Diretiva NIS2

Rui Silva

***Resumo* — O presente artigo retrata o trabalho teórico desenvolvido no âmbito da área dos Sistemas de Gestão da Segurança, mais propriamente em regulamentação, investigação, conformidade e ética nos SGSI e nos modelos e práticas de gestão de segurança.**

O tema abordado neste artigo é sobre a Diretiva NIS2, entrou em vigor a dezembro de 2022 e terá de ser implementada até outubro de 2024, no qual deverão ser adotadas e publicadas as medidas necessárias para cumprir a diretiva. O aumento de ataques cibernéticos, como *ransomware* e violações de dados, têm cada vez mais impacto nas organizações e empresas em toda a União Europeia. A NIS2 tem como objetivo melhorar a cibersegurança entre as entidades mais essenciais, como serviços financeiros, de infraestruturas digitais, saúde e de energia.

A Diretiva NIS2 é um passo importante para melhorar a segurança cibernética na União Europeia. As novas medidas são mais abrangentes e rigorosas comparadas à diretiva anterior. No entanto, a implementação da Diretiva NIS2 será um desafio. As empresas terão de cumprir novas obrigações e os Estados-Membros reforçar as suas capacidades de segurança.

***Lista de Siglas* —**
NIS: Network and Information Security
SGSI: Sistema de Gestão de Segurança da Informação

I. INTRODUÇÃO

Diretiva NIS2, um novo marco para a segurança cibernética na União Europeia.

A nova Diretiva NIS2 da União Europeia estabelece novas regras que irão afetar várias entidades e empresas. Esta diretiva visa reforçar a segurança cibernética das infraestruturas críticas e das empresas que prestam serviços essenciais. Algumas das principais mudanças introduzidas pela diretiva incluem a avaliações de risco e relatórios, implementação de medidas técnicas e organizacionais de segurança, notificação de incidentes cibernéticos às autoridades competentes e cooperação com as autoridades competentes em caso de incidentes.

As organizações que são obrigadas a cumprir com a Diretiva NIS2 são divididas em duas categorias:

1) Operadores de serviços essenciais (OSEs): são organizações que fornecem serviços essenciais, como energia, transporte, saúde e serviços financeiros.
2) Fornecedores de serviços digitais (FSDs): organizações que fornecem serviços digitais que são essenciais para a economia e a sociedade, como serviços de pagamento e serviços de armazenamento em nuvem.

A Diretiva NIS2 entrou em vigor em 27 de junho de 2023, já os Estados-Membros da União Europeia têm até 17 de outubro de 2024 para transpor a diretiva para a sua legislação nacional.

"A garantia de um elevado nível de segurança do ciberespaço é do interesse de todos os cidadãos e atores, públicos ou privados, envolvidos" - João Alves, Coordenador do Departamento de Regulação, Supervisão e Certificação do Centro Nacional de Cibersegurança

A. Abreviaturas e Acrónimos

C.N.C.S.	Centro Nacional de Cibersegurança
F.S.D.	Fornecedores de Serviços Digitais
I.O.T.	Internet of Things
N.I.S.	Network and Information Security
O.S.E.	Operadores de Serviços Essenciais
O.T.	Operational Technology
T.I.	Tecnologias de Informação
U.E.	União Europeia

II. NIS

Diretiva NIS, mais conhecida como diretiva sobre segurança de redes e sistemas de informação, foi publicada pelo Parlamento Europeu em 2016, de modo a gerar um alto nível de segurança na UE. A diretiva NIS foca-se na segurança das nações individuais, colaboração transfronteiriça e em setores críticos, tais como a energia, as finanças, as infraestruturas digitais e os cuidados de saúde.

III. EVOLUÇÃO DA NIS PARA NIS2

A Diretiva NIS foi admitida em 2016, com o propósito de reforçar a adaptação do espaço europeu de cibersegurança em três níveis: europeu, estados-membros e entidades consideradas relevantes.

A evolução da Diretiva NIS para a Diretiva NIS2 pode ser analisada pelos seguintes pontos:

1) Pelo seu alcance, onde a Diretiva NIS2 alcance um conjunto mais alargado de organizações, incluindo os FSDs. Esta alteração é importante para proteger os cidadãos e as empresas dos ataques cibernéticos que

visam estes serviços.

2) As autoridades nacionais, a Diretiva NIS2 reforça as competências das autoridades nacionais de cibersegurança o que garante uma aplicação mais eficaz da Diretiva NIS2.
3) Os requisitos, a Diretiva NIS2 estabelece requisitos mais rigorosos para as organizações. Estas alterações são importantes para aumentar o nível de cibersegurança na UE.

