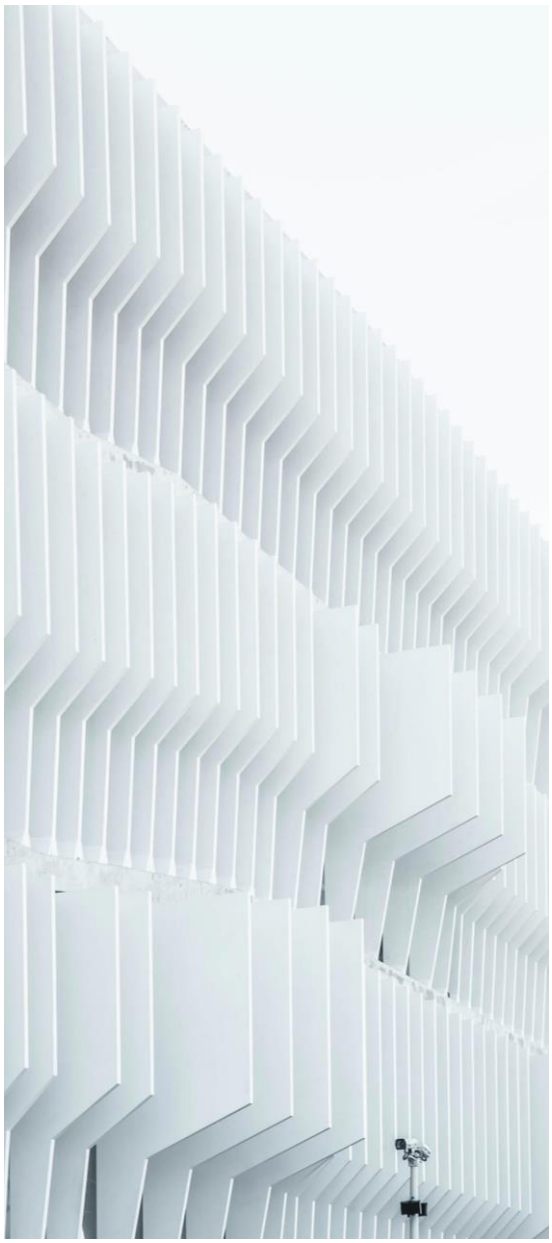
CUATRECASAS

Diretivas NIS e NIS2 – Implementação em Portugal

Diretiva (UE) 2016/1148 (Diretiva NIS) e Diretiva (UE) 2022/2555 (Diretiva NIS2): Uma visão geral da atual implementação em Portugal

Portugal - Legal Flash

6 de novembro de 2023



Aspetos-Chave

- A Diretiva NIS provocou uma mudança na abordagem institucional e regulatória da cibersegurança, mas enfrentou desafios que resultaram na fragmentação entre os Estados-Membros.
- Assim, a Diretiva NIS 2 foi publicada em 14 de dezembro de 2022, com o objetivo de melhorar a cibersegurança em toda a UE, exigindo que os Estados membros a transponham para suas leis nacionais até 17 de outubro de 2024.
- A Diretiva NIS 2 introduz uma série de mudanças em relação à sua antecessora, expandindo o âmbito de aplicação, implementando melhorias na gestão de riscos e na sensibilização organizacional, estabelecendo novos critérios de notificação de incidentes e introduzindo novas entidades, como a EU-CyCLONe, para fortalecer a cooperação entre os Estados-Membros.
- Portugal é incentivado a seguir a abordagem padronizada delineada ao nível da UE, implementando a Diretiva NIS 2 sem desvios, dado que um método de avaliação centralizado e uniforme garante padrões equitativos e uma competição justa entre os operadores de mercado.

Visão geral

Adotada em 2016, a Diretiva NIS[1] visava fortalecer a resiliência em toda a União Europeia por meio de medidas regulatórias. O foco era fortalecer as capacidades de cibersegurança a nível nacional, aprimorar a colaboração entre os Estados-Membros e incorporar a cibersegurança no âmago das organizações, em particular dos operadores de serviços essenciais e provedores de serviços digitais relevantes.

Em Portugal, a Diretiva NIS foi transposta em 2018, estabelecendo o arcabouço legal para a segurança no ciberespaço[2] e designando o Centro Nacional de Cibersegurança (CNCS) como o órgão responsável por supervisionar a implementação da Diretiva. Posteriormente, em 2021, foi publicado o Decreto-Lei n.º 65/2021, regulamentando o regime legal existente e definindo os requisitos para as entidades.

A Diretiva NIS provocou uma mudança de mentalidade na abordagem institucional e regulatória da cibersegurança. No entanto, enfrentou desafios em que a legislação não conseguia oferecer uma resposta adequada, resultando em uma abordagem fragmentada no nível dos Estados-Membros. Nos últimos anos, a rápida expansão do cenário digital, causada por uma ampla gama de circunstâncias, como a rápida sequência de inovações, a pandemia global, a guerra cibernética, garantiu um crescimento igualitário do cenário de ameaças, levando a um aumento no número de ataques cibernéticos direcionados a organizações e Estados-Membros.

Como resultado, em 14 de dezembro de 2022, a Diretiva NIS 2[3] foi publicada para acelerar e estabelecer um nível mais elevado de cibersegurança e resiliência dentro das organizações da União Europeia. Os Estados-Membros da UE terão agora de transpor a Diretiva NIS 2 para sua legislação nacional até 17 de outubro de 2024.

As medidas estabelecidas na Diretiva NIS 2 incluem um amplo escopo de aplicação, criação de novas estratégias de cooperação, obrigações de relatório, abordagens defensivas de cibersegurança, políticas de ciber-higiene, bem como esforços para aumentar a conscientização global sobre cibersegurança.

Esta publicação tem como objetivo fornecer uma visão geral dos desenvolvimentos legais e regulatórios em cibersegurança em Portugal e do processo de implementação da Diretiva NIS 2 no território.

