. Apenas existe uma lista genérica de ameaças internas e externas sem metodologia formal
- ◯ 2. Existe um mapa de ameaças conhecidas associadas a cada tipo de ativo
- ◯ 3. O processo de gestão de riscos encontra-se estabelecido com critérios definidos e os seus resultados e estratégias de tratamento são revistos em intervalos regulares
- ◯ 4. Não sabe/Não aplicável

15. **14. A gestão do risco é efetuada com base na análise de ameaças, vulnerabilidades, probabilidades e impactos?** *

Marcar apenas uma oval.

- ◯ 1. Existe um documento com a metodologia de gestão do risco estabelecida
- ◯ 2. Existe um catálogo de ameaças e vulnerabilidades identificadas na estrutura da organização, categorizado com probabilidade e impacto
- ◯ 3. As avaliações de riscos são suportadas por sistemas específicos para o efeito
- ◯ 4. Não sabe/Não aplicável

16. **15. O processo de gestão de risco encontra-se definido?** *

Marcar apenas uma oval.

- ◯ 1. As estratégias para a gestão de riscos não estão definidas ou não são consistentes em toda a organização
- ◯ 2. Existem estratégias definidas para a gestão de riscos, consistentes em toda a organização, bem como responsáveis pela gestão do processo e pelo tratamento dos riscos identificados
- ◯ 3. A gestão de riscos é suportada por um sistema dedicado, existindo ainda um registo histórico de revisão dos riscos
- ◯ 4. Não sabe/Não aplicável

17. **16. A estratégia de tratamento do risco encontra-se definida?** *

Marcar apenas uma oval.

- ◯ 1. A estratégia de tratamento de riscos é decidida caso a caso de forma ad hoc
- ◯ 2. Está formalizada a estratégia de tratamento de riscos e definida a tolerância ao risco aceite
- ◯ 3. A estratégia de tratamento de riscos é revista regularmente, bem como a tolerância ao risco
- ◯ 4. Não sabe/Não aplicável

18. **17. O risco da cadeia de logística é gerido?** *

Marcar apenas uma oval.

- ◯ 1. A cadeia de logística encontra-se identificada
- ◯ 2. A organização aplica a gestão de riscos na sua cadeia logística
- ◯ 3. Existem avaliações regulares dos riscos dos fornecedores e dos seus impactos
- ◯ 4. Não sabe/Não aplicável

19. **18. Os contratos com fornecedores respeitam o plano de gestão do risco para a cadeia logística?** *

Marcar apenas uma oval.

- ◯ 1. Existe um processo formal para contratação de fornecedores
- ◯ 2. O tema da segurança da informação é incluído nos contratos da cadeia logística
- ◯ 3. Os controlos de segurança dos seus fornecedores são avaliados em intervalos regulares
- ◯ 4. Não sabe/Não aplicável

20. **19. O plano de resposta e recuperação de desastre é exercitado com os fornecedores?** *

Marcar apenas uma oval.

- ◯ 1. Os fornecedores que suportam os processos críticos da organização estão identificados
- ◯ 2. Os planos de resposta e recuperação de desastres definidos consideram a cadeia de fornecedores
- ◯ 3. São feitos testes regulares aos planos de recuperação e resposta, com o envolvimento da cadeia de fornecedores críticos
- ◯ 4. Não sabe/Não aplicável

CAPACIDADE DE PROTEGER

Implementação de medidas destinadas a proteger os processos organizativos e os ativos da organização, independentemente da sua natureza tecnológica. Assim, nesta categoria, são definidas medidas orientadas à proteção da organização nas suas três dimensões: Pessoas, Processos e Tecnologia (CNCS, 2020).
(Selecione a opção em que melhor se enquadra à sua organização)

21. **1. O ciclo de vida de gestão das identidades encontra-se definido?** *

Marcar apenas uma oval.

- ◯ 1. A associação de acessos de identidades é feita com base nos acessos atribuídos no passado
- ◯ 2. Está formalizada uma política de gestão de acessos e existem procedimentos para gerir atribuição, alteração e revogação de acessos
- ◯ 3. Os acessos são geridos conforme o perfil funcional para cada tipo de acesso e são validados regularmente
- ◯ 4. Não sabe/Não aplicável

22. **2. Existem controlos de acesso físico para aceder às redes e sistemas de informação?** *

Marcar apenas uma oval.

- ◯ 1. Existem controlos físicos para restringir o acesso físico às zonas protegidas
- ◯ 2. Os acessos físicos são integrados num sistema transversal de gestão de identidades e acessos
- ◯ 3.Os acessos de pessoas externas são monitorizados e os acessos físicos são avaliados regularmente
- ◯ 4. Não sabe/Não aplicável

23. **3. Os acessos remotos são geridos?** *

Marcar apenas uma oval.

- ◯ 1. A organização suporta acessos remotos, mas não controla nem monitoriza os acessos
- ◯ 2. Os acessos remotos são controlados de maneira centralizada e integrada com sistemas internos
- ◯ 3. Existem bloqueios proativos contra acessos remotos não autorizados e é utilizado duplo fator de autenticação para acessos remotos
- ◯ 4. Não sabe/Não aplicável

24. **4. Os princípios de menor privilégio e segregação de funções são aplicados na Gestão de Acessos?** *

Marcar apenas uma oval.

- ◯ 1. Os acessos são atribuídos nominalmente e as contas não são partilhadas
- ◯ 2. Os perfis de acessos elevados são atribuídos com critérios de restrição
- ◯ 3. Os acessos concedidos com privilégios elevados são revistos regularmente
- ◯ 4. Não sabe/Não aplicável

25. **5. A integridade das redes de comunicações encontra-se protegida?** *

Marcar apenas uma oval.

- ◯ 1. As redes internas encontram-se segregadas por finalidade
- ◯ 2. As alterações de conexão entre redes são documentadas e aprovadas
- ◯ 3. São revistas regularmente as regras de conexão entre redes
- ◯ 4. Não sabe/Não aplicável

26. **6. Os colaboradores têm formação em segurança da informação?** *

Marcar apenas uma oval.

- ◯ 1. São realizadas ações de consciencialização para o tema da segurança da informação
- ◯ 2. Existe um plano de formação de frequência obrigatória em segurança de informação e as presenças são registadas
- ◯ 3. São feitos testes aos colaboradores para aferir a retenção do conhecimento sobre segurança de informação
- ◯ 4. Não sabe/Não aplicável

27. **7. Os utilizadores com acesso privilegiado compreendem quais são os seus papéis e responsabilidades?** *

Marcar apenas uma oval.

- ◯ 1. Os utilizadores com acessos privilegiados são informalmente notificados das responsabilidades acrescidas relativas a acessos atribuídos
- ◯ 2. Os utilizadores de acessos privilegiados têm formação específica sobre segurança da informação, estando também implementados procedimentos de registo da aceitação de condições especiais de acessos
- ◯ 3. São medidos os resultados das ações de formação e consciencialização aos utilizadores com acessos privilegiados e é garantida a atualidade da aceitação das condições especiais de acessos com privilégios elevados
- ◯ 4. Não sabe/Não aplicável

28. **8. A gestão de topo compreende as suas funções e responsabilidades?** *

Marcar apenas uma oval.

- ◯ 1. As funções e responsabilidades da gestão de topo estão definidas de forma informal
- ◯ 2. Os papéis e responsabilidades da gestão de topo, no âmbito da segurança da informação, estão estabelecidos e são registados
- ◯ 3. Estão estabelecidos o envolvimento e a consciencialização da gestão de topo em temas de segurança da informação
- ◯ 4. Não sabe/Não aplicável

29. **9. Os dados armazenados encontram-se protegidos?** *

Marcar apenas uma oval.

- ◯ 1. Estão definidas regras de proteção da confidencialidade, integridade e disponibilidade dos ficheiros, documentos e dados
- ◯ 2. Está estabelecida a classificação da informação consoante a sua sensibilidade e relevância
- ◯ 3. Os dados são armazenados consoante os seus níveis de classificação
- ◯ 4. Não sabe/Não aplicável

30. **10. Os dados em circulação são protegidos?** *

Marcar apenas uma oval.

- ◯ 1. São utilizados controlos comuns disponíveis de proteção de dados em circulação, como protocolos de cifra (p. ex. sítios de internet, formulários de páginas de internet, bancos de dados)
- ◯ 2. Estão formalizadas políticas e procedimentos sobre proteção de dados em circulação
- ◯ 3. Utilização de tecnologias de cifra, de acordo com a classificação da informação
- ◯ 4. Não sabe/Não aplicável

31. **11. Os ativos são geridos durante os procedimentos de remoção, transferência e aprovisionamento?** *

Marcar apenas uma oval.

- ◯ 1. Registo informal ou ad hoc dos dados que entram e saem por meio de armazenamento físico
- ◯ 2. Registo formal dos controlos de dados que entram e saem por meio de armazenamento físico
- ◯ 3. É garantida a destruição dos dispositivos amovíveis, de forma a não expor dados sigilosos, de acordo com procedimentos de destruição
- ◯ 4. Não sabe/Não aplicável

32. **12. É providenciada capacidade adequada para garantir a disponibilidade das redes e dos sistemas de informação?** *

Marcar apenas uma oval.

- ◯ 1. Não existe um processo formal para garantir a disponibilidade das redes e dos sistemas de informação
- ◯ 2. As capacidades dos sistemas de informação e redes de comunicações são monitorizadas
- ◯ 3. É feita a gestão pró-ativa da capacidade instalada, com base em modelos de previsão fundamentados na utilização passada e crescimento futuro
- ◯ 4. Não sabe/Não aplicável

33. **13. São implementadas proteções que evitem exfiltração de informação?** *

Marcar apenas uma oval.

- ◯ 1. Estão implementados procedimentos de prevenção contra exfiltração
- ◯ 2. São implementados controlos de proteção das informações que mitiguem o risco de exfiltração de dados
- ◯ 3. Existem processos e mecanismos de prevenção contra a perda de informações
- ◯ 4. Não sabe/Não aplicável

34. **14. São utilizados mecanismos de verificação para confirmar a integridade de software, firmware e dados?** *

Marcar apenas uma oval.

- 1. A integridade dos sistemas de informação, firmware e dados é verificada de forma não sistematizada
- 2. Estão estabelecidas ações que avaliem e atestem a integridade dos sistemas
- 3. São utilizados algoritmos de verificação de integridade
- 4. Não sabe/Não aplicável

35. **15. A configuração base de redes e sistemas de informação incorpora os princípios de segurança?** *

Marcar apenas uma oval.

- 1. As configurações de segurança são feitas de forma informal e não sistematizada
- 2. Existem regras que definem a configuração base de redes e sistemas
- 3. As configurações base dos sistemas são monitorizadas
- 4. Não sabe/Não aplicável

36. **16. Está implementado o ciclo de vida de desenvolvimento seguro de software?** *

Marcar apenas uma oval.

- 1. Existe um conjunto rudimentar de requisitos de segurança mínimos para os projetos de desenvolvimento
- 2. Estão definidos exaustivamente os requisitos de segurança a seguir nos projetos de desenvolvimento
- 3. Existem processos de testes e validações de segurança estabelecidos no ciclo de desenvolvimento
- 4. Não sabe/Não aplicável

37. **17. Existe um processo de gestão de alterações?** *

Marcar apenas uma oval.

- ◯ 1. Existe um processo informal para a gestão de alterações
- ◯ 2. Existem regras internas para orientar a gestão de alterações
- ◯ 3. É feita revisão periódica dos procedimentos e registos de alterações
- ◯ 4. Não sabe/Não aplicável

38. **18. São realizadas, mantidas e testadas cópias de segurança dos dados da organização?** *

Marcar apenas uma oval.