Foram ainda aplicados regulamentos do regime jurídico do ciberespaço e definidos requisitos para as entidades, tais como, a comunicação do ponto de contato permanente e responsável de segurança, a comunicação do inventário dos ativos essenciais para a prestação dos serviços, execução de análises dos riscos globais e parciais, a elaboração e atualização de um plano de segurança, comunicação de um relatório anual e ainda a implementação de meios que permitam detetar, classificar e notificar incidentes ao CNCS.

Em 14 de dezembro de 2022, a Diretiva NIS2 vem substituir a diretiva NIS. A NIS2 veio reforçar algumas das medidas anteriores, nomeadamente análises de riscos e tratamentos de incidentes. Com a nova diretiva, a União Europeia pretende abordar vulnerabilidades críticas para criar um elevado nível de segurança, na melhor das hipóteses, prevenir ataques cibernéticos e na pior das hipóteses, facilitar a recuperação e a resiliência.

IV. NIS2

A Diretiva NIS2 estabelece uma legislação sobre cibersegurança para toda a União Europeia. A NIS2 é uma atualização da versão anterior e visa tratar da compatibilização de medidas e abordagens em todos os Estados Membros da União Europeia.

A diretiva aperfeiçoa a cibersegurança da UE de diferentes tipos, como criando a estrutura necessária para a gestão de crises cibernéticas (CyCLONe), aumentando o acordo dos requisitos de segurança e obrigação de notificação e incentivando os Estados-Membros a abordar novas áreas, como gestão de vulnerabilidades.

A NIS2 amplia os setores da segurança cibernética e da preparação para a gestão de crises. Foi concebida na sequência dos anos pandémicos enfrentados, onde as ameaças cibernéticas se tornaram mais violentas e alarmantes. Relatórios mostram que, nos últimos tempos, o número das ameaças e ataques cibernéticos mudaram para impactar uma série mais ampla de indústrias e entidades.

São os líderes de TI enviados para avaliar os requisitos de conetividade e segurança dos seus dispositivos, bem como do *software*, de modo a proteger os seus negócios contra acessos não autorizados, manipulação e paralisações inesperadas, causadas por ataques. A maioria das organizações esperam que a responsabilidade pela cibersegurança passe dos diretores e gestores e comecem a ser os CISO a tomar essas decisões. O controlo da cibersegurança têm cada vez mais espaço para crescer em termos de responsabilidade, formação, sensibilização e ação.

As medidas de proteção devem tornar-se mais abrangentes para proteger o maior número possível de órgãos críticos. Assim, a nova diretiva apresentou uma política mais abrangente para reforçar a cibersegurança e a resiliência dos prestadores de serviços essenciais na Europa.

A. *Setores acrescentados*

No âmbito de aplicação da Diretiva NIS2 é acrescentado outros setores à lista de setores críticos da versão NIS anterior, como é ilustrado na figura 1. Relembrando esses setores críticos, são eles a energia, as finanças, as infraestruturas digitais, os cuidados de saúde, abastecimento de água e transportes, são agora adicionados mais setores:

1) Setor de Administração Pública: serviços sociais, segurança pública, regulação económica e representação política;
2) Setor de Fornecedores Digitais: motores de busca, mercado online e redes sociais;
3) Setor de Postal: serviços postais e de entrega rápida;
4) Setor de Gestão de Resíduos: transporte, tratamento e eliminação de resíduos;
5) Setor Espacial: telecomunicações, navegação e segurança nacional;
6) Setor Alimentar: desde a agricultura ao processamento de alimentos, embalagem, transporte e vendas a retalho;
7) Setor Manufatureiro: engloba a fabricação de dispositivos médicos, computadores e eletrônicos, máquinas e equipamentos e equipamentos de transporte;
8) Setor Químico: suporta diversas indústrias como a construção, agricultura, transporte e energia;
9) Setor de Pesquisa: dados de investigação sensíveis.

Fig. 1. Evolução dos setores críticos da NIS para NIS2

B. *Medidas de cibersegurança exigidas pela NIS2*

A NIS2 reforça algumas das medidas já previstas da versão anterior, e inclui de uma forma mais precisa um conjunto mínimo de temas que têm de ser cumpridos pelas organizações, tais como:

1) Análise dos Riscos e de Segurança: As empresas precisam de definir procedimentos para avaliar as

vulnerabilidades dos seus sistemas de informação e elaborar uma política de segurança para migrar esses riscos.

2) Continuidade e Recuperação das Atividades: Necessidade de elaborar um plano de continuidade das atividades para garantir a disponibilidade dos seus serviços em caso de interrupção, como por exemplo uma falha de servidor.

3) Criptografia: As organizações devem definir políticas sobre o uso de criptografia para proteger dados confidenciais.

4) Avaliação de Medidas de Gestão de Riscos Cibernéticos: As organizações devem reavaliar regularmente a sua postura de segurança através de auditorias e testes de vulnerabilidade.