[1] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho de 6 de julho de 2016 relativa a medidas para um elevado nível comum de segurança de sistemas de rede e informação em toda a União

[2] Lei n.º 46/2018, de 13 de agosto

[3] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho de 14 de dezembro de 2022 sobre medidas para um elevado nível comum de cibersegurança em toda a União, alterando o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972, e revogando a Diretiva (UE) 2016/1148 (Diretiva NIS 2).

Histórico da Diretiva em Portugal

A Diretiva NIS (2016)

A Diretiva NIS, adotada em 2016, representou um importante passo em frente nos esforços da UE para reforçar a cibersegurança nos seus Estados-Membros. Devido ao aumento dos incidentes de segurança da informação e à elevada ameaça e impacto no funcionamento das redes e dos sistemas de informação, era necessário, a nível da UE, abordar o panorama de ameaças que afetam sobretudo as empresas com maior exposição a estas ciberameaças.
Esta diretiva foi o primeiro ato legislativo horizontal da UE a abordar os novos desafios da cibersegurança e constituiu um ponto de viragem em termos de resiliência e cooperação da União em matéria de cibersegurança, uma vez que, até então, não existia uma estratégia única para a promoção da cibersegurança, cabendo a cada empresa definir se e como implementar essa estratégia.
Assim, a Diretiva NIS visava melhorar as capacidades nacionais de cibersegurança, reforçar a cooperação a nível da UE e promover uma cultura de gestão de riscos e de comunicação de incidentes entre os principais agentes económicos, nomeadamente:

- **Operadores de serviços essenciais**: são entidades que operam em sectores considerados críticos para a sociedade e para a economia. Aqui incluem-se sectores como (i) Energia (inclui os subsectores da eletricidade, petróleo e gás); (ii) Transportes (incluindo os subsectores dos transportes aéreos, ferroviários, marítimos e fluviais, bem como os transportes rodoviários); (iii) Saúde; d) Serviços bancários; (iv) Infra-estruturas do mercado financeiro; (v) Abastecimento e distribuição de água potável; e (vi) Sector das infra-estruturas digitais (que inclui pontos de troca de tráfego, fornecedores de serviços DNS e registos de nomes de domínio de topo).
- **Prestadores de serviços digitais**: A NIS abrange também os prestadores de serviços digitais, que incluem serviços em linha essenciais para a manutenção de processos críticos para a sociedade, nomeadamente serviços de computação em cloud, serviços de pesquisa em linha e plataformas de comércio eletrónico. As entidades abrangidas por esta diretiva são agora obrigadas a cumprir determinados requisitos, nomeadamente a implementação de medidas de segurança adequadas em função do nível de exposição ao risco, bem como a obrigação de comunicar incidentes de segurança da informação às autoridades nacionais competentes.

A nível nacional, a Diretiva exige também que cada Estado-Membro melhore o desempenho da resposta a incidentes, definindo uma estratégia nacional de cibersegurança, nomeando autoridades competentes neste domínio, criando mecanismos de resposta a incidentes e realizando exercícios regulares para testar e melhorar as suas capacidades de resposta. Introduz também a obrigação de criar estruturas de cooperação a nível da União Europeia para efeitos de cooperação e intercâmbio de informações sobre ameaças emergentes, vulnerabilidades e melhores práticas em matéria de segurança da informação, das redes e dos sistemas.

Transposição para Portugal - Lei n.º 46/2018, de 13 de agosto

Cada Estado-Membro era responsável pela definição das especificidades de cada medida. Assim, em Portugal, a transposição ocorreu através da Lei n.º 46/2018, de 13 de agosto, ao estabelecer o regime jurídico da segurança do ciberespaço.
Este quadro legal transpõe a estratégia nacional de segurança das redes e da informação e, para além dos operadores de serviços essenciais e prestadores de serviços digitais, abrange também a Administração Pública e os operadores de infraestruturas críticas. A estratégia nacional portuguesa vai, assim, além do mínimo exigido pela Diretiva Europeia.

A Lei n.º 46/2018, de 13 de agosto, estabelece e identifica a estrutura nacional para a cibersegurança, que é composta por:

- **Conselho Superior de Cibersegurança**: Este órgão é responsável por assegurar a coordenação político-estratégica da cibersegurança. Verifica a execução e comenta a estratégia nacional definida, emite relatórios e pareceres relacionados com a referida estratégia, bem como outros assuntos relacionados com a cibersegurança. Responde ainda a solicitações do Primeiro-Ministro, do Governo ou de qualquer representante.
- **Centro Nacional de Cibersegurança (CNCS):** É a entidade nacional de supervisão da cibersegurança, que funciona na dependência do Gabinete Nacional de Segurança. É responsável por garantir um ciberespaço seguro e fiável, tanto a nível nacional como internacional. Funciona como ponto de contacto único para a cooperação internacional e tem um papel regulador abrangente. O CNCS tem poderes para emitir instruções de cibersegurança, definir níveis de alerta e emitir pareceres prévios sobre questões de cibersegurança. Além disso, colabora estreitamente com outras entidades nacionais em questões de ciberespionagem, cibercrime e proteção de dados.
- **CERT.PT:** É a entidade responsável pela coordenação operacional na resposta a incidentes de cibersegurança em Portugal. As suas competências incluem a monitorização de incidentes a nível nacional, a ativação de mecanismos de alerta rápido e a intervenção direta na análise e mitigação de incidentes. Além disso, o CERT.PT avalia dinamicamente os riscos cibernéticos e assegura a cooperação com entidades públicas e privadas, promove a adoção de práticas comuns de segurança, representa Portugal em fóruns nacionais e internacionais de cooperação em matéria de cibersegurança e participa em acções de formação para melhorar as suas capacidades.

O Capítulo III da lei em referência também implementa em Portugal os requisitos de notificação de incidentes já identificados pela diretiva. São eles:

Para a Administração Pública, os operadores de infraestruturas críticas e os operadores de serviços essenciais:

- O número de utilizadores afetados;
- A duração do incidente;
- A distribuição geográfica, no que diz respeito à área afetada pelo incidente.