- ◯ 1. São realizadas cópias de segurança de sistemas e ficheiros
- ◯ 2. Estão estabelecidas regras internas formais para a realização das cópias de segurança
- ◯ 3. A confidencialidade, integridade e disponibilidade da informação armazenada das cópias de segurança são garantidas e os procedimentos realizados para as cópias de segurança são verificados
- ◯ 4. Não sabe/Não aplicável

39. **19. Os dados são destruídos de acordo com a política definida?** *

Marcar apenas uma oval.

- ◯ 1. Os dados são destruídos de forma ad hoc
- ◯ 2. Os procedimentos de destruição de informação sigilosa estão documentados
- ◯ 3. A eficácia da destruição da informação em meio físico e digital é avaliada regularmente
- ◯ 4. Não sabe/Não aplicável

40. **20. Os processos de proteção são melhorados continuamente?** *

Marcar apenas uma oval.

- ◯ 1. Os processos de proteção são efetuados de forma não sistematizada
- ◯ 2. Existem procedimentos e controlos de monitorização e melhoria contínua dos processos de proteção
- ◯ 3. São realizadas auditorias internas recorrentes aos controlos de segurança
- ◯ 4. Não sabe/Não aplicável

41. **21. Os planos de resposta e recuperação são testados e exercitados?** *

Marcar apenas uma oval.

- ◯ 1. Os planos de resposta são exercitados de forma não sistematizada
- ◯ 2. Os planos de continuidade são registados e testados quanto ao âmbito definido
- ◯ 3. São avaliadas regularmente as estratégias e ações dos planos de resposta e recuperação, incluindo a execução de simulacros
- ◯ 4. Não sabe/Não aplicável

42. **22. A cibersegurança é contemplada nos processos de gestão de recursos humanos?** *

Marcar apenas uma oval.

- ◯ 1. O registo dos colaboradores é realizado
- ◯ 2. Existem regras para seleção, recrutamento e contratação
- ◯ 3. Existem perfis funcionais com competências em cibersegurança e segurança da informação, para as contratações
- ◯ 4. Não sabe/Não aplicável

43. **23. As vulnerabilidades dos ativos são geridas?** *

Marcar apenas uma oval.

- ◯ 1. Existe um plano de avaliação de vulnerabilidades
- ◯ 2. As vulnerabilidades são tratadas por equipas adequadas
- ◯ 3. O processo de gestão de vulnerabilidades é revisto e melhorado regularmente
- ◯ 4. Não sabe/Não aplicável

44. **24. As atividades de manutenção e reparação dos ativos da organização são realizadas e registadas em programas e planos aprovados e controlados?** *

Marcar apenas uma oval.

- ◯ 1. As atividades de manutenção são realizadas sem seguir um processo formal
- ◯ 2. Existe um processo formal de aprovação das atividades de manutenção e reparação e é realizado o seu planeamento e registo
- ◯ 3. Estão estabelecidos períodos de manutenção preventiva aos ativos da organização e todas as ocorrências são registadas em ferramenta de gestão de pedidos
- ◯ 4. Não sabe/Não aplicável

45. **25. As manutenções remotas são revistas, aprovadas, executadas e registadas?** *

Marcar apenas uma oval.

- ◯ 1. As manutenções remotas não seguem um processo formal
- ◯ 2. As manutenções remotas requerem aprovação prévia e são realizadas através de meios seguros
- ◯ 3. Os controlos de acompanhamento do fluxo de solicitações e aprovações para as manutenções remotas estão automatizados
- ◯ 4. Não sabe/Não aplicável

46. **26. Existem registos de auditoria?** *

Marcar apenas uma oval.

- ◯ 1. Os registos de auditoria não seguem um processo de gestão formal
- ◯ 2. Estão estabelecidos critérios formais para a auditoria de sistemas, os registos de eventos para auditorias são geridos de maneira sistémica e os formatos e taxonomias de registos estão definidos
- ◯ 3. Os registos de auditorias transversais aos sistemas da organização são geridos centralmente e a integridade dos registos de eventos para fins de auditorias é garantida
- ◯ 4. Não sabe/Não aplicável

47. **27. Os suportes de dados amovíveis são protegidos e a sua utilização é restrita de acordo com a política definida?** *

Marcar apenas uma oval.

- ◯ 1. Existe uma implementação básica e ad hoc de medidas de proteção aos suportes de dados amovíveis
- ◯ 2. Estão estabelecidas regras de uso e boas práticas sobre dispositivos amovíveis, estão disponíveis os mecanismos técnicos para proteção de dados e são promovidas ações de sensibilização
- ◯ 3. Está bloqueada a utilização de dispositivos amovíveis ou é garantida a higienização dos dados
- ◯ 4. Não sabe/Não aplicável

48. **28. Os sistemas estão configurados apenas com os serviços necessários?** *

Marcar apenas uma oval.

- ◯ 1. Os sistemas são configurados com os recursos necessários de forma não sistematizada
- ◯ 2. Estão estabelecidas as funcionalidades mínimas para cada operação e sistema
- ◯ 3. Os requisitos mínimos são revistos e atualizados regularmente
- ◯ 4. Não sabe/Não aplicável

49. **29. As redes de comunicações e de controlo são protegidas?** *

Marcar apenas uma oval.

- ◯ 1. As zonas de rede são segregadas de forma não sistematizada
- ◯ 2. As zonas de rede são segmentadas conforme a finalidade
- ◯ 3. São realizadas revisões regulares das definições e dos sistemas de segurança definidos (IDS/IPS, firewalls, proxies, WAFs)
- ◯ 4. Não sabe/Não aplicável

50. **30. São implementados mecanismos de resiliência em situações adversas?** *

Marcar apenas uma oval.

- ◯ 1. A incorporação de resiliência nos sistemas e redes de comunicações é aplicada de forma não sistematizada
- ◯ 2. Os sistemas críticos são resilientes
- ◯ 3. A resiliência das infraestruturas às situações adversas é gerida para garantir a alta-disponibilidade nos sistemas críticos
- ◯ 4. Não sabe/Não aplicável

CAPACIDADE DE DETETAR

Definição e implementação de medidas destinadas a identificar, de forma atempada, os incidentes. Ou seja, a deteção de eventos com um efeito adverso real na segurança das redes e dos sistemas de informação (CNCS, 2020).
(Selecione a opção em que melhor se enquadra à sua organização)

51. **1. Os eventos detetados são analisados para se identificarem os alvos e os métodos de ataque?** *

Marcar apenas uma oval.

- ◯ 1. É realizada uma análise ad hoc dos eventos, sem procedimento de tratamento formalizado e implementado
- ◯ 2. São detetadas tentativas de ataques e os incidentes são registados (alvos e métodos de ataque identificados)
- ◯ 3. Existe um tratamento transversal de todos os eventos de segurança e existe resposta apropriada aos incidentes detetados
- ◯ 4. Não sabe/Não aplicável

52. **2. Os eventos são coletados e correlacionados a partir de várias fontes e sensores?** *

Marcar apenas uma oval.

- ◯ 1. O registo de eventos é coletado num sistema central
- ◯ 2. Os eventos de segurança são geridos e analisados
- ◯ 3. Estão estabelecidos mecanismos de controlo de eventos de segurança nas infraestruturas
- ◯ 4. Não sabe/Não aplicável

53. **3. O impacto dos eventos é classificado?** *

Marcar apenas uma oval.

- ◯ 1. Os eventos de segurança são classificados conforme o seu impacto percebido
- ◯ 2. Existe um processo formal de gestão de eventos com procedimentos para aferir o impacto de um evento
- ◯ 3. A gestão de incidentes é acionada a partir da gestão de eventos e os eventos classificados como graves geram incidentes de segurança
- ◯ 4. Não sabe/Não aplicável

54. **4. As redes e sistemas de informação são monitorizados para detetar potenciais incidentes?** *

Marcar apenas uma oval.

- ◯ 1. A monitorização é realizada sem um sistema automático de deteção ou com deteção manual
- ◯ 2. Existe monitorização e proteção de comportamentos anómalos que possam representar incidentes
- ◯ 3. Os eventos de segurança são detetados e são correlacionados com múltiplas fontes
- ◯ 4. Não sabe/Não aplicável

55. **5. Os ambientes físicos são monitorizados para se detetar potenciais incidentes de segurança?** *

Marcar apenas uma oval.

- ◯ 1. São feitos registos ad hoc de deteção de incidentes de segurança física
- ◯ 2. Existem controlos implementados de monitorização de áreas seguras
- ◯ 3. Os acessos físicos às áreas seguras são auditados regularmente para detetar não-conformidades
- ◯ 4. Não sabe/Não aplicável

56. **6. A atividade dos colaboradores é monitorizada para se detetar potenciais incidentes?** *

Marcar apenas uma oval.

- ◯ 1. A atividade dos colaboradores é monitorizada de forma ad hoc
- ◯ 2. Estão estabelecidos padrões fiáveis de monitorização de colaboradores
- ◯ 3. É feita uma análise de tendências e deteção de padrões anómalos à atividade dos colaboradores, que permite antecipar incidentes
- ◯ 4. Não sabe/Não aplicável

57. **7. O código malicioso é detetado?** *

Marcar apenas uma oval.

- ◯ 1. A deteção da presença de código malicioso na infraestrutura é reativa
- ◯ 2. Estão estabelecidas regras formais de avaliação de códigos maliciosos e são feitas verificações periódicas à integridade do código
- ◯ 3. Há integração do sistema de antivírus com o sistema central de gestão de eventos de segurança
- ◯ 4. Não sabe/Não aplicável

58. **8. As aplicações não autorizadas em dispositivos móveis são detetadas?** *

Marcar apenas uma oval.

- ◯ 1. As aplicações em dispositivos móveis da organização são monitorizadas de forma não sistematizada
- ◯ 2. Existe uma lista de aplicações permitidas e não permitidas em local de fácil acesso e a lista é comunicada aos colaboradores
- ◯ 3. A gestão dos equipamentos móveis e as suas aplicações são feitas através de sistema centralizado
- ◯ 4. Não sabe/Não aplicável

59. **9. As atividades dos prestadores de serviços são monitorizadas?** *

Marcar apenas uma oval.

- ◯ 1. As atividades dos prestadores de serviços externos são monitorizadas e a deteção de incidentes é manual e não sistematizada
- ◯ 2. Os pedidos de acesso remoto são identificados e avaliados
- ◯ 3. Os acessos e permissões concedidas a prestadores de serviços externos são avaliados regularmente e é realizada a avaliação dos eventos relativos aos acessos externos
- ◯ 4. Não sabe/Não aplicável

60. **10. As vulnerabilidades dos ativos são detetadas automaticamente?** *

Marcar apenas uma oval.

- ◯ 1. A pesquisa por vulnerabilidades nos sistemas e redes de comunicação é feita pontualmente
- ◯ 2. As vulnerabilidades identificadas nos sistemas e redes de comunicação são analisadas regularmente
- ◯ 3. A análise de vulnerabilidades está integrada com processos de testes e análises de segurança em sistemas e aplicações
- ◯ 4. Não sabe/Não aplicável

61. **11. Estão definidos os papéis e as responsabilidades na deteção de eventos anómalos?** *

Marcar apenas uma oval.

- ◯ 1. As responsabilidades estão informalmente definidas
- ◯ 2. Estão identificados os responsáveis pelo tratamento dos eventos anómalos
- ◯ 3. Estão estabelecidas as responsabilidades no processo de deteção de eventos anómalos
- ◯ 4. Não sabe/Não aplicável

62. **12. Os processos de deteção são testados?** *

Marcar apenas uma oval.

- ◯ 1. Os processos de deteção são medidos de forma ad hoc
- ◯ 2. Existe um processo sistemático de avaliação da eficácia dos processos de deteção
- ◯ 3. Existe um processo de melhoria contínua que atesta a integridade e fiabilidade dos mecanismos de deteção
- ◯ 4. Não sabe/Não aplicável

63. **13. As deteções de eventos são comunicadas?** *

Marcar apenas uma oval.

