NIS 2 | Novo Regime Jurídico da Cibersegurança

Conformidade legal, resiliência operacional e responsabilidade da gestão

Enquadramento Geral

A Diretiva (UE) 2022/2555, conhecida como NIS 2, foi transposta para o ordenamento jurídico nacional através do **Decreto-Lei n.º 125/2025**, que aprova o novo Regime Jurídico da Segurança do Ciberespaço. Este diploma revoga o regime anterior de 2018, introduzindo um quadro normativo substancialmente mais exigente, alinhado com as melhores práticas europeias em matéria de cibersegurança.

Num contexto de crescente digitalização, interdependência tecnológica e sofisticação das ameaças cibernéticas, a NIS 2 assume-se como um pilar essencial de **resiliência operacional, continuidade de negócio e conformidade legal**, alargando significativamente o seu âmbito de aplicação a setores e entidades anteriormente não abrangidos.

Objetivos Estratégicos

O Decreto-Lei n.º 125/2025 prossegue objetivos claros e estruturantes:

- **Reforço da ciberresiliência:** assegurar que entidades públicas e privadas dispõem de capacidades adequadas para prevenir, resistir, responder e recuperar de incidentes de cibersegurança.
- **Harmonização nacional e europeia:** alinhamento dos requisitos de segurança entre Estados-Membros, sob coordenação e supervisão do Centro Nacional de Cibersegurança (CNCS).
- **Segurança da cadeia de abastecimento:** imposição de obrigações específicas de avaliação e gestão dos riscos associados a fornecedores e prestadores de serviços críticos.
- **Responsabilização dos órgãos de gestão:** integração da cibersegurança como matéria de governação, com deveres diretos e consequências legais e financeiras para administradores e gerentes.

Quem Está Abrangido

O novo regime expande de forma significativa o universo de entidades obrigadas, adotando um critério combinado de **setor de atividade e dimensão organizacional.**

Critério de Dimensão (Regra Geral)

Estão abrangidas as entidades que operem nos setores identificados pela lei e que se qualifiquem como **médias ou grandes empresas**, designadamente:

- Mais de 50 trabalhadores; ou
- Volume de negócios anual ou balanço total superior a 10 milhões de euros.

Nota: Determinadas entidades (por exemplo, fornecedores de redes públicas de comunicações eletrónicas, serviços de confiança ou infraestruturas digitais críticas) encontram-se abrangidas independentemente da sua dimensão.

Classificação das Entidades Abrangidas

O regime distingue dois níveis de entidades, com diferentes graus de exigência regulatória e modelos de supervisão (ex-ante e ex-post):

Entidades Essenciais (Alta Criticidade)

- Energia (eletricidade, petróleo, gás, hidrogénio)
- Transportes (aéreo, ferroviário, marítimo e rodoviário)
- Saúde (hospitais, indústria farmacêutica, laboratórios)
- Água potável e águas residuais
- Infraestruturas digitais e serviços TIC (cloud, data centers, redes)
- Administração Pública (central e regional)
- Setor bancário e mercados financeiros

Entidades Importantes (Outros Setores Críticos)

- Serviços postais e de estafeta
- Gestão de resíduos
- Fabricação, produção e distribuição de produtos químicos
- Produção, transformação e distribuição de alimentos
- Indústria transformadora (dispositivos médicos, eletrónica, maquinaria)
- Fornecedores de serviços digitais (marketplaces, motores de busca)
- Investigação e instituições de ensino com atividades de I&D relevantes

O Que Muda com o Decreto-Lei n.º 125/2025

- **Registo obrigatório:** as entidades abrangidas devem efetuar o registo na plataforma eletrónica do CNCS, nos prazos legalmente previstos.
- **Designação de Responsável de Cibersegurança:** é obrigatória a nomeação de um Responsável de Cibersegurança (CISO) e de um Ponto de Contacto Permanente, com comunicação formal ao CNCS.
- **Modelo de supervisão diferenciado:**
    - As **Entidades Essenciais** estão sujeitas a fiscalização preventiva e contínua.
    - As **Entidades Importantes** são, regra geral, fiscalizadas de forma reativa, na sequência de incidentes ou indícios de incumprimento.

Requisitos de Segurança e Gestão de Riscos
(Artigo 20.º do Decreto-Lei n.º 125/2025)

As entidades devem implementar medidas técnicas, operacionais e organizativas adequadas e proporcionais aos riscos identificados. O regime nacional prevê, entre outras, as seguintes obrigações mínimas:

- Definição de **políticas de segurança da informação**, suportadas por análises de risco periódicas;
- **Prevenção, deteção e gestão de incidentes** de cibersegurança;
- **Continuidade de negócio e resiliência operacional**, incluindo planos de gestão de crises, cópias de segurança e recuperação de desastres;
- **Gestão da segurança da cadeia de abastecimento**, com avaliação sistemática de fornecedores e prestadores de serviços críticos;
- Utilização de **mecanismos de criptografia e controlo de acessos** adequados;
- Promoção da **higiene cibernética**, incluindo ações de sensibilização e formação dos colaboradores.