Para fornecedores de serviços digitais:

- O número de utilizadores afetados pelo incidente, em especial os que dependem do serviço para prestar os seus próprios serviços;
- A duração do incidente;
- A distribuição geográfica, no que diz respeito à área afetada pelo incidente;
- O nível de gravidade da interrupção do serviço;
- A extensão do impacto nas atividades económicas e sociais.

A Diretiva NIS introduziu ainda, nos considerandos (35), (59) e (72), a referência à partilha voluntária de informação sobre incidentes em grupos de especialidade para aumentar a resiliência no combate às ciberameaças. Neste sentido, e seguindo as orientações da Diretiva, este quadro legal destaca a importância desta recomendação através do artigo 20.º, consagrando assim uma recomendação para a notificação voluntária de incidentes. Esta recomendação tem como objetivo dar a conhecer alguns tipos de incidentes mais frequentes, vulnerabilidades conhecidas, e dar uma visão geral à entidade supervisora sobre o panorama de ameaças.
Quanto à especificação das medidas de segurança, este quadro jurídico da cibersegurança remete para uma lei complementar que definirá, para além das medidas de segurança previstas, os prazos para a comunicação dos incidentes.

No que respeita às infrações, a lei prevê:

- Infrações muito graves: 5 000 a 25 000 euros, no caso de uma pessoa singular, e de 10 000 a 50 000 euros, no caso de uma pessoa coletiva;
- Infrações graves: de 1 000 a 3 000 euros, no caso de uma pessoa singular, e de 3 000 a 9 000 euros, no caso de uma pessoa coletiva; e
- Negligência: A negligência é punível, sendo os limites mínimo e máximo das coimas reduzidos para metade.

Decreto-Lei n.º 65/2021, de 30 de julho

Através da Lei n.º 46/2018, de 13 de agosto, que aprovou o regime jurídico da Cibersegurança, foi transposta para o ordenamento jurídico nacional a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016. Esta Diretiva diz respeito a medidas destinadas a garantir um elevado nível comum de segurança das redes e dos sistemas de informação em toda a União (Diretiva NIS).
A Lei n.º 46/2018 remete para legislação complementar a definição dos requisitos de segurança das redes e sistemas de informação, bem como as regras de notificação de incidentes. Estes devem ser cumpridos pela Administração Pública, operadores de infraestruturas críticas, operadores de serviços essenciais e prestadores de serviços digitais.
Assim, o presente Decreto-Lei n.º 65/2021, de 30 de julho, veio regulamentar o Regime Jurídico da Cibersegurança e definir obrigações em matéria de certificação de cibersegurança. Os requisitos previstos no Decreto-Lei em apreço constituem um mínimo a assegurar pelas entidades abrangidas pela Lei n.º 46/2018, de 13 de agosto. Tal não prejudica as regras que, em função da natureza das entidades, de aspetos específicos da atividade desenvolvida, ou do contexto em que esta se desenvolve, possam ser estabelecidas por outras autoridades.
Assim, o Decreto-Lei foca-se essencialmente na obrigatoriedade de criação de duas figuras de cooperação empresarial (o Responsável de Segurança e o Ponto de Contacto Permanente) e de análise periódica dos riscos e respetiva documentação, no reforço da colaboração entre entidades e entre estas e a entidade de supervisão, na criação de um plano de segurança adequado e proporcional à dimensão e exposição ao risco da empresa, na elaboração de um inventário de cativos, na especificação dos prazos de reporte de incidentes e na introdução de uma taxonomia de incidentes, que harmoniza e simplifica o processo de caraterização dos incidentes.

As especificidades deste diploma jurídico incidem principalmente nos seguintes temas:

- **Análise de Risco:**
  a) Análise de Risco Global:
     i. Pelo menos uma vez por ano; e/ou
     ii. Após notificação pelo CNCS de um risco, ameaça ou vulnerabilidade emergente que implique uma elevada probabilidade de ocorrência de um incidente com impacto significativo, dentro do prazo estabelecido pelo CNCS.
  b) Análise de Risco de âmbito Parcial:
     i. Durante o planeamento e a preparação para a introdução de uma alteração no ativo ou ativos, em relação ao ativo ou ativos envolvidos;
     ii. Após a ocorrência de um incidente com impacto significativo ou outra situação extraordinária, em relação aos ativos afetados; e/ou
     iii. Após notificação pelo CNCS de um risco, ameaça ou vulnerabilidade emergente que implique uma elevada probabilidade de ocorrência de um incidente com impacto significativo, dentro do prazo estabelecido pelo CNCS.

c) Documentação, preparação, execução e apresentação dos resultados das análises de risco
d) Inclusão na análise de risco de cada ativo:
    i. Identificação de ameaças, internas ou externas, intencionais ou não intencionais (falha do sistema, fenómeno natural, erro humano, ataque malicioso e/ou falha no fornecimento de bens ou serviços por terceiros); e
    ii. Caracterização do impacto e probabilidade de ocorrência das ameaças identificadas no ponto anterior.
e) Consideração dos seguintes critérios para a análise de risco:
    i. O historial de situações extraordinárias ocorridas;
    ii. O historial de incidentes e, em particular, de incidentes com impacto significativo;
    iii. O número de utilizadores afetados pelos incidentes;
    iv. A duração dos incidentes;
    v. A distribuição geográfica, em termos da área afetada pelos incidentes; e
    vi. As dependências intersectoriais para a prestação de serviços, incluindo as previstas no anexo ao Regime Jurídico da Cibersegurança e do sector das comunicações eletrónicas.
f) Adoção de medidas técnicas e organizativas adequadas à gestão dos riscos de segurança das redes e sistemas de informação que utilizam, decorrentes de regulamentação setorial aprovada pelo CNCS ou do Quadro de Referência Nacional de Cibersegurança.

> **Prazos para a notificação de incidentes:**

a) Notificação Inicial: deve ser efetuada logo que a entidade possa concluir que existe ou pode existir um impacto significativo ou substancial, e no prazo de duas horas após essa verificação;
b) b) Notificação do fim do impacto significativo ou substancial: deve ser apresentada ao CNCS o mais rapidamente possível, num prazo máximo de duas horas após a perda do impacto significativo ou substancial, e conter uma atualização em relação à notificação inicial;
c) Notificação Final: deve ser enviada no prazo de 30 dias úteis a partir do momento em que o incidente deixou de ocorrer e conter todas as informações obtidas sobre o incidente.

