CS'Legal Update 12'25

Diretiva NIS2 em Portugal: o Decreto-Lei n.º 125/2025, de 4 de dezembro confirma o Novo Regime Jurídico da Cibersegurança.

Diogo Frada Almeida
ASSOCIADO COORDENADOR

Joana Alves Trindade
ASSOCIADA

A Diretiva UE 2022/2555 (Diretiva NIS2) foi oficialmente transposta para a legislação portuguesa através do Decreto-Lei n.º 125/2025, publicado no Diário da República em 4 de dezembro de 2025. O Novo Regime Jurídico de Cibersegurança transpõe para o ordenamento jurídico português o quadro regulatório comum de Cibersegurança na União Europeia estabelecido pela Diretiva NIS2.

Com a entrada em vigor do Novo Regime Jurídico de Cibersegurança em Portugal, as entidades enfrentam um novo padrão de responsabilidade digital e requisitos de cibersegurança. Mais do que um conjunto de obrigações, trata-se de um novo paradigma de responsabilidade em matéria de cibersegurança, exigindo planeamento, investimento e compromisso das organizações, enquanto representa uma oportunidade para reforçar a confiança, a competitividade e a resiliência num ambiente digital cada vez mais complexo e interdependente.

I. Entidades abrangidas

O Novo Regime Jurídico de Cibersegurança aplica-se a Entidades consideradas essenciais, importantes, ou entidades públicas relevantes.

Entidades essenciais:

- Entidades de um dos tipos referidos no Anexo I do Decreto-Lei n.º 125/2025, que excedam os limiares previstos para as médias empresas;
- Prestadores de serviços de confiança qualificados e registo de nomes de domínio de topo e prestadores de serviços de sistemas de nomes de domínio;
- Empresas que oferecem redes públicas de comunicações eletrónicas ou serviços de comunicações eletrónicas acessíveis ao público que sejam consideradas médias empresas;

- Entidades da Administração Pública que tenham como atribuições a prestação de serviços nas áreas do desenvolvimento, manutenção e gestão de infraestruturas de tecnologias de informação e comunicação ou aquelas que apresentem um grau particularmente elevado de integração digital na prestação dos seus serviços, e ainda a entidade pública responsável pela área da avaliação educativa;
- Entidades identificadas como críticas, nos termos da Diretiva (UE) 2022/2557 do Parlamento Europeu e o Conselho, de 14 de dezembro, relativa à resiliência das entidades críticas.

Entidades Importantes:

- Entidades dos tipos referidos nos Anexos I e II do Decreto-Lei n.º 125/2025 que não sejam consideradas entidades essenciais;
- Outras entidades de um dos tipos constantes nos Anexos I ou II que sejam identificadas como entidades importantes, que justifiquem tal qualificação com base no respetivo grau de exposição da entidade aos riscos, na dimensão da entidade e na probabilidade de ocorrência de incidentes e a sua gravidade, incluindo o seu impacto social e económico.

Entidades Públicas relevantes

- Entidades da Administração Pública, incluindo organismos e serviços dependentes do Estado, salvo aqueles com funções especificamente excluídas no diploma (defesa nacional, segurança interna, serviços de informações e investigação criminal).

A qualificação das entidades em essenciais ou importantes tem por base os setores identificados no Anexo I e II do Decreto-Lei n.º 125/2025. A tabela seguinte elenca os setores indicados nos Anexos I e II do Decreto-Lei n.º 125/2025:

Setores de Importância Crítica Anexo I	Outros Setores Críticos Anexo II
Energia	Serviços Postais e Estafetas
Transportes	Gestão de Resíduos
Sector Bancário	Produção, fabrico e distribuição de produtos químicos
Infraestruturas do mercado financeiro	Produção, transformação e distribuição de produtos alimentares
Saúde	Indústria transformadora
Água Potável	Prestação de Serviços Digitais
Águas Residuais	Investigação
Infraestruturas Digitais	
Gestão de Serviços de tecnologias de informação	
Espaço	

II. O que muda na prática – principais obrigações e prazos

O Novo Regime Jurídico de Cibersegurança impõe um conjunto de novas obrigações às entidades abrangidas, incluindo:

- Os órgãos de gestão, direção e administração de entidades essenciais e importantes devem aprovar as medidas de gestão de risco de cibersegurança, supervisionar a aplicação de medidas e assegurar a periodicidade regular de ações de formação em cibersegurança, de forma a promover uma cultura de gestão interna sobre práticas de gestão dos riscos de cibersegurança.