- ◯ 1. Os eventos de segurança são reportados internamente e de forma informal
- ◯ 2. Estão estabelecidos internamente os canais formais de comunicação e os incidentes detetados são registados adequadamente
- ◯ 3. Existe uma plataforma central onde é coordenada a resposta a incidentes de segurança
- ◯ 4. Não sabe/Não aplicável

CAPACIDADE DE RESPONDER

Definição e implementação de medidas de ação apropriadas, em caso de deteção de um incidente. As medidas propostas no âmbito deste objetivo pretendem mitigar o impacto do incidente, ou seja, reduzir os seus potenciais efeitos adversos (CNCS, 2020).
(Selecione a opção em que melhor se enquadra à sua organização)

64. **1. Os planos de resposta são executados durante ou após a ocorrência de um incidente?** *

Marcar apenas uma oval.

- ◯ 1. São implementados procedimentos ad hoc de resposta a incidentes, de forma reativa
- ◯ 2. Os processos de resposta são executados, sistematizados e incluem as fases de contenção e erradicação e a identificação dos diversos responsáveis e o escalonamento
- ◯ 3. É garantida a integridade das evidências analisadas
- ◯ 4. Não sabe/Não aplicável

65. **2. Os colaboradores conhecem as suas responsabilidades na resposta a um incidente?** *

Marcar apenas uma oval.

- ◯ 1. Existe conhecimento informal e não estruturado das funções de cada interveniente da organização
- ◯ 2. Os colaboradores têm conhecimento sobre os procedimentos e responsabilidades e estão estabelecidos os guiões de resposta a incidentes
- ◯ 3. As partes externas relevantes são envolvidas na resposta a incidentes
- ◯ 4. Não sabe/Não aplicável

66. **3. Existem critérios para reportar incidentes?** *

Marcar apenas uma oval.

- ◯ 1. Existe conhecimento informal e não estruturado dos canais de reporte de incidentes
- ◯ 2. Estão estabelecidos critérios de reporte de incidentes
- ◯ 3. Estão estabelecidos critérios para envolver as partes interessadas externas no tratamento dos incidentes
- ◯ 4. Não sabe/Não aplicável

67. **4. As informações são partilhadas de acordo com o plano de resposta?** *

Marcar apenas uma oval.

- ◯ 1. É realizado registo das partes interessadas, internas e externas, na comunicação de incidentes de forma não estruturada
- ◯ 2. Há um plano de comunicação de incidentes
- ◯ 3. Estão estabelecidos canais seguros para comunicação de incidentes e as partes externas interessadas estão envolvidas na resposta no tratamento dos incidentes
- ◯ 4. Não sabe/Não aplicável

68. **5. A coordenação com as partes interessadas ocorre conforme os planos de resposta?** *

Marcar apenas uma oval.

- ◯ 1. A comunicação com as partes interessadas é feita de forma ad hoc
- ◯ 2. Existe identificação das partes interessadas externas e coordenação com as mesmas
- ◯ 3. Estão estabelecidos níveis de responsabilização na resposta a incidentes e é realizada análise e avaliação dos registos de comunicação em referência aos critérios estabelecidos
- ◯ 4. Não sabe/Não aplicável

69. **6. Existe partilha voluntária de informação com partes interessadas externas?** *

Marcar apenas uma oval.

- ◯ 1. A partilha voluntária de informação é feita de forma informal e não estruturada
- ◯ 2. Estão identificadas as partes interessadas externas e respetivos pontos de contacto em registo atualizado
- ◯ 3. Existe um plano de comunicação que regula as necessidades de comunicação externas e documentos de apoio do plano de comunicação voluntária de incidentes
- ◯ 4. Não sabe/Não aplicável

70. **7. As notificações dos sistemas de deteção são investigadas?** *

Marcar apenas uma oval.

- ◯ 1. Existe registo de notificações de eventos elevados a incidentes, ainda que não estruturado
- ◯ 2. As deteções são investigadas segundo o plano de resposta a incidentes
- ◯ 3. Existe uma plataforma central de gestão de correlação de eventos, onde as notificações são analisadas transversalmente
- ◯ 4. Não sabe/Não aplicável

71. **8. O impacto dos incidentes é avaliado?** *

Marcar apenas uma oval.

- 1. O impacto dos incidentes é avaliado de forma informal e não estruturada
- 2. Os incidentes de segurança são categorizados pelo nível de impacto percebido
- 3. O risco dos incidentes é analisado e são estabelecidas métricas relativas à resposta e tratamento de incidentes
- 4. Não sabe/Não aplicável

72. **9. São realizadas análises forenses?** *

Marcar apenas uma oval.

- 1. As análises forenses são feitas de forma não estruturada
- 2. Estão definidos procedimentos de identificação, coleta e aquisição de registos e informações, e existem procedimentos para a captura dos dados no seu formato original, para análise forense
- 3. A integridade e cadeia de custódia das evidências recolhidas são garantidas e existem meios específicos para a realização de análises forenses
- 4. Não sabe/Não aplicável

73. **10. Existem processos para receber, analisar e responder a vulnerabilidades provenientes de fontes internas e externas?** *

Marcar apenas uma oval.

- 1. Existe processo ad hoc para submissão de vulnerabilidades
- 2. Existem mecanismos para que a organização seja informada sobre vulnerabilidades, de forma interna ou externa, e estão estabelecidos processos de tratamento às vulnerabilidades sobre as quais a organização é informada
- 3. As vulnerabilidades registadas são analisadas e avaliadas sistematicamente
- 4. Não sabe/Não aplicável

74. **11. Os incidentes são contidos?** *

Marcar apenas uma oval.

- ◯ 1. A resposta aos incidentes de segurança é feita de forma não sistematizada
- ◯ 2. Estão estabelecidos processos de resposta aos incidentes
- ◯ 3. As causas para a origem de incidentes são analisadas e avaliadas
- ◯ 4. Não sabe/Não aplicável

75. **12. Os incidentes são mitigados?** *

Marcar apenas uma oval.

- ◯ 1. O tratamento dos incidentes é efetuado de forma reativa e não estruturada
- ◯ 2. Estão estabelecidas práticas para a redução do impacto dos incidentes e existem procedimentos que documentam a mitigação de incidentes
- ◯ 3. Os incidentes são erradicados e é feita uma análise do tratamento dos incidentes para efeitos de melhoria contínua
- ◯ 4. Não sabe/Não aplicável

76. **13. As vulnerabilidades identificadas são mitigadas ou documentadas como riscos aceites?** *

Marcar apenas uma oval.

- ◯ 1. O tratamento das vulnerabilidades é avaliado de forma não estruturada
- ◯ 2. Existe um registo de riscos formalmente aceites e um processo de gestão de vulnerabilidades implementado
- ◯ 3. Existe um processo de análise de risco às vulnerabilidades
- ◯ 4. Não sabe/Não aplicável

CAPACIDADE DE RECUPERAR

Definição e implementação de atividades, que visam a gestão de planos e medidas de recuperação dos processos e serviços afetados por um incidente de cibersegurança. As medidas pertencentes a este objetivo pretendem assegurar a resiliência da organização nas suas dimensões: Pessoas, Processos e Tecnologia. E que, no caso de existência de um incidente, a organização consiga utilizar as medidas para suporte à recuperação em tempo útil da sua atividade (CNCS, 2020).
(Selecione a opção em que melhor se enquadra à sua organização)

77. **1. A organização segue um plano de recuperação durante ou após um incidente?** *

Marcar apenas uma oval.

- 1. Existem procedimentos ad hoc de cópias de segurança
- 2. Estão formalizadas regras e procedimentos para recuperação de incidentes com recurso a cópias de segurança e está estabelecido um processo de gestão de cópias de segurança
- 3. Existe uma equipa dedicada ao tratamento e recuperação de incidentes e são implementadas ações preditivas para dar respostas adequadas
- 4. Não sabe/Não aplicável

78. **2. Está implementado um plano de comunicação?** *

Marcar apenas uma oval.

- ◯ 1. A comunicação às partes interessadas sobre eventos de segurança é reativa
- ◯ 2. Está estabelecido um plano de comunicação sobre eventos de segurança e as partes interessadas relevantes estão identificadas
- ◯ 3. São realizadas ações de consciencialização proativamente
- ◯ 4. Não sabe/Não aplicável

79. **3. As atividades de recuperação são comunicadas às partes interessadas, internas e externas, bem como às equipas executivas e de gestão?** *

Marcar apenas uma oval.

- ◯ 1. A comunicação é efetuada de forma reativa e não estruturada
- ◯ 2. Está estabelecido um plano de comunicação e para cada objetivo a ser comunicado é efetuada a identificação de audiência
- ◯ 3. Está estabelecida uma estratégia de comunicação adequada para as equipas executivas e de gestão
- ◯ 4. Não sabe/Não aplicável

Anexo II – Questionário (respostas)

Respostas ao Questionário

Legenda

Individuo	Setor
I1	Gestão de serviços TIC (entre empresas)
I2	Prestadores de serviços digitais
I3	Investigação
I4	Gestão de serviços TIC (entre empresas)
I5	Administração pública
I6	Gestão de resíduos
I7	Outros
I8	Setor bancário
I9	Administração pública
I10	Setor bancário
I11	Administração pública
I12	Prestadores de serviços digitais
I13	Outros
I14	Prestadores de serviços digitais
I15	Prestadores de serviços digitais
I16	Gestão de serviços TIC (entre empresas)
I17	Outros
I18	Gestão de resíduos
I19	Infraestruturas digitais
I20	Administração pública
I21	Outros
I22	Gestão de resíduos
I23	Administração pública
I24	Setor bancário
I25	Energia
I26	Outros
I27	Prestadores de serviços digitais
I28	Água potável
I29	Outros
I30	Administração pública

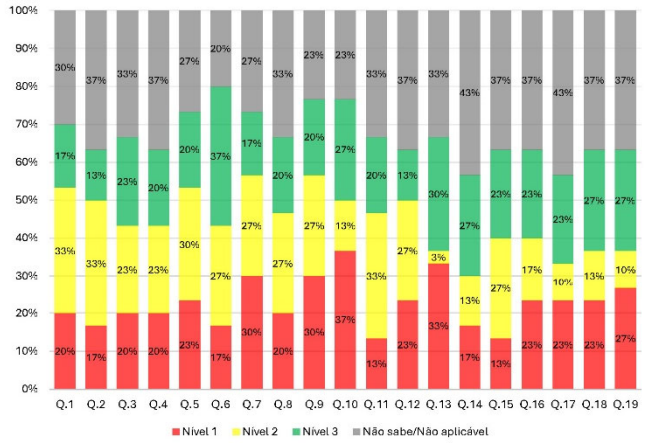
Capacidade de Identificar

Individuo	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13	Q.14	Q.15	Q.16	Q.17	Q.18	Q.19
I1	2	2	2	2	2	3	2	3	3	2	1	1	1	3	3	1	4	1	4
I2	3	2	3	2	2	2	3	2	1	3	3	2	3	3	3	3	3	3	3
I3	2	2	2	1	1	3	1	1	2	1	2	2	1	1	1	1	1	1	1
I4	3	2	3	2	3	3	2	2	3	3	3	2	3	3	3	3	3	2	1
I5	2	2	2	2	2	3	2	3	2	3	2	2	3	2	2	2	3	3	2
I6	2	4	1	1	2	4	1	1	4	1	3	1	4	3	1	4	1	1	1
I7	4	4	4	4	4	4	4	4	4	4	4	4	4	4	1	1	1	4	4
I8	3	2	2	3	2	3	2	2	2	4	2	3	2	2	1	2	2	3	2
I9	1	1	1	1	1	3	1	4	2	1	1	1	1	1	2	1	1	1	1
I10	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
I11	2	1	2	1	1	3	1	4	2	1	2	1	1	3	4	1	1	1	1
I12	2	3	3	2	3	3	2	2	2	3	2	3	3	2	2	3	3	3	3
I13	1	1	1	4	2	4	1	3	1	1	2	4	1	4	2	1	4	4	1
I14	4	4	4	4	3	4	2	3	4	4	4	4	4	4	4	4	4	3	4
I15	2	2	3	3	2	2	2	2	1	2	2	2	3	2	2	2	2	2	2
I16	4	4	4	4	4	1	3	4	1	1	4	4	1	4	4	4	1	4	4
I17	4	4	4	4	4	2	4	4	4	4	4	4	4	4	4	4	4	4	4
I18	4	4	4	4	4	2	4	4	1	1	4	1	4	4	4	4	4	4	4
I19	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
I20	4	4	2	1	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4
I21	1	4	4	4	3	1	1	1	1	1	1	4	3	4	2	4	4	4	3
I22	4	4	4	4	4	1	4	4	4	4	4	4	4	4	4	4	4	4	4
I23	1	4	4	4	1	2	4	4	1	4	4	4	4	4	4	4	4	4	4
I24	2	2	3	3	4	2	4	2	2	2	3	4	4	4	3	3	4	4	4
I25	2	3	1	3	2	3	3	2	3	3	2	2	3	3	3	3	3	2	3
I26	4	4	4	4	4	4	4	4	2	3	4	2	4	4	4	4	4	4	4
I27	4	2	4	4	4	1	2	1	4	1	4	1	1	1	4	4	4	1	1
I28	2	2	1	1	2	2	1	1	1	2	2	2	1	1	2	2	1	2	3
I29	1	1	2	2	1	2	1	2	3	1	1	1	1	1	2	2	2	3	3