> **Taxonomia de incidentes:**

a) Para efeitos do presente Decreto-lei, são consideradas as seguintes categorias de causas raiz:
    i. Falha do sistema
    ii. Fenómeno natural
    iii. Erro humano
    iv. Ataque malicioso; e/ou
    v. Falha no fornecimento de bens ou serviços por terceiros.
b) Os incidentes podem ter os seguintes efeitos:
    i. Infeção por *malware*;
    ii. Disponibilidade;
    iii. Recolha de informações;

iv. Intrusão;
v. Tentativa de intrusão;
vi. Segurança da informação;
vii. Fraude;
viii. Conteúdo abusivo;
ix. Outro.

Por último, este Decreto-Lei introduz ainda um conjunto de obrigações de notificação, para além da obrigação de comunicação de incidentes anteriormente estabelecida. Assim, as entidades abrangidas são obrigadas a notificar o Centro Nacional de Cibersegurança relativamente a:

- O Ponto de Contacto Permanente;
- O Responsável pela Segurança;
- O inventário dos ativos críticos para a continuidade das operações; e
- O relatório anual.

Em síntese, este Decreto-Lei detalha a forma como as obrigações definidas na Lei n.º 46/2018, de 13 de agosto, devem ser executadas e cumpridas em termos de requisitos técnicos. Ora, como analisaremos no ponto seguinte, o Regulamento n.º 183/2022, de 21 de fevereiro de 2022, que constitui a instrução técnica do CNCS, define detalhadamente as formas de comunicação entre as entidades abrangidas pelo regime jurídico do Ciberespaço e o CNCS, para cumprimento das obrigações determinadas neste Decreto-Lei.

Regulamento n.º 183/2022 de 21 de fevereiro de 2022

O Regulamento n.º 183/2022, de 21 de fevereiro de 2022, estabelece a instrução técnica para as comunicações entre as entidades e o Centro Nacional de Cibersegurança. Esta instrução técnica está relacionada com a comunicação e informação relativa ao Ponto de Contacto Permanente, ao Responsável de Segurança, ao inventário de ativos, aos relatórios anuais e às notificações de incidentes.

Relativamente às questões mencionadas, assumem-se os cenários seguintes:

- **Envio e tratamento de informação:** Conforme indicado no artigo 1.º do regulamento em análise, a informação a enviar ao CNCS ao abrigo dos artigos 4.º (Ponto de Contacto Permanente), 5.º (Responsável de Segurança), 6.º (Inventário de Ativos) e 8.º (Relatório Anual) do Decreto-Lei n.º 65/2021, deve ser comunicada por via eletrónica para o endereço de correio eletrónico sri@cncs.gov.pt, ou através de uma API (*application programming interface*) disponibilizada pelo CNCS para o efeito. Caso as entidades pretendam enviar informação protegida por métodos criptográficos, podem proteger a informação utilizando a chave pública PGP associada ao endereço de correio eletrónico acima referido, publicada no

sítio do CNCS. O CNCS é obrigado a manter e gerir a informação recebida num sistema de informação seguro.

- **Agente de Segurança:** A designação da pessoa que vai exercer as funções de Responsável de Segurança deve ser comunicada ao CNCS nos termos dos n.ºs 2, 3 e 4 do artigo 5.º do Decreto-Lei n.º 65/2021. Assim, a comunicação ao CNCS deve indicar o nome da pessoa designada para desempenhar as funções de Responsável de Segurança e os respetivos contactos.
- **Inventário de Ativos**: As informações pormenorizadas que devem ser incluídas no inventário são definidas tanto para os equipamentos como para as aplicações:
    a) Os dispositivos e sistemas físicos devem ser inventariados com as seguintes informações:
        i. Número de inventário;
        ii. Nome e modelo do equipamento;
        iii. Número de série;
        iv. Localização;
        v. Classificação quanto ao seu carácter crítico para a entidade.
    b) Os dispositivos ligados em rede devem apresentar as seguintes informações adicionais:
        i. Endereço IP; e
        ii. Endereço *hardware*.
    c) As pessoas responsáveis pelos dispositivos e sistemas devem ser identificadas com, pelo menos, os seguintes elementos:
        i. Nome;
        ii. Contacto; e
        iii. Departamento.
    d) As aplicações devem ser registadas com as seguintes informações:
        i. Nome do *software*;
        ii. Versão;
        iii. Fabricante;
        iv. Nome da pessoa responsável;
        v. Contacto da pessoa responsável;
        vi. Departamento da pessoa responsável;
        vii. Classificação quanto ao seu carácter crítico para a entidade; e
        viii. O tipo de contrato de suporte em vigor com o fornecedor da aplicação ou plataforma de *software* (quando aplicável).
    e) Os ativos diretamente acessíveis ao público através da Internet devem ser identificados com as seguintes informações:
        i. Serviço suportado;
        ii. Nome do equipamento/nome do *software*;
        iii. Modelo/Versão;
        iv. Endereço IP (se aplicável);
        v. *Fully Qualified Domain Names* (FQDNs) (se aplicável); e

vi. Fabricante.