5) Tratamento de Incidentes: As organizações devem ter um plano de resposta a ataques cibernéticos, incluindo notificação de incidentes às autoridades competentes.

6) Ferramentas de Comunicação Segura: As empresas protegem os recursos de comunicação para coordenar as respostas no caso de um incidente grave, como por exemplo uma sala equipada com tecnologia de comunicação confiável.

7) Políticas de Controle de Acesso e Gestão de Ativos: As organizações devem treinar seus funcionários em práticas de segurança, gerenciar direitos de acesso a sistemas e monitorar o uso de ativos de TI.

8) Segurança para Aquisição, Desenvolvimento e Manutenção de Redes e Sistemas de Informação: Ao adquirir novo software, as organizações devem garantir que ele esteja livre de vulnerabilidades conhecidas e aplicar *patches* quando necessário.

9) Autenticação multifatores: Uma organização pode exigir que os usuários façam login nos seus sistemas usando dois métodos de autenticação.

10) Relatórios de Incidentes: As organizações são obrigadas a comunicar quaisquer incidentes cibernéticos significativos que afetem a segurança das suas redes e sistemas de informação às autoridades nacionais designadas.

O CNCS aplica multas às entidades que não cumpram estas medidas previstas na Lei do Ciberespaço e são dirigidas a quem coloque em risco infraestruturas críticas e serviços essenciais.

C. Penalidades para o não cumprimento das normas

A Diretiva NIS2 estabelece penalidades específicas para o não cumprimento das suas normas. As multas específicas variam consoante o Estado-Membro, mas a diretiva estabelece uma lista mínima de sanções administrativas para a infração das obrigações de gestão e comunicação de riscos de cibersegurança. As sanções incluem:

1) Penalidades não monetárias: ordens de conformidade, instruções vinculativas, ordens de implementação de auditorias de segurança e ordens de notificação de ameaças aos clientes das entidades.

2) Multas administrativas: Para entidades essenciais, exige que os Estados-Membros forneçam um nível máximo de multa de pelo menos 10 milhões de euros ou 2% da receita anual global, dependendo do que for mais elevado. Para entidades importantes, as multas máximas são de pelo menos 7 milhões de euros ou 1,4% da receita anual global.

3) Sanções criminais para a gestão: onde existe a possibilidade de as autoridades dos Estados-Membros responsabilizarem pessoalmente a gestão de topo por negligência grave no caso de incidente de segurança. Pode incluir a obrigação de tornar públicas as infrações de conformidade, a identificação pública dos responsáveis pelas infrações e, em casos de infrações repetidas por entidades essenciais, a proibição temporária de um indivíduo de ocupar cargos de gestão.

V. DECRETOS-LEIS

O Decreto-Lei nº 46/2018, de 13 de agosto, estabeleceu o regime jurídico da segurança do ciberespaço, ultrapassando a Diretiva 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a UE.

O Decreto-Lei nº 65/2021 (DL65) de Portugal, regulamenta o regime jurídico do ciberespaço, alinhando-se com as obrigações da Diretiva NIS. A Diretiva NIS2, que veio a substituir a Diretiva NIS, amplia o âmbito de aplicação e reforça as obrigações de segurança cibernética das entidades abrangidas. Enquanto o Decreto-Lei nº 65/2021 estabeleceu um marco na regulamentação da cibersegurança em Portugal, a Diretiva NIS2 impõe requisitos adicionais e mais detalhados que as entidades devem cumprir, relacionados com a análise de riscos e o tratamento de incidentes.

O decreto-Lei 65/2021, de 30 de julho, veio regulamentar alguns aspetos na Lei 46/2018, que aprovou o Regime Jurídico da Segurança do Ciberespaço, através da qual foi criado o Conselho Superior de Segurança do Ciberespaço, órgão de consulta do primeiro-ministro para os assuntos relativos à segurança do ciberespaço.

A aprovação e publicação do decreto-Lei 65/2021 e do regulamento 183/2022 consistiu em um importante passo para cibersegurança em Portugal.

O DL65 estabelece que o CNCS é a Autoridade Nacional de Certificação da Cibersegurança, e garante a conformidade com um Quadro Nacional de Certificação da Cibersegurança (QNCS), através do qual é estabelecido o enquadramento institucional necessário à produção de vários esquemas nacionais de certificação de cibersegurança.

VI. CONCLUSÃO

A implementação efetiva da diretiva requer uma mudança de mentalidade, onde a cibersegurança deve ser encarada como uma prioridade em vez de uma despesa dispensável.

Um estudo da Nozomi e da Exclusive Networks mostra que a Diretiva NIS2 será um desafio substancial para as empresas, nomeadamente para as que operam em indústrias com infraestruturas críticas. As coimas por incumprimento podem ascender a dez milhões de euros.