Individuo	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13	Q.14	Q.15	Q.16	Q.17	Q.18	Q.19
I30	1	1	1	2	1	1	1	1	1	1	2	4	1	4	4	1	4	1	1

Percentagem das respostas por nível de maturidade

Nível	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13	Q.14	Q.15	Q.16	Q.17	Q.18	Q.19
Nível 1	20%	17%	20%	20%	23%	17%	30%	20%	30%	37%	13%	23%	33%	17%	13%	23%	23%	23%	27%
Nível 2	33%	33%	23%	23%	30%	27%	27%	27%	27%	13%	33%	27%	3%	13%	27%	17%	10%	13%	10%
Nível 3	17%	13%	23%	20%	20%	37%	17%	20%	20%	27%	20%	13%	30%	27%	23%	23%	23%	27%	27%
Não sabe/Não aplicável	30%	37%	33%	37%	27%	20%	27%	33%	23%	23%	33%	37%	33%	43%	37%	37%	43%	37%	37%



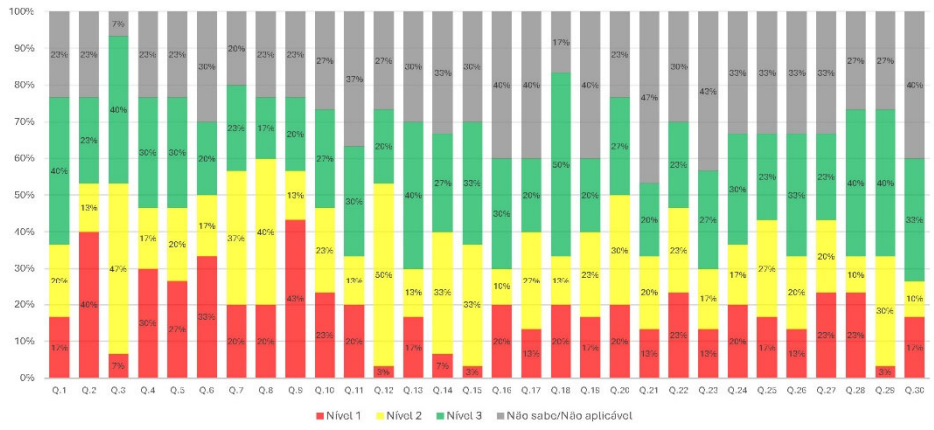
Capacidade de Proteger

Indivíduo	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13	Q.14	Q.15	Q.16	Q.17	Q.18	Q.19	Q.20	Q.21	Q.22	Q.23	Q.24	Q.25	Q.26	Q.27	Q.28	Q.29	Q.30
I1	3	3	2	2	2	1	2	2	3	2	2	2	3	1	3	2	2	3	2	2	2	4	4	1	2	4	1	3	2	4
I2	3	3	2	3	3	2	2	3	2	2	2	2	3	2	3	2	2	3	2	2	2	2	2	3	3	3	2	3	3	3
I3	1	4	2	2	1	1	1	1	1	1	1	2	1	2	2	1	1	2	1	1	1	1	4	2	2	2	2	1	2	1
I4	3	1	3	2	3	3	3	3	1	2	3	3	3	3	3	3	2	3	3	3	3	3	3	3	3	3	3	3	3	3
I5	2	2	3	4	1	2	2	2	1	1	2	3	2	3	3	3	3	3	2	2	3	2	3	2	2	3	2	3	3	3
I6	3	1	3	1	1	4	1	2	1	4	1	2	3	2	2	4	1	3	4	2	1	1	1	1	2	4	1	3	2	1
I7	4	1	1	4	4	4	4	1	4	4	4	4	4	4	4	4	4	1	1	4	4	4	4	4	4	4	1	1	1	4
I8	1	1	3	3	3	2	2	2	2	2	1	2	3	2	2	3	2	3	2	2	2	3	2	3	2	2	2	2	2	2
I9	3	2	2	2	2	1	3	1	3	1	3	2	2	2	1	1	2	3	1	1	2	2	1	2	1	2	2	1	2	3
I10	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
I11	2	1	3	1	1	1	2	2	1	1	1	2	1	2	2	1	2	2	1	1	4	1	1	1	1	2	4	1	3	4
I12	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
I13	3	2	3	3	1	1	1	1	1	1	3	2	3	2	2	4	1	1	3	3	1	1	2	1	2	1	1	3	3	2
I14	3	3	3	3	3	1	2	2	3	3	4	4	3	4	4	4	4	1	4	2	4	3	4	4	3	4	4	4	4	4
I15	2	1	2	3	2	2	2	2	1	2	3	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2
I16	3	4	3	4	4	4	4	4	1	4	4	4	4	4	2	1	4	1	4	3	4	2	3	1	1	1	4	1	4	4
I17	4	4	4	4	4	3	3	4	1	1	4	2	1	2	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
I18	4	1	2	1	3	4	4	4	4	4	4	4	4	4	4	4	4	3	4	4	4	1	4	4	4	3	4	4	3	4
I19	3	3	3	1	2	2	2	2	2	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
I20	4	4	2	4	3	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
I21	2	4	2	1	1	4	1	4	2	3	4	2	1	2	2	3	4	1	4	1	4	1	4	4	4	4	1	1	2	1
I22	1	1	1	1	4	4	4	1	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
I23	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4	4
I24	4	2	2	1	2	3	3	2	1	2	3	2	2	3	4	4	4	3	2	3	4	2	3	3	4	3	3	3	3	3
I25	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3	3
I26	2	1	2	4	4	1	2	2	4	1	4	4	4	4	4	4	4	2	4	2	4	1	4	4	4	2	4	4	4	4
I27	4	4	2	1	4	1	1	4	1	3	1	1	4	4	4	1	1	4	4	4	4	4	4	4	4	4	4	4	4	4
I28	1	1	2	2	1	1	2	2	1	2	2	2	3	1	2	1	3	3	2	1	1	2	1	2	2	3	1	1	2	1
I29	1	1	2	3	1	4	1	1	4	4	1	2	4	4	2	4	4	1	1	1	2	4	4	1	1	1	3	2	2	1

Indivíduo	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13	Q.14	Q.15	Q.16	Q.17	Q.18	Q.19	Q.20	Q.21	Q.22	Q.23	Q.24	Q.25	Q.26	Q.27	Q.28	Q.29	Q.30
I30	2	1	2	1	2	1	2	2	1	3	4	2	1	3	3	3	2	3	4	2	4	4	2	3	1	1	1	3	3	3

Percentagem das respostas por nível de maturidade

Nível	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13	Q.14	Q.15	Q.16	Q.17	Q.18	Q.19	Q.20	Q.21	Q.22	Q.23	Q.24	Q.25	Q.26	Q.27	Q.28	Q.29	Q.30
Nível 1	17%	40%	7%	30%	27%	33%	20%	20%	43%	23%	20%	3%	17%	7%	3%	20%	13%	20%	17%	20%	13%	23%	13%	20%	17%	13%	23%	23%	3%	17%
Nível 2	20%	13%	47%	17%	20%	17%	37%	40%	13%	23%	13%	50%	13%	33%	33%	10%	27%	13%	23%	30%	20%	23%	17%	17%	27%	20%	20%	10%	30%	10%
Nível 3	40%	23%	40%	30%	30%	20%	23%	17%	20%	27%	30%	20%	40%	27%	33%	30%	20%	50%	20%	27%	20%	23%	27%	30%	23%	33%	23%	40%	40%	33%
Não sabe/Não aplicável	23%	23%	7%	23%	23%	30%	20%	23%	23%	27%	37%	27%	30%	33%	30%	40%	40%	17%	40%	23%	47%	30%	43%	33%	33%	33%	33%	27%	27%	40%



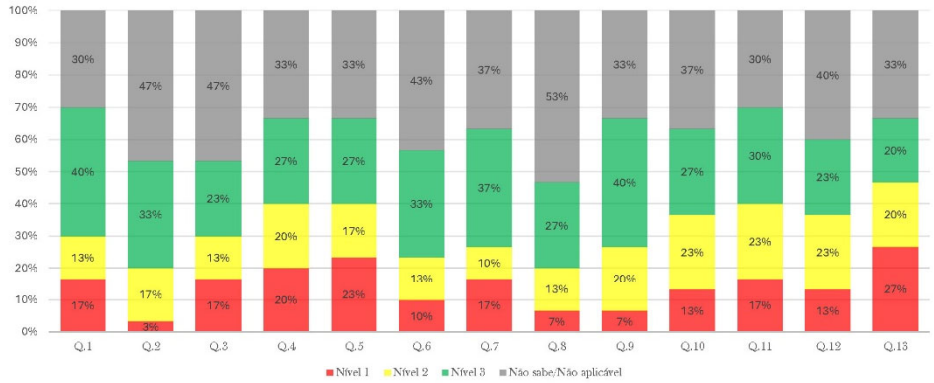
Capacidade de Detetar

Individuo	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13
I1	3	2	1	1	1	1	3	4	2	1	3	1	1
I2	3	3	2	2	2	2	2	2	2	2	2	2	2
I3	2	2	1	2	1	4	1	4	1	1	2	1	2
I4	3	3	3	3	3	3	3	3	3	3	3	3	3
I5	3	3	3	3	3	3	3	2	2	2	2	3	2
I6	1	4	4	2	1	3	3	4	3	2	2	2	1
I7	4	4	4	4	4	4	4	4	4	4	4	4	4
I8	1	2	2	1	3	3	1	3	3	1	3	2	2
I9	1	1	1	1	1	1	1	1	1	1	1	1	1
I10	3	3	3	3	3	3	3	3	3	3	3	3	3
I11	2	2	1	2	2	2	2	4	2	2	1	1	1
I12	3	3	3	3	3	3	3	3	3	3	3	3	3
I13	1	3	1	3	2	3	1	4	3	2	2	2	1
I14	4	4	4	4	4	4	4	4	4	4	4	4	4
I15	3	3	2	3	2	2	3	3	3	3	3	2	2
I16	2	4	4	2	4	4	4	4	4	4	2	4	4
I17	4	4	4	4	4	4	4	4	4	4	4	4	4
I18	4	4	4	4	4	4	3	2	3	4	4	4	4
I19	3	3	3	3	3	3	3	3	3	3	3	3	3
I20	4	4	4	4	4	4	4	4	4	4	4	4	4
I21	4	4	4	1	1	4	4	4	4	4	1	4	1
I22	4	4	4	4	4	4	4	4	4	4	4	4	4
I23	4	4	4	4	4	4	4	4	4	4	4	4	4
I24	3	4	4	4	3	3	4	3	3	3	3	3	3
I25	3	3	3	3	3	3	3	3	3	3	3	3	3
I26	2	4	4	4	4	4	4	4	4	4	4	4	4
I27	4	4	4	4	4	4	4	4	4	4	4	4	4
I28	3	2	2	2	1	2	3	2	2	3	2	2	1
I29	1	4	4	1	2	4	1	1	2	2	1	4	1