- **Relatório Anual:** Deve ser comunicada ao CNCS nos termos dos n.ºs 2 e 3 do artigo 8.º do Decreto-Lei n.º 65/2021, contendo a informação referida no n.º 1 do mesmo artigo. Ou seja, deve incluir as principais atividades desenvolvidas em matéria de segurança das redes e sistemas de informação, estatísticas trimestrais de incidentes, análise agregada de incidentes com impacto significativo ou substancial, recomendações de atividades, medidas ou práticas que promovam a melhoria da segurança das redes e sistemas de informação, bem como problemas identificados e medidas implementadas na sequência de incidentes.
- **Notificação de Incidentes**: O envio das notificações de incidentes e informações adicionais, nos termos dos artigos 11.º a 16.º do Decreto-Lei n.º 65/2021 (obrigação em vigor desde o último trimestre de 2021), deve ser efetuado através do sítio do CNCS (https://www.cncs.gov.pt) na funcionalidade "Notificação de Incidentes", mediante o preenchimento do modelo de reporte estabelecido para o efeito, ou via API (*application programming interface*) disponibilizada pelo CNCS para o efeito. Nos casos em que a entidade, em resultado do incidente ou por outro motivo de natureza predominantemente técnica devidamente justificado, careça temporariamente de capacidade operacional para assegurar a notificação no site do CNCS, ou nos casos em que este se encontre indisponível, a notificação poderá ser feita, excecionalmente, através de:
    - Correio eletrónico enviado para o seguinte endereço: cert@cert.pt;
    - Por telefone através do número (+351) 210 497 399;
    - Por telefone através do número (+351) 910 599 284, permanentemente disponível (24 horas por dia, sete dias por semana).

Caso as entidades pretendam enviar a notificação protegida por métodos criptográficos, podem proteger a informação utilizando a chave pública PGP, associada ao endereço de correio eletrónico referido na alínea a) do número anterior, publicada no site do CNCS.

A Diretiva (EU) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022 (Diretiva NIS2)

Introdução

A Diretiva NIS2, publicada oficialmente em 27 de dezembro de 2022 no Jornal Oficial da União Europeia, visa reforçar a postura de cibersegurança dos Estados-Membros da UE. Baseia-se na Diretiva NIS original de 2016, alargando o seu âmbito e introduzindo novas medidas para fazer face à evolução do panorama das ciberameaças.

Ambas as Diretivas visam reforçar a infraestrutura de cibersegurança e os mecanismos de resposta em toda a União Europeia. No entanto, a Diretiva NIS2 introduz vários elementos novos e melhoramentos que facilitam a adaptação à evolução do panorama das ciberameaças.

Âmbito de aplicação alargado

A NIS2 cria uma designação que diferencia as entidades essenciais das entidades importantes, em conformidade com o artigo 3.º[4]. Assim, os Anexos I e II estabelecem os sectores críticos, enquanto as entidades importantes são todas as que constam dos anexos, mas que não são abrangidas pelo conceito de entidades essenciais, nos termos do n.º 1 do artigo 3º. Além disso, foram acrescentados outros sectores e entidades à lista de sectores críticos. Não obstante, até 2025, os Estados-Membros devem estabelecer uma lista de entidades essenciais e entidades importantes, com o objetivo de identificar as entidades altamente expostas a uma ameaça cibernética significativa.

O quadro que segue abaixo destaca as entidades adicionais abrangidas pela NIS2:

Entidades Essenciais	Entidades Importantes
> Energia (Eletricidade, Sistemas de aquecimento e arrefecimento urbano, petróleo, gás e hidrogénio) > Transportes (Transporte aéreo, marítimo, ferroviário e rodoviário) > Setor bancário > Infraestruturas do mercado financeiro > Saúde (Prestadores de cuidados de saúde, laboratórios de referência da UE, entidades que fabricam produtos farmacêuticos de base e preparação farmacêuticas, entidades que realizam atividades de investigação e desenvolvimento de medicamento e entidades que fabricam dispositivos médicos considerados críticos durante uma emergência de saúde pública (lista de dispositivos médicos críticos para a emergência de saúde pública)) > Água potável > Águas residuais	> Serviços postais e de estafeta > Gestão de resíduos > Produção, fabrico e distribuição de produtos químicos > Produção, transformação e distribuição de produtos alimentares > Indústria transformadora (Fabrico de dispositivos médicos e dispositivos médicos para diagnóstico in vitro, fabrico de equipamentos informáticos, equipamentos para comunicação, produtos eletrónicos e óticos, fabrico de equipamento elétrico, fabrico de máquinas e equipamentos (não especificados), fabrico de veículos automóveis, reboques e semirreboques e fabrico de outro equipamento de transporte) > Prestadores de serviços digitais (de mercados em linha, de motores de pesquisa em linha e de plataformas de serviços de redes sociais)

[4] A Diretiva NIS (2016) apenas diferenciava entre operadores de serviços essenciais e prestadores de serviços digitais.

> Infraestrutura Digital (Fornecedores de pontos de troca de tráfego, prestadores de serviços de DNS, excluindo operadores de servidores de nomes raiz, Registos de nomes de TLD, Prestadores de serviços de computação em nuvem, Prestadores de serviços de centro de dados, Fornecedores de redes de distribuição de conteúdos, Prestadores de serviços de confiança, — Fornecedores de redes públicas de comunicações eletrónicas e Prestadores de serviços de comunicações eletrónicas acessíveis ao público) > Gestão de serviços TIC (entre empresas) > Administração Pública > Espaço	> Organismos de investigação

Para além das novas definições inseridas no artigo 6.º da nova Diretiva, onde são acrescentados mais de vinte novos conceitos em relação à NIS1, ao nível das obrigações das entidades, a nova Diretiva:

> Reforça algumas das medidas já previstas no Decreto-Lei n.º 65/2021, nomeadamente no que respeita à avaliação de riscos e ao tratamento de incidentes; e
> Inclui, de forma mais clara, um conjunto mínimo de aspetos de cibersegurança que as organizações devem abordar.

À semelhança do que estava previsto na NIS (2016), a nova diretiva mantém algumas das funções e obrigações impostas aos Estados-Membros e às instituições europeias.

