Bom dia,

Bem-vindo(a) à newsletter #114 da DPO Consulting, o nosso meio informativo sobre o mundo da Privacidade, Proteção de Dados, *Compliance* e Inteligência Artificial.

Contacte-nos e leve a sua conformidade a outro nível.

Proteja os Dados. Reforce a Confiança. Simplifique a Conformidade.

Novo Decreto-Lei 125/2025: A NIS2 está oficialmente transposta. O que muda para as organizações portuguesas?

Foi publicado esta quarta-feira em Diário da República o Decreto-Lei n.º 125/2025, de 4 de dezembro, que transpõe a Diretiva (UE) 2022/2555 – NIS2,

estabelecendo o novo regime jurídico de cibersegurança aplicável a entidades essenciais e importantes em Portugal.

A entrada em vigor está prevista para o 2.º trimestre de 2026, deixando às organizações um período curto para se prepararem perante um enquadramento significativamente mais exigente.

A NIS2 representa uma das reformas mais ambiciosas da União Europeia no domínio da resiliência digital, elevando padrões, ampliando o número de setores abrangidos e reforçando a responsabilização da gestão de topo.

Os principais objetivos da NIS2

A Diretiva NIS2 foi construída com metas muito claras, que agora passam a ser obrigatórias no ordenamento jurídico português:

1. Elevar o nível comum de cibersegurança na UE
Uniformizar regras, reduzir disparidades entre Estados-Membros e criar uma base mínima robusta de proteção, transversal aos setores público e privado.

2. Alargar o âmbito de aplicação
Ao contrário da NIS de 2018, a NIS2 abrange um número muito maior de entidades, incluindo:

- Energia, transportes, água, saúde, infraestruturas digitais
- Administração pública
- Indústria química, alimentar e farmacêutica
- Serviços financeiros e seguros
- Correios, digital providers, data centers, e-commerce

Para muitas organizações, este é o primeiro contacto com obrigações formais de cibersegurança, com impactos profundos na sua operação.

3. Reforçar a gestão de riscos e medidas de segurança
A NIS2 introduz um conjunto de requisitos mínimos obrigatórios, incluindo:

- Políticas de gestão de riscos de cibersegurança
- Gestão de incidentes
- Continuidade de negócio e recuperação
- Segurança da cadeia de fornecimento
- Ciber-higiene e formação
- Políticas de controlo de acesso
- Auditorias e avaliação periódica

Esta abordagem impõe um modelo contínuo, não meramente documental.

4. Responsabilizar a gestão de topo
Um dos aspetos mais transformadores da NIS2 é a exigência de envolvimento direto da administração e da gestão executiva na supervisão das políticas de cibersegurança.

Prevê-se responsabilidade sancionatória quando a gestão falha no cumprimento dos deveres de governação.

5. Reforçar mecanismos de reporte
As entidades abrangidas terão prazos apertados para notificar incidentes significativos, assegurando:

- Notificação inicial em 24 horas
- Relatório intermédio em 72 horas
- Relatório final em 30 dias

Este mecanismo pretende aumentar a transparência e a capacidade europeia de resposta coordenada.

Porque é que a NIS2 é tão relevante para as organizações portuguesas?

1. Portugal está entre os países mais visados por ciberataques na UE
Os incidentes têm aumentado de forma consistente, especialmente ataques de:

- Ransomware
- Interrupção operacional
- Phishing avançado
- Compromissos de supply chain

A NIS2 coloca disciplina e maturidade num contexto onde muitas organizações ainda estão em níveis iniciais.

2. Exigência regulatória + impacto reputacional
A não conformidade pode resultar em:

- multas elevadas
- perdas operacionais
- responsabilidade para administradores
- danos reputacionais sérios
- restrições de atividade em setores críticos

A NIS2 não é apenas uma obrigação legal: é um requisito estratégico de sobrevivência.

3. Competitividade internacional
A adoção de padrões NIS2 reforça:

- Confiança de investidores
- Resiliência operacional
- Acesso a cadeias internacionais
- Alinhamento com certificações e frameworks globais (ISO 27001, NIST, DORA, etc.)

Organizações não conformes arriscarão ficar "fora do circuito".
A DPO Consulting está preparada para apoiar a implementação da NIS2

Com equipas especializadas em cibersegurança, governance, auditorias e implementação, a DPO Consulting dispõe de uma abordagem integrada que inclui:

- Diagnóstico NIS2 (gap analysis)
- Plano de implementação e governança
- Desenvolvimento de políticas, processos e procedimentos
- Modelos de gestão de risco
- Apoio na preparação para auditorias do CNCS

- Formação executiva e técnica
- Programas de literacia e capacitação
- Consultoria contínua e monitorização

A NIS2 exige competência técnica, visão jurídica e capacidade estratégica, um tripé que está no centro da atuação da DPO Consulting.

Fale connosco para agendar um diagnóstico inicial

Partilhe, querendo, a newsletter da DPO Consulting.

Ficamos ao dispor para qualquer esclarecimento que haja por conveniente e voltamos ao contacto na próxima newsletter, com mais novidades e informações de relevo.

Até breve.
Elsa Veloso
CEO da DPO Consulting

DPO Consulting
Avenida da República, nº 18 3º - 1050-191 Lisboa
Rua Eugénio de Castro, 370 – H185 4100-225 Porto