Individuo	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13
I30	3	3	3	1	1	1	2	4	3	2	1	2	2

Percentagem das respostas por nível de maturidade

Nível	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13
Nível 1	17%	3%	17%	20%	23%	10%	17%	7%	7%	13%	17%	13%	27%
Nível 2	13%	17%	13%	20%	17%	13%	10%	13%	20%	23%	23%	23%	20%
Nível 3	40%	33%	23%	27%	27%	33%	37%	27%	40%	27%	30%	23%	20%
Não sabe/Não aplicável	30%	47%	47%	33%	33%	43%	37%	53%	33%	37%	30%	40%	33%



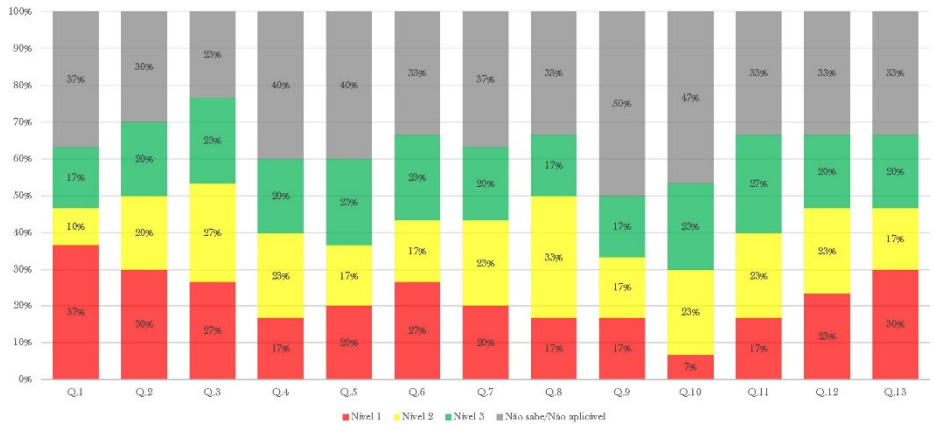
Capacidade de Responder

Individuo	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13
I1	1	2	1	2	1	1	2	2	4	1	3	2	2
I2	2	2	2	2	2	2	2	2	2	3	3	3	3
I3	1	1	2	2	2	2	2	2	1	2	1	2	1
I4	3	3	3	3	3	3	3	3	2	3	3	3	3
I5	2	2	2	2	4	3	2	2	2	2	2	2	2
I6	1	1	1	1	1	2	1	2	4	3	2	2	1
I7	4	4	4	4	4	4	4	4	4	4	4	4	4
I8	1	3	2	2	2	3	2	2	3	2	2	2	2
I9	1	1	1	1	1	1	1	1	1	1	1	1	1
I10	3	3	3	3	3	3	3	3	3	3	3	3	3
I11	1	1	2	1	1	1	1	2	1	2	2	1	1
I12	3	2	3	3	3	3	3	3	3	2	3	3	3
I13	1	3	3	1	2	1	1	1	1	4	3	1	1
I14	4	2	4	4	4	4	4	4	4	4	4	4	4
I15	2	2	2	3	3	2	2	2	2	2	2	2	2
I16	4	1	1	4	4	1	1	1	1	4	1	1	1
I17	4	4	4	4	4	4	4	4	4	4	4	4	4
I18	4	4	1	4	4	4	4	4	4	4	4	4	4
I19	3	3	3	3	3	3	3	3	3	3	3	3	3
I20	4	4	4	4	4	4	4	4	4	4	4	4	4
I21	1	4	1	4	4	1	4	1	4	4	2	1	1
I22	4	4	4	4	4	4	4	4	4	4	4	4	4
I23	4	4	4	4	4	4	4	4	4	4	4	4	4
I24	4	4	4	4	3	4	4	4	4	4	4	4	4
I25	3	3	3	3	3	3	3	3	3	3	3	3	3
I26	4	4	2	4	4	4	4	4	4	4	4	4	4
I27	4	1	1	1	4	4	4	4	4	4	4	4	4
I28	1	1	3	2	2	2	2	2	2	3	2	2	2
I29	1	1	2	2	1	1	1	1	4	4	1	1	1

Individuo	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13
I30	1	1	1	4	1	1	3	2	4	2	1	1	1

Percentagem das respostas por nível de maturidade

Nível	Q.1	Q.2	Q.3	Q.4	Q.5	Q.6	Q.7	Q.8	Q.9	Q.10	Q.11	Q.12	Q.13
Nível 1	37%	30%	27%	17%	20%	27%	20%	17%	17%	7%	17%	23%	30%
Nível 2	10%	20%	27%	23%	17%	17%	23%	33%	17%	23%	23%	23%	17%
Nível 3	17%	20%	23%	20%	23%	23%	20%	17%	17%	23%	27%	20%	20%
Não sabe/Não aplicável	37%	30%	23%	40%	40%	33%	37%	33%	50%	47%	33%	33%	33%



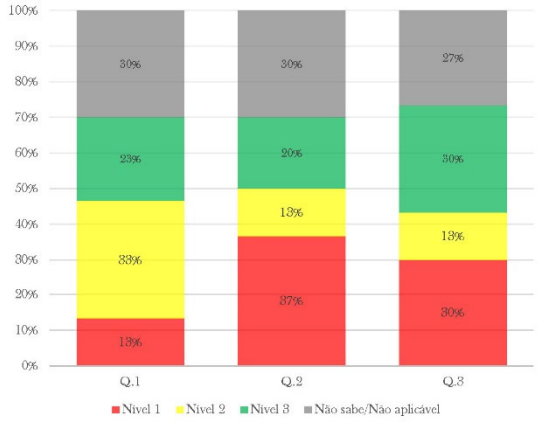
Capacidade de Recuperar

Indivíduo	Q.1	Q.2	Q.3
I1	2	1	1
I2	2	2	2
I3	1	1	1
I4	3	3	3
I5	3	3	3
I6	2	1	1
I7	4	4	4
I8	1	1	1
I9	2	1	1
I10	3	3	3
I11	1	1	1
I12	2	3	3
I13	2	1	1
I14	4	4	3
I15	2	2	2
I16	4	1	1
I17	4	4	4
I18	4	4	4
I19	3	3	3
I20	4	4	4
I21	1	1	4
I22	4	4	4
I23	4	4	4
I24	3	4	3
I25	3	3	3
I26	3	2	2
I27	4	4	4
I28	2	2	2
I29	2	1	1

Indivíduo	Q.1	Q.2	Q.3
I30	2	1	3

Percentagem das respostas por nível de maturidade

Nível	Q.1	Q.2	Q.3
Nível 1	13%	37%	30%
Nível 2	33%	13%	13%
Nível 3	23%	20%	30%
Não sabe/Não aplicável	30%	30%	27%


100%
90%
80%
70%
60%
50%
40%
30%
20%
10%
0%
30%
23%
33%
13%
30%
20%
13%
37%
27%
30%
13%
30%
Q.1
Q.2
Q.3
Nível 1
Nível 2
Nível 3
Não sabe/Não aplicável

Anexo III – Entrevistas (perguntas)

Entrevista

1. Conhecimento e Adoção da Diretiva NIS2

- A sua organização está ciente da Diretiva NIS2 e dos requisitos que ela impõe?
- Quem na sua organização é responsável por acompanhar as normas e regulamentações relacionadas com a cibersegurança, incluindo a NIS2?
- A sua organização já iniciou a implementação das medidas previstas pela NIS2?
- Qual é o grau de conhecimento da empresa (área de SI e gestão/administração) sobre os requisitos específicos da NIS2?

2. Implementação dos Requisitos

- Quais requisitos da NIS2 foram implementados até agora na sua organização?
- Houve alguma dificuldade técnica ou organizacional na implementação desses requisitos?
- Quais as áreas em que foi mais difícil avançar na implementação (por exemplo, sistemas de deteção, gestão de riscos, notificações de incidentes)?
- A sua organização já estabeleceu uma gestão formal de incidentes de cibersegurança conforme exigido pela NIS2?
- Foi necessário reforçar ou alterar alguma infraestrutura tecnológica para cumprir a Diretiva?

3. Desafios Enfrentados

- Quais foram as principais dificuldades encontradas durante o processo de adaptação à NIS2?

- Aspetos técnicos?
- Aspetos financeiros?
- Capacitação e formação de recursos humanos?
- Integração com outras normas de cibersegurança?

- A sua organização teve algum desafio relacionado com a colaboração com fornecedores ou parceiros em conformidade com a NIS2?

4. Impactos nos Processos Organizacionais, Técnicos e Operacionais

- De que forma a implementação da NIS2 afetou os processos organizacionais dentro da sua organização?
  - Reestruturação de políticas de segurança?
  - Alocação de recursos?
  - Planeamento e governação?
- Que impactos a NIS2 trouxe para a sua arquitetura técnica e para as soluções de cibersegurança em uso?
- Quais foram as mudanças nos processos operacionais, como resposta a incidentes ou na gestão de dados críticos?
- A sua organização tem recursos (técnicos e financeiros) suficientes para garantir a conformidade contínua com a NIS2?

Anexo IV – Entrevistas (respostas)

Entrevistado 1

RESPOSTAS AO QUESTIONÁRIO

1. Conhecimento e Adoção da Diretiva NIS2

A sua organização está ciente da Diretiva NIS2 e dos requisitos que ela impõe?

Sim, a organização tem pleno conhecimento da Diretiva NIS2 e dos seus requisitos. Desde a publicação da diretiva, temos acompanhado de perto os desenvolvimentos e preparado a nossa estratégia de implementação.

Quem na sua organização é responsável (cargo?) por acompanhar as normas e regulamentações relacionadas com a cibersegurança, incluindo a NIS2?

A responsabilidade está distribuída entre o CIO e o Responsável de Compliance, com supervisão direta da administração. Esta estrutura garante tanto a perspetiva técnica como a regulamentar.

A sua organização já iniciou a implementação das medidas previstas pela NIS2?

Sim, iniciámos um projeto estruturado de adequação no início de 2024, com planeamento faseado até ao final de 2025, antecipando-nos aos prazos legais.

Qual é o grau de conhecimento da empresa (áreas de Sistemas de Informação e de Gestão/Administração) sobre os requisitos específicos da NIS2?

O conhecimento está bem disseminado. Realizámos sessões de sensibilização para a gestão de topo e formação técnica específica para as equipas de TI. A área de gestão compreende os impactos estratégicos, enquanto a área técnica domina os requisitos operacionais.

2. Implementação dos Requisitos

Em que áreas da NIS2 a sua organização sente que já conseguiu avançar na implementação?

Conseguimos progressos significativos em:

- Gestão de vulnerabilidades com implementação de scanning automatizado
- Sistemas de backup e recuperação com testes regulares
- Monitorização de segurança através de SIEM centralizado
- Atualização das políticas de segurança
- Processos de gestão de incidentes

Houve alguma dificuldade técnica ou organizacional na implementação desses requisitos?

As principais dificuldades técnicas centraram-se na integração de sistemas legados com novas ferramentas de monitorização. Organizacionalmente, o maior desafio foi alinhar processos descentralizados com os novos requisitos centralizados de reporting e governação.

Quais as áreas em que foi mais difícil avançar na implementação (por exemplo, gestão de riscos, sistemas de deteção ou notificações de incidentes)?