Melhorias na gestão dos riscos de cibersegurança

Tanto as entidades essenciais como as importantes devem adotar medidas técnicas, operacionais e organizacionais adequadas para fazer face aos riscos que afetam a segurança das redes e dos sistemas de informação. Foram também melhorados os mecanismos de comunicação direta e de notificação de informações obrigatórias às autoridades competentes.
A presente diretiva reforça três aspetos principais da gestão de riscos:

> Políticas de análise de risco e de segurança dos sistemas de informação;
> Gestão de incidentes;

- Continuidade das atividades, como a gestão de cópias de segurança, a recuperação de desastres, e gestão de crises;
- Segurança da cadeia de abastecimento, incluindo aspetos relacionados com a segurança das relações entre cada entidade e os seus fornecedores diretos ou prestadores de serviços;
- Segurança na aquisição, desenvolvimento e manutenção de redes e sistemas de informação, incluindo o tratamento de vulnerabilidades e divulgação;
- Políticas e procedimentos para avaliar a eficácia das medidas de gestão dos riscos de cibersegurança;
- Práticas básicas de higiene cibernética e formação em cibersegurança;
- Políticas e procedimentos relativos à utilização da criptografia e, se for caso disso, da encriptação;
- Segurança dos recursos humanos, políticas de controlo de acesso e gestão de ativos;
- A utilização de soluções de autenticação multifator ou de autenticação contínua, de comunicações seguras de voz, vídeo e texto e de sistemas seguros de comunicação de emergência na entidade, se for caso disso.

Obrigações de comunicação

Ao contrário do que é atualmente referido na Lei de transposição da Diretiva NIS em Portugal, no que respeita aos limiares de notificação (incidente com impacto relevante ou substancial), as entidades abrangidas pela NIS2 são obrigadas a informar imediatamente a autoridade competente da ocorrência de qualquer incidente de cibersegurança, real ou potencial.

Isto significa que, independentemente do impacto causado, as entidades em causa devem notificar o incidente às autoridades de controlo, mesmo que se trate apenas de incidentes potenciais.

Cooperação a nível da União Europeia sobre questões de cibersegurança

Esta diretiva reforça o grupo de cooperação e a rede de equipas nacionais responsáveis pela resposta a incidentes de segurança, que se revelaram insuficientes ou inadequados no decurso da Diretiva NIS (2016). Com estes requisitos em mente, são criadas *Computer Security Incident Response Team* (CSIRT) [5] para monitorizar as ciberameaças e vulnerabilidades a nível nacional. Além disso, a Agência da União Europeia para a Cibersegurança (ENISA) fornecerá orientações e modelos relativos às obrigações dos acordos de partilha de informações. Além disso, a Diretiva NIS2 reforça a importância de os Estados-Membros garantirem que a partilha de informações possa continuar a ser feita numa base voluntária, seguindo o exemplo da sua antecessora.
Por último, a criação de um quadro para a resposta da UE a crises de cibersegurança através das redes de cooperação existentes, nomeadamente a Rede de Organizações de Coordenação de Cibercrises (EU-CyCLONe). A EU-CyCLONe é composta por representantes das autoridades de gestão de crises de

[5] Em Portugal, representado pelo CERT.PT

cibersegurança dos Estados-Membros, da Comissão Europeia (especialmente quando um incidente de cibersegurança tem um impacto significativo nos serviços e atividades abrangidos pela diretiva em questão) e da ENISA (Agência da União Europeia para a Cibersegurança).

As principais funções do EU-CyCLONe incluem:

- Preparar os Estados-Membros para a gestão de crises e incidentes de cibersegurança em grande escala.
- Criar um conhecimento geral das crises e incidentes de cibersegurança em grande escala.
- Avaliar as consequências e o impacto de crises e incidentes relevantes e propor medidas de atenuação.
- Coordenar a gestão de crises e apoiar a tomada de decisões a nível político.
- A pedido do Estado-Membro em causa, discutir os planos nacionais de resposta a crises e incidentes de cibersegurança.

Sensibilização no que respeita à cibersegurança

A diretiva incentiva a prática da ciber-higiene, que envolve passos básicos como atualizações regulares de software, formação dos funcionários e autenticação multifator, entre outros. Estas práticas visam criar uma cultura de sensibilização para a segurança em que todos os intervenientes compreendem o seu papel na proteção dos ativos digitais da organização.
O reforço destes aspetos pela Diretiva NIS2 alinha-se com a estratégia mais ampla da UE para criar um mercado único digital, em que um elevado nível de cibersegurança é essencial para a confiança dos consumidores e o funcionamento sem descontinuidades dos serviços transfronteiriços. Ao impor normas mais elevadas e promover a sensibilização, a diretiva visa criar um ecossistema digital mais resiliente, contribuindo assim para a estabilidade económica e a segurança pública.

Não cumprimento das regras estabelecidas pela NIS2

Para garantir a eficácia da fiscalização, a Diretiva prevê a aplicação de coimas em caso de incumprimento das regras estabelecidas[6]. Embora a transposição do NIS em Portugal já previsse a aplicação de coimas para este efeito, o NIS2 veio aumentar os montantes, como se pode verificar de seguida:

6 A Diretiva NIS2 prevê que "a fim de assegurar o cumprimento das obrigações estabelecidas na presente diretiva, cada autoridade competente deverá ter o poder de impor ou solicitar a aplicação de coimas".

Lei nº 46/2018	Diretiva NIS2
Infrações muito graves: 5 000 a 25 000 euros, no caso de uma pessoa singular, e de 10 000 a 50 000 euros, no caso de uma pessoa coletiva.	Entidades essenciais: coimas de um montante máximo de, pelo menos, 10 000 000 euros ou de um montante máximo de, pelo menos, 2 % do volume de negócios anual total a nível mundial realizado no exercício financeiro anterior pela empresa a que pertence a entidade essencial, consoante o montante mais elevado.
Infrações graves: 1 000 a 3 000 euros, no caso de uma pessoa singular, e 3 000 a 9 000 euros, no caso de uma pessoa coletiva.	Entidades importantes: coimas de um montante máximo de, pelo menos, 7 000 000 EUR ou de um montante máximo de, pelo menos, 1,4 % do volume de negócios anual total a nível mundial realizado no exercício financeiro anterior pela empresa a que pertence a entidade importante, consoante o montante mais elevado
Negligência: A negligência é punível, sendo os limites mínimo e máximo das coimas reduzidos para metade.	

