

Informação Empresarial

NOVO REGIME JURÍDICO DA CIBERSEGURANÇA: O QUE MUDA PARA AS EMPRESAS?



Com a publicação do **Decreto-Lei n.º 125/2025**, Portugal adaptou-se às novas regras europeias de cibersegurança (a conhecida **Diretiva NIS2**). O objetivo é simples: tornar o nosso tecido empresarial mais resistente a ataques informáticos, que são cada vez mais frequentes e agressivos.

Este novo regime entra oficialmente em vigor a **3 de abril de 2026** e traz obrigações muito concretas para milhares de entidades em Portugal.

A MINHA EMPRESA É OBRIGADA A CUMPRIR?

Geralmente, se a empresa opera num dos setores abaixo e tem **mais de 50 trabalhadores** ou uma faturação **anual superior a 10 milhões de euros**, é muito provável que esteja abrangida.

Nota importante: Mesmo que a empresa seja uma micro ou pequena empresa (menos de 50 trabalhadores), pode ficar abrangida, se for um fornecedor crítico de uma grande empresa, privada ou de um organismo público. A segurança da cadeia de abastecimento é um dos pontos fortes da NIS2.

A lei divide as empresas abrangidas em dois grandes grupos: **Entidades Essenciais** e **Entidades Importantes**. O critério principal tem a ver com o setor de atividade e a dimensão da empresa.

> SETORES ALTAMENTE CRÍTICOS (ENTIDADES ESSENCIAIS)

- Energia (eletricidade, petróleo, gás, hidrogénio)
- Transportes (aéreo, ferroviário, marítimo e rodoviário)
- Saúde e banca, nfraestruturas digitais e administração pública

> OUTROS SETORES CRÍTICOS (ENTIDADES IMPORTANTES)

- Serviços postais e de estafeta
- Gestão de resíduos
- Produção, fabrico e distribuição de produtos químicos
- Produção, transformação e distribuição de produtos alimentares
- Fabrico de produtos eletrónicos, maquinaria e equipamento de transporte, Fornecedores de serviços digitais (como plataformas de comércio eletrónico ou

QUAIS SÃO AS PRINCIPAIS IMPLICAÇÕES PARA AS EMPRESAS?

- **Responsabilidade da Gestão de Topo:** A administração e a gerência passam a ser diretamente responsáveis pela aprovação e supervisão das medidas de cibersegurança.
- **Nomeação de um Responsável:** Até 20 dias úteis após a entrada em vigor da lei (ou seja, no final de abril de 2026), as empresas têm de nomear um Responsável de Cibersegurança e um ponto de contacto permanente (24/7) para comunicar com o Centro Nacional de Cibersegurança (CNCS).
- **Avaliação de Riscos e Planos de Continuidade:** É obrigatório mapear os riscos informáticos e ter um plano de como a empresa continua a trabalhar se sofrer um ataque (cópias de segurança, planos de recuperação).
- **Reporte de Incidentes:** Se houver um ataque ou falha grave, a empresa tem prazos muito curtos (em alguns casos, alertas iniciais em 24 horas) para notificar o CNCS.
- **Formação:** Dar formação básica de cibersegurança aos trabalhadores passa a ser uma obrigação legal.

E SE A EMPRESA NÃO CUMPRIR?

O regime sancionatório é pesado. As coimas para incumprimentos graves podem chegar aos **10 milhões de euros ou 2% do volume de negócios anual a nível mundial** (o que for mais elevado). No entanto, há um período de carência de 12 meses (até abril de 2027) onde não serão aplicadas coimas se a empresa demonstrar que já está a fazer um esforço interno e um plano para se adaptar.

Esta informação, não dispensa a consulta da legislação indicada: a [Diretiva NIS2](#), explicação sobre a Diretiva do [Centro Nacional de Cibersegurança \(CNCS\) – Informação sobre a Diretiva NIS 2](#) e o [Decreto-Lei n.º 125/2025, de 4 de dezembro](#).