A notificação de incidentes foi particularmente complexa, exigindo novos fluxos de comunicação com as autoridades competentes e definição precisa de critérios de classificação. A gestão da cadeia de fornecimento também se revelou desafiante, necessitando reavaliação de contratos existentes.

Foi necessário reforçar ou alterar alguma infraestrutura tecnológica para cumprir com os requisitos da Diretiva?

Sim, foi necessário investimento em:

- Plataforma SIEM/SOAR
- Ferramentas de gestão de vulnerabilidades
- Sistemas de backup geograficamente distribuídos
- Soluções de endpoint detection and response
- Ferramentas de network monitoring avançado

3. Desafios Enfrentados

Aspetos técnicos?

- Complexidade na integração de ferramentas de múltiplos fornecedores
- Necessidade de customização para as especificidades organizacionais
- Gestão de identidades em ambientes complexos
- Harmonização de logs e eventos de diferentes sistemas

Aspetos financeiros?

O investimento inicial foi considerável, especialmente em licensing de ferramentas especializadas e formação das equipas. Optimizámos custos através de parcerias estratégicas e aproveitamento de acordos quadro existentes.

Capacitação e formação de recursos humanos?

Implementámos:

- Programa de certificações em cibersegurança
- Workshops internos sobre NIS2
- Formação contínua em threat intelligence
- Desenvolvimento de competências internas de security operations
- Aproveitamos a formação gratuita da Universidade Aberta ao abrigo do PRR em diversas microcredenciais que robusteceram muitíssimo a capacidade dos nossos recursos humanos (por exemplo Diretores de Segurança Cibernética).

Integração com outras normas de cibersegurança?

A harmonização com frameworks existentes (ISO 27001, NIST) facilitou o processo, mas exigiu ajustes nos controlos para atender aos requisitos específicos da NIS2, particularmente nos tempos de notificação e critérios de reporte.

Outros?

Gestão de expectativas internas e comunicação das mudanças organizacionais necessárias foi um desafio transversal.

A sua organização teve algum desafio relacionado com a colaboração de fornecedores ou parceiros em conformidade com a NIS2?

Sim, alguns fornecedores críticos precisaram de tempo adicional para adequar os seus SLAs aos requisitos de notificação e reporting. Estabelecemos um programa de avaliação contínua e renegociação de contratos quando necessário.

4. Impactos nos processos Organizacionais, Técnicos e Operacionais

Na reestruturação de políticas de segurança?

Criámos um Comité de Cibersegurança multidisciplinar e revimos completamente as políticas de gestão de risco com foco específico em ciberameaças. Implementámos também novos processos de Business Continuity para cenários de ciberincidentes.

Na alocação de recursos?

Estabelecemos um orçamento dedicado exclusivamente à cibersegurança e criámos posições especializadas na equipa. A alocação passou a ser plurianual para garantir sustentabilidade dos investimentos.

No planeamento e governação?

A governação evoluiu para incluir reporting regular à administração sobre postura de cibersegurança, com dashboards executivos e KPIs específicos. O planeamento estratégico passou a integrar cenários de ciberrisco.

Outros?

Desenvolvimento de uma cultura organizacional de cibersegurança mais madura, com sensibilização regular de todos os colaboradores.

Que impactos a NIS2 trouxe para a sua arquitetura técnica e para as soluções de cibersegurança em uso?

A arquitetura está a evoluir para um modelo "security by design" com:

- Implementação progressiva de zero-trust architecture
- Micro-segmentação de rede

- Automatização de security operations
- Integração de threat intelligence em tempo real

A sua organização tem recursos (técnicos e financeiros) suficientes para garantir a conformidade contínua com a NIS2?

Criámos um modelo de financiamento sustentável através de orçamento plurianual, parcerias estratégicas e optimização através de automação. Do ponto de vista técnico, investimos no desenvolvimento de competências internas e estabelecemos parcerias com fornecedores especializados.

Entrevistado 2

From: gepesteves@sapo.pt
To:
Subject: Perspetiva pessoal de um (Advisor em GRC, Privacidade e Cibersegurança)
Date: 7 de outubro de 2025 15:54:11

Boa tarde, Pedro Esteves,

Partilho um resumo da minha perceção face as questões que colocou:

1. Conhecimento e Adoção da Diretiva NIS2

Pelo que tenho observado, muitas organizações já têm consciência da NIS2, mas ainda estão numa fase de interpretação e planeamento e/ou a aguardar que outras entidades avancem.
Normalmente, a responsabilidade pelo acompanhamento destas matérias está dividida entre as áreas de IT/Cybersecurity e Compliance/GRC.
Há casos em que o processo de implementação já começou, sobretudo com diagnósticos de maturidade e gap analysis, mas a maior parte das empresas ainda está a definir estratégia.
De forma geral, noto que a área técnica tem um nível de conhecimento mais sólido, enquanto a gestão e administração ainda está a familiarizar-se com o enquadramento e impacto regulatório, mas muito focados "na pressão" do artigo 20º.

2. Implementação dos Requisitos

As áreas onde se nota mais progresso são as de gestão de incidentes, governação e políticas internas de segurança e plano de continuidade do negócio.
As maiores dificuldades tendem a ser organizacionais, relacionadas com a definição de responsabilidades, e técnicas, no que toca à integração de ferramentas e processos de monitorização.
A parte de gestão de risco e notificação de incidentes continua a ser, para muitos, o "calcanhar de Aquiles".
Também tenho visto um reforço da infraestrutura tecnológica, sobretudo com soluções de deteção, resposta e gestão de vulnerabilidades e testes de resiliência: Pen-testing.

3. Desafios Enfrentados

Os desafios são variados, mas destacaria:

- Complexidade técnica na integração de sistemas; (Nomeadamente sistemas legacy)
- Limitações orçamentais, especialmente em PME;
- Falta de formação e sensibilização interna;
- E a coordenação com fornecedores, que muitas vezes não estão ao mesmo nível de maturidade.
  Há também o desafio cultural de transformar a conformidade com a NIS2 num processo contínuo e estratégico, e não apenas numa resposta pontual à legislação.

4. Impactos nos Processos Organizacionais, Técnicos e Operacionais

A NIS2 está a obrigar as empresas a rever políticas, redefinir papéis e reforçar a governação de cibersegurança e para quem implementou bem o RGPD tiram partido das

MTOs (Medidas Técnicas e Organizativas) e gestão de ativos.
Tem também impacto direto na alocação de recursos e no planeamento estratégico, já que a cibersegurança passou a estar mais presente nas decisões de gestão.
A nível técnico, há um movimento claro no sentido de modernizar arquiteturas e automatizar respostas e validar fornecedores / subcontratantes.
Ainda assim, o equilíbrio entre recursos e exigências continua a ser um ponto crítico especialmente para garantir conformidade e melhoria contínua a médio prazo.

Se pretender tem o meu consentimento para mencionar o meu nome assim como o desta Empresa/Grupo.

Abraço,

Entrevistado 3

From:
To: "Pedro Esteves"
Subject: RE: Pedro Esteves - Entrevista | Trabalho Final Mestrado
Date: 22 de setembro de 2025 10:00:19
Attachments:

Bom dia Pedro,

Preenchimento do questionário Infra.

-- QUESTIONÁRIO --

1. Conhecimento e Adoção da Diretiva NIS2

Sem entrar em detalhes confidenciais, gostava que perceber, de forma geral, qual o grau de conhecimento atual da sua organização em relação à NIS2, nomeadamente:

- A sua organização está ciente da Diretiva NIS2 e dos requisitos que ela impõe? **RM: Como consultora a EY presta serviços no âmbito de conformidade com regulamentação de Cibersegurança. Posto isto, foi um assunto que desde a sua origem despoletou nas nossas equipas europeias de cibersegurança a criação de uma *task-force* para avaliação da evolução das transposições realizadas pelos diferentes países da Europa, garantindo uma visão centralizada das normas e *standards* adotadas. De notar que muito embora as grandes organizações já demonstrem uma clara preocupação com o cumprimento com nova regulamentação, as pequenas e médias empresas parecem de alguma forma desprevenidas com o alargamento da abrangência da NIS2.**
- Quem na sua organização é responsável (cargo?) por acompanhar as normas e regulamentações relacionadas com a cibersegurança, incluindo a NIS2? **RM: No paradigma que observamos verificamos diferentes estados de maturidade nas organizações que iniciam a sua demonstração de preocupação com a regulamentação a entrar em vigor. Para diferentes sectores e dimensões organizacionais temos desde estruturas bem definidas hierarquicamente nas temáticas de segurança de informação, assim como organizações para as quais não existe ainda uma estrutura formal de segurança de informação. Posto isto a responsabilidade de acompanhamento de normas está estabelecida em organizações mais maduras, no entanto o que verificamos é que muitas das pequenas e médias empresas ainda não definem formalmente estas responsabilidades.**
- A sua organização já iniciou a implementação das medidas previstas pela NIS2?
- Qual é o grau de conhecimento da empresa (áreas de Sistemas de Informação e de Gestão/Administração) sobre os requisitos específicos da NIS2? RM: respondido na pergunta 1 – "A sua organização está ciente da Diretiva NIS2 e dos requisitos que ela impõe?".

2. Implementação dos Requisitos

Sem entrar em detalhes confidenciais, gostava que perceber, de forma geral, qual o ponto de

situação atual da sua organização em relação à implementação dos requisitos da NIS2, nomeadamente:

- Em que áreas da NIS2 a sua organização sente que já conseguiu avançar na implementação? **RM: A nossa experiencia dita-nos que existem diferentes áreas com lacunas em diferentes organizações, não obstante, parece-nos que os processos de gestão de terceiros e continuidade de negócio são um desafio claro para organizações que até ao momento não estavam abrangidas por uma regulamentação de segurança de informação baseada em Standards de referência.**
- Houve alguma dificuldade técnica ou organizacional na implementação desses requisitos? **RM: Diferentes dificuldades são observadas, muitas das vezes por falta de recursos humanos para realização das atividades, falta de experiencia ou ainda falta de recursos financeiros para colmatar lacunas em infraestruturas por vezes obsoletas.**
- Quais as áreas em que foi mais difícil avançar na implementação (por exemplo, gestão de riscos, sistemas de deteção ou notificações de incidentes)?
- Foi necessário reforçar ou alterar alguma infraestrutura tecnológica para cumprir com os requisitos da Diretiva? **RM: Na maior parte das organizações que não se encontram ainda preparadas para estas temáticas, na sua maioria, sim a necessidade de tecnologia é muitas das vezes essencial para estruturar os diferentes processos e capacidades da organização. Esta tecnologia vai desde ferramentas centralizadoras como ITSM, como especificas de Segurança de informação como soluções de SIEM.**

3. Desafios Enfrentados

Sem entrar em detalhes confidenciais, quais as principais dificuldades encontradas durante o processo de implementação dos requisitos da NIS2? Por exemplo:

  - Aspetos técnicos?
  - Aspetos financeiros?
  - Capacitação e formação de recursos humanos?
  - Integração com outras normas de cibersegurança?
  - Outros?
- **RM: Diria que na nossa experiencia, tanto aspetos técnicos, financeiros e de recursos humanos de aplicam em diferentes clientes, destacando sempre a lacuna mais presente que verificamos na maioria das organizações ferentes a TPRM.**
- A sua organização teve algum desafio relacionado com a colaboração de fornecedores ou parceiros em conformidade com a NIS2?

4. Impactos nos processos Organizacionais, Técnicos e Operacionais

Sem entrar em detalhes confidenciais, de que forma a implementação da NIS2 afetou os processos organizacionais dentro da sua organização? Por exemplo:

  - Na reestruturação de políticas de segurança?