Prazos de implementação

A Diretiva NIS2 entrou em vigor na União Europeia a 16 de janeiro de 2023. No entanto, conforme estipulado no artigo 41.º da Diretiva, a transposição da NIS2 para a legislação nacional dos Estados-Membros tem como prazo limite o dia 17 de outubro de 2024, sendo as suas disposições aplicáveis a partir de 18 de outubro de 2024.
Até à data, não houve uma consulta pública para discutir a aplicação da Diretiva NIS2, o que pode suscitar preocupações quanto ao nível de preparação, deixando as empresas e outras entidades sem orientações claras sobre a forma de se prepararem para as próximas alterações à legislação em matéria de cibersegurança.
No entanto, sabe-se que Portugal é um dos países da União Europeia que se tem atrasado na transposição das Diretivas, tendo inclusivamente falhado o prazo de implementação da Diretiva NIS. Não obstante, é aconselhável que as entidades abrangidas por estas diretivas comecem a preparar-se e a adaptar-se à nova diretiva com base na legislação europeia, mantendo o cumprimento da Diretiva NIS (2016). Tal deve-se ao facto de se esperar que algumas obrigações se mantenham inalteradas.

A transposição da Diretiva NIS 2 em Portugal

As diretrizes como legislação secundária levam à harmonização dos sistemas legais em toda a União Europeia. São particularmente úteis quando o objetivo é harmonizar as leis dentro de uma determinada área. As diretrizes podem ser dirigidas a todos os Estados-Membros ou a qualquer um deles e são vinculativas quanto ao objetivo a ser alcançado, ao prazo em que devem ser realizadas, deixando algumas escolhas quanto à forma e método abertos aos Estados-Membros[7]. Ao contrário do caso de regulamentos ou decisões, a transposição

[7] O Artigo 288.º do Tratado sobre o Funcionamento da União Europeia (TFUE) afirma: "*Uma Diretiva será vinculativa, quanto ao resultado a ser alcançado, para cada Estado-Membro a quem for endereçada, mas deixará às autoridades nacionais a escolha da forma e dos métodos*".

nacional das diretrizes é considerada necessária pelo Tratado, cujo processo visa garantir a eficácia do direito da União Europeia, de acordo com o princípio de cooperação sincera estabelecido no artigo 4(3) do Tratado da União Europeia.

Com base na experiência dos países da União Europeia e no Tribunal de Justiça Europeu na implementação de Diretivas Comunitárias, algumas regras gerais podem ser estabelecidas quanto à implementação correta de Diretivas:

- Cada Estado decide que tipo de ato legislativo deve ser promulgado com base na sua ordem constitucional para efeitos de transposição de Diretivas. No entanto, o status de promulgação doméstica deve corresponder ao status do ato que regulamentava anteriormente determinada matéria na lei doméstica.
- O órgão responsável pela promulgação de um ato de implementação é definido pela lei doméstica. Pode também ser o governo regional ou local se a questão estiver dentro da sua competência. Em qualquer caso, as agências governamentais centrais são responsáveis pela correta implementação de uma Diretiva. Os Estados não podem invocar a sua lei doméstica (incluindo disposições constitucionais) para justificar o não cumprimento das obrigações decorrentes do direito comunitário[8].
- A nomenclatura e terminologia da Diretiva não precisam ser traduzidas palavra por palavra na legislação doméstica, pois essa tradução cria o perigo de introduzir instituições desconhecidas na legislação doméstica. A legislação doméstica deve refletir o espírito ou ideia, em vez das palavras de uma Diretiva[9], o que significa que as medidas nacionais devem atingir os objetivos estabelecidos pela Diretiva.
- No entanto, no caso de algumas Diretivas, especialmente aquelas que usam uma linguagem muito técnica e são muito detalhadas, a única solução pode ser a transposição literal do texto de uma Diretiva na legislação doméstica. No entanto, não é admissível tratar a Diretiva como um anexo a um ato de legislação doméstica.
- Se necessário, a legislação doméstica em situações extremas e específicas deve citar expressamente a Diretiva que está implementando (geralmente as disposições específicas da Diretiva) para evitar interpretações equivocadas.
- As leis domésticas que transpõem diretivas devem ser promulgadas dentro do prazo estabelecido em uma Diretiva. Atrasos devido a fatores domésticos não são uma base para justificação[10].
- Se a legislação doméstica existente garante a implementação adequada de uma Diretiva ou das disposições de uma Diretiva, não há necessidade de emitir um novo ato, no entanto, a Comissão Europeia deve ser informada disso[11].
- O ato de legislação doméstica deve possuir tanto as disposições substantivas de uma Diretiva quanto os procedimentos necessários para sua implementação, incluindo órgãos competentes e as penalidades pelo não cumprimento.
- Medidas de implementação de uma Diretiva na legislação doméstica devem ser notificadas à Comissão.

[8] Case 163/78 Commission v. Italy, (1979) ECR 771
[9] Case 131/88 Commission v. Germany, (1991) ECR I825
[10] Case 43/80 Commission v. Italy, (1980) ECR 3543
[11] Case 69/90 Commission v. Italy, (1991) ECR I-6011

As diretrizes mencionadas acima são de natureza prática e seria de grande benefício segui-las ao aprovar um ato legal para a transposição da Diretiva NIS 2 em Portugal.

O princípio geral que se destaca ao transpor uma Diretiva para a legislação doméstica é que os objetivos estabelecidos pela Diretiva devem ser devidamente materializados nas regras domésticas. Portanto, uma legislação doméstica que visa implementar uma diretriz, mas que vai além dos objetivos mínimos da diretriz (referido como "gold plating"), não deve (1) impedir o funcionamento do mercado interno da UE e (2) não infringir o princípio de não discriminação nos termos do artigo 18 do TFEU.