Notificação de Incidentes
(Artigo 23.º – Regime das 24 Horas)

A NIS 2 introduz um modelo de reporte em cascata particularmente exigente. Os incidentes significativos — isto é, aqueles que causem perturbações operacionais relevantes ou impactos financeiros ou materiais — devem ser comunicados ao CNCS nos seguintes termos:

- **Até 24 horas (aviso prévio):** notificação inicial com indicação preliminar da natureza do incidente, eventual origem ilícita e impacto transfronteiriço.
- **Até 72 horas (notificação de incidente):** atualização com avaliação inicial da gravidade e indicadores de compromisso.
- **Até 1 mês (relatório final):** descrição detalhada do incidente, análise da causa raiz, medidas de mitigação adotadas e lições aprendidas.

Responsabilidade dos Órgãos de Gestão

Cibersegurança como dever de governação

O novo regime representa uma mudança estrutural ao nível da governação:

- **Aprovação formal** das políticas e medidas de gestão de riscos de cibersegurança;
- **Supervisão efetiva** da sua implementação;
- **Formação obrigatória** em matérias de cibersegurança para membros dos órgãos de administração ou gestão;
- **Responsabilidade civil pessoal**, sempre que o incumprimento origine danos para a entidade ou terceiros.

Serviço BDO | NIS 2

Da interpretação legal à implementação operacional

Abordagem Metodológica

A nossa intervenção assenta numa abordagem faseada, proporcional ao setor, dimensão e perfil de risco da entidade:

1. Diagnóstico de Enquadramento Legal e Regulatório

- Determinação do estatuto da entidade (Essencial ou Importante);
- Análise do âmbito de aplicação material e subjetivo;
- Avaliação do modelo de supervisão aplicável (ex-ante ou ex-post).

2. Avaliação de Maturidade e Análise de Lacunas (Gap Analysis)

- Avaliação do sistema de gestão de cibersegurança face ao artigo 20.º do Decreto-Lei n.º 125/2025;
- Identificação de gaps técnicos, organizativos e documentais;
- Priorização de riscos com impacto legal e operacional.

3. Desenho e Implementação do Modelo NIS 2

- Definição e formalização de políticas e procedimentos de segurança;
- Apoio na estruturação da função de Responsável de Cibersegurança (CISO);
- Integração da segurança da cadeia de abastecimento nos processos de compras e outsourcing;
- Articulação com frameworks reconhecidas (ISO 27001, NIST, ENS).

4. Governança, Formação e Responsabilização da Gestão

- Apoio à aprovação formal das medidas pelos órgãos de gestão;
- Programas de formação obrigatória para administradores e gerentes;
- Definição de mecanismos de supervisão e reporting.

5. Preparação para Incidentes e Supervisão do CNCS

- Implementação de procedimentos de notificação nos prazos legais;
- Testes de resposta a incidentes e simulações (tabletop exercises);
- Apoio em ações de fiscalização e pedidos de informação do CNCS.

Benefícios para a Organização

- Conformidade legal robusta e auditável;
- Redução do risco de sanções financeiras e reputacionais;
- Reforço da resiliência operacional e da continuidade de negócio;
- Proteção dos órgãos de gestão face a riscos de responsabilidade pessoal;
- Alinhamento com melhores práticas europeias de cibersegurança.

Regime Sancionatório (Artigos 51.º e 52.º) (Artigos 51.º e 52.º)

O Decreto-Lei n.º 125/2025 estabelece um regime sancionatório robusto, alinhado com o nível de exigência do RGPD:

- Entidades Essenciais: coimas até 10.000.000 € ou 2% do volume de negócios anual mundial do exercício anterior (o montante mais elevado).
- Entidades Importantes: coimas até 7.000.000 € ou 1,4% do volume de negócios anual mundial (o montante mais elevado).

Sanções acessórias

Para além das coimas, podem ser aplicadas, entre outras, as seguintes sanções:

- Interdição temporária do exercício de funções de gestão ou administração;
- Suspensão de certificações, licenças ou autorizações relevantes;
- Publicação da decisão sancionatória em Diário da República e nos meios de comunicação social.

Entre em contato connosco

Saiba como implementar o NIS 2 | Novo Regime Jurídico da Cibersegurança na sua organização.

César Benú Soares
Manager | ISA
cesar.soares@bdo.pt
+351 937 990 127

Rute Miriam Neto
Supervisor | ISA
rute.neto@bdo.pt
+351 932 301 733

Lisboa

Av. República, 50,
10º 1069-211 Lisboa
T+ 351 21 799 0420
Mail: bdo@bdo.pt

Faro

Rua Dr. Manuel Arriaga 23
A 8000-334 Faro - Portugal
T+ 351 289 880 820
Mail: bdo.faro@bdo.pt

Porto

Rua S. João Brito, 605E Esc.
3.2 4100-455 Porto
T+ 351 226 166 140
Mail: bdo.porto@bdo.pt

Maia

Rua da Nossa Sra. da Maia,
77 Sala 16 4470-204 Maia
T+ 351 229 436 960
Mail: bdo.maia@bdo.pt

Braga

Rua Marcelino Sá Pires, 15 -
4º, Sala 43 4700-924 Braga
T+ 351 253 600 390
Mail: bdo.braga@bdo.pt

Leiria

Rua da Europa, EDF 2000 B,
3º,Escritório 1, 2400-136
LeiriaT+351 217 990 420
Mail: bdo.leiria@bdo.pt

Funchal

Rua dos Aranhas, 5, r/c
9000-044 Funchal
T+ 351 291 213 370
Mail: bdo.funchal@bdo.pt