  - Na alocação de recursos?
  - No planeamento e governação?
  - Outros?
- **RM: Muitas das organizações que identificámos reestruturaram os seus modelos de governo da organização por forma a garantir a integração de segurança de informação nos processos fundamentais da organização.**

- Que impactos a NIS2 trouxe para a sua arquitetura técnica e para as soluções de cibersegurança em uso?
- **RM: Muitas das organizações demonstram lacunas em parte da sua organização, muitas das vezes em processos de *supply Chain*¸ pela ausência até então de regulamentação de obrigue a existência de controlos de segurança transversais aos processos da organização.**
- A sua organização tem recursos (técnicos e financeiros) suficientes para garantir a conformidade contínua com a NIS2?
- **RM: Parece-me que é desafio para pequenas e médias empresas tanto para o sector privado, como para o sector publico.**

Entrevistado 4

From:
To: "Pedro Esteves"
Subject: RE: Pedro Esteves - Entrevista | Trabalho Final Mestrado - confirmação respostas
Date: 13 de outubro de 2025 12:46:19
Attachments:

Bom dia,

Obrigado pelo envio. Vou ter de pedir que sejam alterados alguns pontos (~~rasurados~~ quando for para eliminar ou a **negrito** para integrar no texto) – justificação a verde. Sugiro que minha identificação no estudo seja de "colaborador do CNCS".

Atenciosamente,

From: Pedro Esteves <pedro.esteves@ecoambiente.pt>
Sent: 11 de outubro de 2025 11:09
To:
Subject: Pedro Esteves - Entrevista | Trabalho Final Mestrado - confirmação respostas
Importance: High

Bom dia.

No seguimento da entrevista, a qual agradeço desde já, solicito confirmação do que foi transcrito para as respostas, para garantir que estão de acordo com o que foi transmitido por si.
Aguardo o seu feedback.

-- QUESTIONÁRIO –

1. **Conhecimento e Adoção da Diretiva NIS2**

Sem entrar em detalhes confidenciais, gostava que perceber, de forma geral, qual o grau de conhecimento atual da sua organização em relação à NIS2, nomeadamente:

- A sua organização está ciente da Diretiva NIS2 e dos requisitos que ela impõe?
- Quem na sua organização é responsável (cargo?) por acompanhar as normas e regulamentações relacionadas com a cibersegurança, incluindo a NIS2?
- A sua organização já iniciou a implementação das medidas previstas pela NIS2?
- Qual é o grau de conhecimento da empresa (áreas de Sistemas de Informação e de Gestão/Administração) sobre os requisitos específicos da NIS2?

R.: O Centro Nacional de Cibersegurança (CNCS) encontra-se **a acompanhar de perto a transposição** da Diretiva NIS2 e dos requisitos que esta impõe no contexto europeu e nacional. A Diretiva NIS2 surge no seguimento da evolução do mercado único digital europeu, procurando colmatar as limitações identificadas na Diretiva anterior (NIS 1), nomeadamente no que respeita à abrangência dos critérios de identificação das entidades e à heterogeneidade na aplicação das medidas de segurança entre Estados-Membros.
A nova Diretiva introduz uma abordagem mais objetiva e harmonizada, ampliando o número de setores abrangidos e estabelecendo critérios de dimensão como um dos principais fatores de determinação das entidades obrigadas. Este alargamento visa reduzir o desfasamento anteriormente existente entre as necessidades reais de segurança e o enquadramento legal em

vigor, promovendo uma maior coerência e proporcionalidade na aplicação das medidas.
Destaca-se também que, embora algumas organizações de menor dimensão possam agora ser incluídas no âmbito da NIS2, a Diretiva prevê mecanismos de flexibilidade proporcional, permitindo adequar as exigências à capacidade das entidades, de modo a não comprometer a sua viabilidade operacional.
No caso da Administração Pública, esta já se encontrava abrangida pela legislação nacional que transpôs a primeira Diretiva NIS — a Lei n.º 46/2018. Contudo, a definição do que constitui a "administração pública central" não é expressamente estabelecida na NIS2, cabendo a cada Estado-Membro essa clarificação. Em Portugal, foi introduzido o conceito de "entidades públicas relevantes", criado pelo legislador nacional, o qual distingue dois grupos principais:
Grupo A, correspondente a entidades de maior dimensão e criticidade, sujeitas a medidas mais ~~exigentes~~, **havendo em boa parte uma correspondência às medidas exigidas para obter o ~~associadas ao~~** selo de maturidade Prata;
Grupo B, composto por entidades de menor dimensão ou complexidade, **havendo em boa parte uma correspondência às medidas exigidas para obter o ~~enquadradas nas exigências do~~** selo de maturidade Bronze. Descrição mais precisa
O CNCS ~~encontra-se abrangido pela Diretiva NIS2,~~ desempenhando ~~simultaneamente~~ um papel de autoridade competente ~~e de entidade regulada~~, o que reforça o seu envolvimento direto na transposição, acompanhamento e aplicação prática do novo regime jurídico nacional A posição não foi publicamente assumida e pode ser alterada de acordo com o texto legislativo final.

-

2. **Implementação dos Requisitos**

Sem entrar em detalhes confidenciais, gostava que perceber, de forma geral, qual o ponto de situação atual da sua organização em relação à implementação dos requisitos da NIS2, nomeadamente:

- Em que áreas da NIS2 a sua organização sente que já conseguiu avançar na implementação?
- Houve alguma dificuldade técnica ou organizacional na implementação desses requisitos?
- Quais as áreas em que foi mais difícil avançar na implementação (por exemplo, gestão de riscos, sistemas de deteção ou notificações de incidentes)?
- Foi necessário reforçar ou alterar alguma infraestrutura tecnológica para cumprir com os requisitos da Diretiva?

R.: No que respeita à implementação dos requisitos previstos na Diretiva NIS2, o Centro Nacional de Cibersegurança (CNCS) reconhece avanços significativos, mas também desafios estruturais que continuam a condicionar o processo de plena execução.
A principal dificuldade identificada relaciona-se com a contratação e retenção de técnicos especializados em cibersegurança ~~pelo próprio CNCS~~. A discrepância entre as condições salariais oferecidas pela administração pública e as do setor privado tem dificultado a atração e manutenção de profissionais altamente qualificados para o setor público, no geral. Apesar deste constrangimento, os recursos humanos atualmente contratualizados pelo CNCS revelam um elevado nível de competência técnica e desempenham um papel determinante na consolidação da capacidade operacional da organização -Informação que não é de natureza pública.
Do ponto de vista organizacional, destaca-se a dificuldade de várias entidades abrangidas em compreender e operacionalizar as exigências da NIS2, sobretudo nas áreas de gestão de riscos, deteção de incidentes e mecanismos de notificação. Esta lacuna reflete a necessidade de um maior investimento em capacitação técnica e sensibilização das organizações, de modo a garantir uma implementação uniforme e eficaz da Diretiva.
~~Em termos tecnológicos, destaca-se a importância estratégica da adoção de sistemas SIEM (Security Information and Event Management) e SOC (Security Operations Center), considerados~~

~~fundamentais para a monitorização contínua, deteção precoce e resposta coordenada a incidentes de cibersegurança. A promoção e integração destas soluções são vistas como elementos essenciais para reforçar a resiliência das infraestruturas críticas e alinhar as práticas nacionais com os padrões europeus de segurança digital.~~ Isto vai depender muito da realidade das entidades, não podemos generalizar como uma recomendação para todas as entidades abrangidas pela diretiva.

-

3. **Desafios Enfrentados**

- Sem entrar em detalhes confidenciais, quais as principais dificuldades encontradas durante o processo de implementação dos requisitos da NIS2? Por exemplo:
  - Aspetos técnicos?
  - Aspetos financeiros?
  - Capacitação e formação de recursos humanos?
  - Integração com outras normas de cibersegurança?
  - Outros?

- A sua organização teve algum desafio relacionado com a colaboração de fornecedores ou parceiros em conformidade com a NIS2?

R.: A Entre os principais desafios associados à implementação dos requisitos da Diretiva NIS2, o Centro Nacional de Cibersegurança (CNCS) destaca as ~~dificuldades de~~ **necessidade de mapeamento** ~~da integração~~ com outras normas e referenciais de cibersegurança já existentes. Embora a NIS2 introduza um quadro harmonizado a nível europeu, a correspondência direta entre os seus requisitos e os padrões internacionais, como a ISO/IEC 27001 ou o NIST Cybersecurity Framework, ~~não é totalmente linear~~ **requer algum trabalho**. Correção para maior precisão.
Neste contexto, o CNCS recomenda a utilização do Quadro Nacional de Referência de Cibersegurança (QNRC) como instrumento de orientação para o alinhamento normativo. O QNRC disponibiliza um mapeamento de correspondências entre diferentes referenciais e pode ser consultado através das plataformas oficiais do CNCS. Adicionalmente, é referenciado o CyberFundamentals Framework, desenvolvido pelo Governo Belga, como exemplo de um modelo de medidas concretas destinadas a reduzir o risco de ciberataques e a aumentar a resiliência organizacional.
Outro aspeto identificado prende-se com a implementação de medidas de segurança na cadeia de fornecimento, uma exigência prevista na NIS2. Apesar das pequenas entidades fornecedoras poderem não estar diretamente abrangidas pela Diretiva, é recomendável que os contratos celebrados com essas organizações incluam cláusulas e evidências relacionadas com boas práticas de cibersegurança, assegurando assim um mínimo de conformidade e mitigação de risco.
Por fim, foi salienta-se a importância de, nas avaliações de risco, serem explicitamente identificados os pequenos fornecedores que integram a cadeia de abastecimento, de modo a garantir uma visão abrangente das potenciais vulnerabilidades externas e uma aplicação proporcional das medidas de mitigação.

-

4. **Impactos nos processos Organizacionais, Técnicos e Operacionais**

Sem entrar em detalhes confidenciais, de que forma a implementação da NIS2 afetou os processos organizacionais dentro da sua organização? Por exemplo:
  - Na reestruturação de políticas de segurança?
  - Na alocação de recursos?
  - No planeamento e governação?
  - Outros?

- Que impactos a NIS2 trouxe para a sua arquitetura técnica e para as soluções de

cibersegurança em uso?

- A sua organização tem recursos (técnicos e financeiros) suficientes para garantir a conformidade contínua com a NIS2?

R.: A implementação da Diretiva NIS2 tem provocado uma mudança estrutural significativa na forma como as organizações encaram a cibersegurança, conduzindo a uma transformação cultural e organizacional em torno do tema. Verifica-se que as chefias de topo deixaram de poder ignorar esta matéria, passando a ter uma responsabilidade acrescida na governação e na conformidade com os requisitos da Diretiva. Este enquadramento reforça a necessidade de uma abordagem de cibersegurança integrada na estratégia global das organizações, com responsabilidades bem definidas ao nível da gestão.
No plano organizacional, observa-se uma crescente necessidade de reformular os processos de recrutamento e integração de novos colaboradores, garantindo que estes recebam formação adequada em cibersegurança desde o início das suas funções. Paralelamente, torna-se essencial incluir, nos orçamentos institucionais, rubricas específicas destinadas a serviços e produtos de cibersegurança, assegurando a sustentabilidade financeira das medidas a implementar.
Em termos de capacitação e formação, é destaca-se a importância de promover formações diferenciadas — tanto para níveis de gestão superior, centradas em governação e tomada de decisão, como para perfis técnicos e administrativos, orientadas para a aplicação prática de medidas de segurança. Estas iniciativas são fundamentais para aumentar a disponibilidade de recursos humanos qualificados e, consequentemente, elevar o nível de maturidade das organizações no domínio da cibersegurança. **Portugal tem dado passos importantes na capacitação com o desenvolvimento da C-Academy, em parceria com as universidade e politécnicos.**
Contudo, reconhece-se que ~~nem todas as organizações dispõem de~~ **será requerido um esforço financeiro às empresas** ~~recursos financeiros suficientes~~ para garantir a conformidade plena e contínua com a NIS2. A pressão associada ao receio de perda de dados e às coimas previstas para contraordenações pode, no entanto, funcionar como um estímulo para o investimento em medidas de segurança digital. Em contrapartida, defende-se que a aplicação da Diretiva deve respeitar o princípio da proporcionalidade, permitindo alguma flexibilidade na intensidade dos investimentos, sobretudo para entidades de menor dimensão ou com recursos limitados.