Com a Diretiva NIS 2, o objetivo final é introduzir um alto nível comum de cibersegurança na União Europeia que irá impedir a fragmentação em diferentes níveis no mercado interno[12] e eliminar divergências nos requisitos de cibersegurança e na implementação de medidas de cibersegurança nos diferentes Estados-Membros. Esse objetivo geral de aumentar um nível comum de cibersegurança na União Europeia a longo prazo será implementado por uma avaliação coordenada de riscos a nível da União Europeia[13].
Dito isso, Portugal não deve desviar da abordagem harmonizada acordada a nível da União Europeia e deve transpor a Diretiva NIS 2 e o seu mecanismo de avaliação e risco "como está", pois apenas uma metodologia centralizada e uniforme garantirá cumulativamente o padrão igual de avaliação e assegurará a igualdade de condições no mercado entre os operadores.
O exercício de transposição da Diretiva NIS 2 em Portugal também deve levar em consideração os Princípios Gerais do Direito da União Europeia, nomeadamente:

- Os princípios de livre circulação de bens e liberdade de prestação de serviços estabelecidos nos artigos 28, 34 e 56 do TFEU, proíbem qualquer restrição quantitativa e todas as medidas que tenham um efeito equivalente sobre bens ou serviços dentro do mercado interno. Restrições à livre circulação só podem ser justificadas se servirem a um objetivo legítimo e forem proporcionais. Embora a proteção da segurança nacional possa, em princípio, constituir um objetivo legítimo, a exceção de segurança pública disponível nos termos do TFEU é interpretada de forma restrita. Está disponível apenas quando existe "uma ameaça genuína e suficientemente séria que afeta um dos interesses fundamentais da sociedade[14]". Portanto, Portugal não deve criar barreiras à livre circulação de uma variedade de bens e tecnologia sem identificar claramente uma "ameaça cibernética", conforme definido pela Diretiva NIS 2.
- O princípio da proporcionalidade (Artigo 5(4) do Tratado da União Europeia (TUE)), que exige que uma medida não vá além do que é necessário para alcançar seu objetivo, ou seja, uma medida deve servir ao objetivo perseguido para ser proporcional. Portanto, Portugal deve seguir as medidas de segurança técnica estabelecidas na Diretiva NIS 2 e abster-se de estabelecer critérios não técnicos (políticos), considerando sua natureza desproporcional.

[12] Vide considerando (4), NIS 2 Directive
[13] Vide considerando (4), NIS 2 Directive
[14] Case C-546/07, Commission v Germany (2000) EU:C:2010:25

- O princípio da segurança jurídica, segundo o qual os Estados-Membros precisam redigir suas regras legais "de forma inequívoca" para que as entidades envolvidas tenham uma compreensão clara e precisa de seus direitos e obrigações e para permitir que os tribunais nacionais garantam que esses direitos e obrigações sejam respeitados. Qualquer critério não técnico (político) está sujeito a uma interpretação ampla e, portanto, dificuldade de implementação pelas entidades e interpretação por reguladores e tribunais nacionais.
- O princípio da não discriminação (Artigo 2 TUE, 18 TFEU) na medida em que qualquer critério de avaliação que não seja baseado em critérios objetivos torna o mecanismo de avaliação de risco inerentemente discriminatório e em contradição com este princípio da UE.

Um ponto adicional que vale a pena mencionar é a aplicabilidade das regras nacionais sob a Diretiva nº 2015/153522 (Diretiva TRIS).

De acordo com esta Diretiva, quando um Estado-Membro tem a intenção de promulgar uma lei que contenha regulamentos técnicos, relacionados a produtos, o Estado-Membro deve notificar a Comissão Europeia. Em suma, um regulamento técnico é um regulamento (uma lei em um Estado-Membro) que os Estados-Membros pretendem introduzir para produtos, proibindo a fabricação, importação, comercialização ou uso de um produto ou proibindo a prestação ou uso de um serviço ou estabelecimento como fornecedor de serviço. O objetivo da notificação é garantir que os textos estejam em conformidade com a legislação da União Europeia e os princípios do mercado interno.

A partir do momento da notificação, começa a correr um período de três meses, conhecido como "período de espera". Durante esses três meses, o Estado-Membro notificante não pode adotar a regra técnica relevante. A Comissão publica a notificação através do Sistema de Informação de Regulamentação Técnica (TRIS). O período de espera permite que a Comissão e os outros Estados-Membros examinem a intenção de um regulamento técnico e reajam adequadamente. Se parecer que a intenção de adotar o regulamento técnico pode prejudicar a livre circulação de bens ou serviços, ou a legislação secundária da União Europeia, o período de espera pode ser prorrogado por mais três meses, durante os quais o Estado-Membro terá de propor emendas para acomodar as preocupações legais levantadas.

Conclusão

A Diretiva NIS 2 representa uma evolução significativa em relação à sua predecessora de 2016. Ela aborda lacunas e ambiguidades na diretiva original, oferecendo um arcabouço mais abrangente e detalhado para a cibersegurança na UE. Ao expandir seu escopo, aprimorar definições e introduzir novas medidas para gestão de riscos e capacidades operacionais, a NIS 2 tem como objetivo criar um ambiente digital mais resiliente e seguro em toda a UE.

A diretiva também tem o potencial de harmonizar as práticas de cibersegurança em toda a UE, facilitando a cooperação transfronteiriça e tornando o mercado único digital mais seguro para consumidores e empresas.
Em resumo, a NIS 2 não é apenas uma atualização legislativa; é uma mudança de paradigma que coloca a cibersegurança no centro das estratégias digitais, impactando não apenas o funcionamento das empresas, mas também a forma como os Estados-Membros colaboram para enfrentar ameaças cibernéticas emergentes.
Em conformidade com os princípios fundamentais do direito da União Europeia, os Estados-Membros devem agir em pleno respeito à abertura do mercado interno da União Europeia e aos seus princípios.
Embora a Diretiva NIS 2 apresente uma harmonização mínima (conforme endossado pelo Artigo 5 da Diretiva NIS 2), os Estados-Membros, ao buscar adotar ou manter disposições que garantam um nível mais elevado de cibersegurança, devem respeitar as obrigações estabelecidas no direito da União Europeia.
Portugal deve, portanto, garantir, durante a transposição da Diretiva NIS 2, que não sejam criadas barreiras no mercado interno da União Europeia e que critérios desproporcionais e pouco claros não sejam estabelecidos.

Para obter informação adicional sobre o conteúdo deste documento, por favor dirija-se ao seu contacto habitual na *Cuatrecasas.*