Numa última análise, a NIS 2 é um passo importante na proteção das organizações e dos cidadãos da União Europeia, a sua eficácia dependerá da aplicação rigorosa e consistente de todos os Estados Membros e das empresas.

"Somos todos peças de um puzzle e temos o dever de cuidar de forma diligente e preventiva, para que em caso de incidente significativo os danos sejam minimizados e mitigados ao máximo, com as menores repercussões possíveis" - Alexandra Palma, Information Security Consultant da Integrity

REFERÊNCIAS

[1] F24, "The Complete Guide to NIS2," 2023. [Online]. Available: https://f24.com/en/the-complete-guide-nis2-steps-to-become-compliant/.

[2] EUR-Lex, "DIRECTIVE (EU) 2022/2555 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL," [Online]. Available: https://eur-lex.europa.eu/eli/dir/2022/2555.

[3] M. B. Fernandes, "NIS 2: "Uma evolução (e não uma revolução)" da segurança das redes e sistemas de informação," 2023. [Online]. Available: https://www.itsecurity.pt/news/compliance/nis-2-uma-evolucao-e-nao-uma-revolucao-da-seguranca-das-redes-e-sistemas-de-informacao.

[4] C. Caldeira, "Diretiva NIS 2: uma necessidade ou um obstáculo?," 2023. [Online]. Available: https://observador.pt/opiniao/diretiva-nis-2-uma-necessidade-ou-um-obstaculo/.

[5] M. T. Pereira, "De NIS a NIS2 – a evolução da legislação europeia de cibersegurança," [Online]. Available: https://www.pwc.pt/pt/sala-imprensa/artigos-opiniao/2023/legislacao-ciberseguranca-nis2.html.

[6] G. Erismann, "Navigating the Impact of NIS2 on Network Monitoring for Critical Infrastructure: A Comprehensive Guide," 2023. [Online]. Available: https://exeon.com/blog/nis2.

[7] European Commission, "Directive on measures for a high common level of cybersecurity across the Union (NIS2 Directive)," 14 Setembro 2023. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/nis2-directive.

[8] SecurityMagazine, "NIS 2: Requisitos De Segurança Vão Abarcar Mais Empresas E Sectores," 08 Fevereiro 2021. [Online]. Available: https://www.securitymagazine.pt/2021/02/08/nis-2-requisitos-de-seguranca-vao-abarcar-mais-empresas-e-sectores/.

[9] CNCS, "Regime Jurídico," 26 Setembro 2022. [Online]. Available: https://www.cncs.gov.pt/.

[10] Enisa, "Cybersecurity Support Action," 15 Março 2023. [Online]. Available: https://www.enisa.europa.eu/.

[11] Cyber Risk GmbH, "The NIS 2 Directive," [Online]. Available: https://www.nis-2-directive.com/.

[12] Enisa, "NIS Directive," [Online]. Available: https://www.enisa.europa.eu/topics/cybersecurity-policy/nis-directive-new.

[13] Assembleia da República, "Lei n.º 46/2018, de 13 de agosto," 13 08 2018. [Online]. Available: https://diariodarepublica.pt/dr/detalhe/lei/46-2018-116029384.

[14] Assembleia da República, "Decreto-Lei n.º 65/2021, de 30 de julho," 30 07 2021. [Online]. Available: https://diariodarepublica.pt/dr/detalhe/decreto-lei/65-2021-168697988.

[15] IT Security, "NIS 2 será desafio substancial para infraestruturas críticas," 13 09 2023. [Online]. Available: https://www.itsecurity.pt/news/compliance/nis-2-sera-desafio-substancial-para-infraestruturas-criticas.

[16] M. B. Fernandes, "Decreto-lei 65/2021: um pequeno passo para o homem, um salto gigante para as organizações nacionais," 14 04 2022. [Online]. Available: https://www.itsecurity.pt/news/compliance/decreto-lei-652021-um-pequeno-passo-para-o-homem-um-salto-gigante-para-as-organizacoes-nacionais.

[17] SecurityMagazine, "Cibersegurança: Directiva NIS 2 Publicada," 28 12 2022. [Online]. Available: https://www.securitymagazine.pt/2022/12/28/ciberseguranca-directiva-nis-2-publicada/.

[18] NIS2 Directive, "The NIS2 Directive Explained," [Online]. Available: https://nis2directive.eu/.

[19] IBM, "Conformidade com a IBM Cloud®: Diretiva NIS (UE)," [Online]. Available: https://www.ibm.com/br-pt/cloud/compliance/nis-directive-eu.

Rui Silva
Nascido no distrito de Leiria em 1997.
Licenciado em Engenharia Informática, no Instituto Politécnico de Leiria
Atualmente estudante no mestrado em Cibersegurança e Informática Forense, no Instituto Politécnico de Leiria