Com os melhores cumprimentos,

EcoAmbiente
Serviços e Meio Ambiente, S.A.
Por um melhor amanhã

Pedro Esteves
Responsável TIC
EM pedro.esteves@ecoambiente.pt
TM (+351) 935 061 133

Parque Industrial da Abrunheira
Quinta do Lavi, Edifício 2,
2710-089 Sintra

TL (+351) 219 156 090
www.ecoambiente.pt

Entrevistado 5

From:
To: pedro esteves
Cc:
Subject: Re: Pedro Esteves - Entrevista | Trabalho Final Mestrado - confirmação respostas
Date: 11 de outubro de 2025 13:31:36
Attachments:

Bom dia Pedro

Já li e no contexto geral parece-me bem.

No meu entendimento podes avançar.

Atentamente,

PROLOGIN
PRODUTOS E SERVIÇOS

SOPHOS
PLATINUM PARTNER

De: "pedro esteves" <pedro.esteves@ecoambiente.pt>
Para:
Cc:
Itens enviados: Sábado, 11 de Outubro de 2025 9:32:25
Assunto: Pedro Esteves - Entrevista | Trabalho Final Mestrado - confirmação respostas

Bom dia.

No seguimento da entrevista, a qual agradeço desde já, solicito confirmação do que foi transcrito para as respostas, para garantir que estão de acordo com o que foi transmitido pela Prologin.
Aguardo o seu feedback.

-- QUESTIONÁRIO –

1. **Conhecimento e Adoção da Diretiva NIS2**

Sem entrar em detalhes confidenciais, gostava que perceber, de forma geral, qual o grau de conhecimento atual da sua organização em relação à NIS2, nomeadamente:

- A sua organização está ciente da Diretiva NIS2 e dos requisitos que ela impõe?

R.: Sim. A organização encontra-se ciente da Diretiva NIS2 e dos requisitos que esta estabelece no domínio da segurança das redes e dos sistemas de informação. Este conhecimento resulta do acompanhamento das políticas europeias em matéria de cibersegurança e da necessidade de garantir a conformidade com o novo enquadramento legal que reforça as obrigações de gestão de risco, reporte de incidentes e resiliência operacional.

- Quem na sua organização é responsável (cargo?) por acompanhar as normas e regulamentações relacionadas com a cibersegurança, incluindo a NIS2?

R.: A informação relativa ao cargo ou função responsável pelo acompanhamento das normas e regulamentações em matéria de cibersegurança, incluindo a Diretiva NIS2, é de carácter confidencial. Contudo, a organização assegura que essa responsabilidade está atribuída a uma estrutura interna competente, com funções específicas de monitorização, conformidade e implementação das orientações decorrentes do enquadramento normativo europeu e nacional.

- A sua organização já iniciou a implementação das medidas previstas pela NIS2?

R.: Sim. A organização já se encontra numa fase muito avançada do processo de implementação das medidas previstas pela Diretiva NIS2, estimando-se que cerca de 95% das ações necessárias estejam concluídas. Este grau de execução reflete o compromisso institucional com o reforço da cibersegurança, bem como a integração progressiva das exigências legais e técnicas impostas pelo novo enquadramento normativo europeu.

- Qual é o grau de conhecimento da empresa (áreas de Sistemas de Informação e de Gestão/Administração) sobre os requisitos específicos da NIS2?

R.: O grau de conhecimento da organização relativamente aos requisitos específicos da Diretiva NIS2 é elevado, abrangendo aproximadamente 95% dos requisitos da NIS 2. Contudo, observa-se que, no contexto mais amplo do mercado público e privado, o nível de conhecimento e maturidade relativamente à Diretiva é bastante heterogéneo. Estima-se que cerca de 40% das entidades tenham apenas consciência da existência da NIS2, sem conhecimento aprofundado sobre os seus requisitos; 15% revelem um entendimento mais consolidado da diretiva; e aproximadamente 45% estejam a desenvolver ações de adaptação, ainda que sem grandes progressos estruturais. Esta disparidade evidencia diferentes estágios de preparação e sensibilização entre os vários setores.
De forma geral, constata-se que a maioria dos clientes encara a NIS2 mais como uma obrigação regulamentar do que como uma necessidade estratégica para o reforço da cibersegurança. Tal perceção leva a que o processo de conformidade seja frequentemente visto como um exercício burocrático, semelhante ao que ocorreu com o RGPD, cuja implementação prática acabou, em muitos casos, por não gerar mudanças significativas nos comportamentos organizacionais.

2. **Implementação dos Requisitos**

Sem entrar em detalhes confidenciais, gostava que perceber, de forma geral, qual o ponto de situação atual da sua organização em relação à implementação dos requisitos da NIS2, nomeadamente:

- Em que áreas da NIS2 a sua organização sente que já conseguiu avançar na implementação?

R.: A organização já alcançou um nível de implementação muito elevado das medidas previstas pela Diretiva NIS2, estimando-se que cerca de 95% dos requisitos se encontrem cumpridos. Neste sentido, pode afirmar-se que todas as áreas contempladas pela Diretiva estão devidamente asseguradas, refletindo uma abordagem integrada à gestão da cibersegurança e à conformidade normativa. Este resultado decorre de um planeamento estruturado e de uma articulação eficaz entre as diferentes unidades internas responsáveis pela segurança da informação, pela administração e pela

governação tecnológica.

- Houve alguma dificuldade técnica ou organizacional na implementação desses requisitos?

R.: Sim. As principais dificuldades registadas durante o processo de implementação dos requisitos da Diretiva NIS2 concentraram-se sobretudo na **vertente organizacional**, particularmente ao nível **processual e documental**. A necessidade de formalizar procedimentos, atualizar políticas internas e harmonizar a documentação existente com os novos requisitos implicou um esforço adicional de coordenação e adaptação. No entanto, nas restantes áreas — sobretudo nas dimensões técnicas e operacionais — a organização já se encontrava, em grande medida, em conformidade com as exigências da Diretiva, o que facilitou a transição e mitigou o impacto global do processo de implementação.

- Quais as áreas em que foi mais difícil avançar na implementação (por exemplo, gestão de riscos, sistemas de deteção ou notificações de incidentes)?

R.: A área que revelou maior complexidade na fase de implementação correspondeu à elaboração e consolidação dos relatórios de evidências necessários para demonstrar o cumprimento dos requisitos previstos na Diretiva NIS2. A principal dificuldade prendeu-se com a necessidade de reunir, sistematizar e documentar de forma estruturada as provas de conformidade exigidas, garantindo simultaneamente a rastreabilidade e a coerência entre os diferentes processos internos. Este desafio decorreu, em grande parte, da exigência de uma documentação detalhada e verificável, que vai além da simples execução técnica das medidas, exigindo um grau elevado de maturidade organizacional e de alinhamento entre as áreas técnica e administrativa.

- Foi necessário reforçar ou alterar alguma infraestrutura tecnológica para cumprir com os requisitos da Diretiva?

R.: Sim. No âmbito do processo de adequação à Diretiva NIS2, foi necessário reforçar a infraestrutura tecnológica, nomeadamente através da implementação de uma solução mais robusta para a gestão de passwords, bem como do aperfeiçoamento dos mecanismos de recuperação de desastre (Disaster Recovery) e de cópias de segurança (backups). Estas medidas visaram aumentar a resiliência dos sistemas de informação, garantindo a proteção, integridade e disponibilidade dos dados críticos da organização, em conformidade com os princípios de segurança e continuidade operacional exigidos pela Diretiva.

3. **Desafios Enfrentados**

- Sem entrar em detalhes confidenciais, quais as principais dificuldades encontradas durante o processo de implementação dos requisitos da NIS2? Por exemplo:
  - Aspetos técnicos?
  - Aspetos financeiros?
  - Capacitação e formação de recursos humanos?
  - Integração com outras normas de cibersegurança?
  - Outros?

R.: A principal dificuldade identificada durante o processo de implementação dos requisitos da Diretiva NIS2 prendeu-se essencialmente com a dimensão burocrática associada ao cumprimento das exigências formais. A necessidade de produzir, organizar e validar um volume significativo de documentação e evidências processuais revelou-se particularmente desafiante, exigindo um esforço acrescido de coordenação entre as diferentes áreas da organização. Esta componente administrativa, embora fundamental para garantir a conformidade e a rastreabilidade das ações, representou o aspeto mais moroso e complexo de todo o processo de implementação.

- A sua organização teve algum desafio relacionado com a colaboração de fornecedores ou parceiros em conformidade com a NIS2?

R.: Não. A organização não enfrentou desafios significativos relacionados com a colaboração de fornecedores ou parceiros no âmbito da conformidade com a Diretiva NIS2. Os parceiros externos demonstraram disponibilidade e alinhamento com as exigências estabelecidas, o que contribuiu para uma integração fluída das medidas de segurança e para a manutenção da coerência nos processos de implementação.

4. **Impactos nos processos Organizacionais, Técnicos e Operacionais**

Sem entrar em detalhes confidenciais, de que forma a implementação da NIS2 afetou os processos organizacionais dentro da sua organização? Por exemplo:

- Na reestruturação de políticas de segurança?
- Na alocação de recursos?
- No planeamento e governação?
- Outros?

R.: O principal impacto da implementação da Diretiva NIS2 verificou-se ao nível dos processos organizacionais, que passaram a estar mais estruturados e documentados. A adoção das medidas impostas pela Diretiva conduziu à formalização de procedimentos e à criação de registos documentais que permitem comprovar, de forma objetiva, o cumprimento dos requisitos e a existência de evidências verificáveis.
Além disso, foram introduzidos novos processos internos de monitorização, controlo e reporte, o que contribuiu para uma melhoria significativa na rastreabilidade e na transparência das práticas de cibersegurança. Em termos globais, estas mudanças resultaram num aumento da maturidade organizacional e numa maior capacidade de demonstração de conformidade perante auditorias ou entidades reguladoras.

- Que impactos a NIS2 trouxe para a sua arquitetura técnica e para as soluções de cibersegurança em uso?

R.: A implementação da Diretiva NIS2 gerou melhorias significativas na arquitetura técnica e nas soluções de cibersegurança em utilização. O processo impulsionou uma revisão das infraestruturas tecnológicas, levando à otimização de sistemas existentes e à adoção de medidas adicionais de proteção e monitorização, o que resultou num reforço da resiliência global da organização.
Embora estas melhorias tenham implicado alguns custos adicionais, estes já se encontravam, em grande parte, previstos e assegurados através de investimentos anteriores em modernização tecnológica e segurança da informação. Assim, o impacto financeiro direto foi limitado, permitindo que as melhorias fossem implementadas de forma sustentável e alinhada com o planeamento estratégico de cibersegurança da organização.

A sua organização tem recursos (técnicos e financeiros) suficientes para garantir a conformidade contínua com a NIS2?

R.: Sim. No caso da organização, não se registaram custos acrescidos para garantir a conformidade contínua com a Diretiva NIS2. Os recursos técnicos e financeiros necessários já se encontravam previamente assegurados, em resultado de investimentos anteriores em modernização tecnológica e em políticas de segurança da informação. Esta preparação prévia permitiu uma integração fluída das exigências da Diretiva, assegurando a sustentabilidade das medidas implementadas e a manutenção da conformidade a longo prazo.

Com os melhores cumprimentos,


EcoAmbiente
Serviços e Meio Ambiente, S.A.
Por um melhor amanhã
Pedro Esteves
Responsável TIC
EM pedro.esteves@ecoambiente.pt
TM (+351) 935 061 133
Parque Industrial da Abrunheira
Quinta do Lavi, Edifício 2,
2710-089 Sintra
TL (+351) 219 156 090
www.ecoambiente.pt