- As entidades essenciais e importantes são responsáveis por garantir a segurança das redes e dos sistemas de informação, tomando as medidas técnicas, operacionais e organizativas adequadas para gerir os riscos que se colocam à segurança das redes e dos sistemas de informação que utilizam nas suas operações e para impedir ou minimizar o impacto de incidentes nos destinatários dos seus serviços e noutros serviços.

- As entidades essenciais e importantes devem adotar, tendo em consideração a matriz de risco definida, medidas de cibersegurança, nomeadamente, nas seguintes áreas:
  - › Tratamento de incidentes;
  - › Continuidade de atividades;
  - › Segurança da cadeia de abastecimento;
  - › Segurança na aquisição, desenvolvimento e manutenção dos sistemas de rede e de informação;
  - › Políticas e procedimentos para avaliar a eficácia das medidas de gestão de risco de cibersegurança;
  - › Práticas básicas de ciber-higiene e formação em cibersegurança;
  - › Políticas e procedimentos relativos à utilização de criptografia e de cifragem;
  - › Segurança dos recursos humanos;
  - › Utilização de autenticação multifator, entre outras.

- As medidas de cibersegurança a adotar relativas à segurança da cadeia de abastecimento devem considerar:
  - › As vulnerabilidades de cada fornecedor direto e de cada prestador de serviços;
  - › A qualidade global dos produtos na componente de cibersegurança;
  - › As práticas de cibersegurança dos fornecedores e prestadores;
  - › As avaliações coordenadas dos riscos de segurança de cadeias de abastecimento de produtos de TIC, sistemas de TIC ou serviços de TIC críticos;
  - › As decisões relativas a aplicações de restrições à utilização, a cessação de utilização ou exclusão de equipamentos, componentes ou serviços de tecnologias de informação e comunicação.

- As entidades essenciais e importantes devem elaborar e manter um relatório anual e enviar ao Centro Nacional de Cibersegurança.

- As entidades essenciais, importantes e públicas relevantes devem notificar à autoridade de cibersegurança competente qualquer incidente significativo. De acordo com o Novo Regime Jurídico de Cibersegurança, um incidente significativo corresponde a um incidente que: (i) Cause, ou seja suscetível de causar, graves perturbações operacionais dos serviços ou perdas financeiras à entidade em causa; e (ii)Afete, ou seja suscetível de afetar outras pessoas singulares ou coletivas, causando danos materiais ou imateriais consideráveis.

Prazos de adaptação:

- O Novo Regime Jurídico da Cibersegurança entrará em vigor no dia **3 de abril de 2026** (120 dias após a sua publicação), e o Centro Nacional de Cibersegurança terá de aprovar as normas regulamentares de execução, designadamente quanto ao funcionamento da plataforma eletrónica, Quadro Nacional de Referência para a Cibersegurança e medidas de cibersegurança mínimas. Algumas normas do Novo Regime Jurídico de Cibersegurança apenas produzirão efeitos após ter decorrido o prazo de 24 meses para a aprovação das normas regulamentares.

III. Sanções aplicáveis

O incumprimento das obrigações e normas previstas no Novo Regime Jurídico da Cibersegurança pode ser objeto da aplicação de coimas até €10 milhões ou 2% do volume de negócios anual a nível mundial, bem como de sanções acessórias ou sanções pecuniárias compulsórias.

IV. Recomendações

Para garantir conformidade e reduzir riscos, as entidades devem:

- Avaliar a aplicabilidade do Novo Regime Jurídico da Cibersegurança e após esta análise, devem promover a identificação da entidade junto do Centro Nacional de Cibersegurança.
- Rever políticas e processos internos e alinhá-las com as novas exigências e requisitos legais, adotando as medidas mais adequadas às entidades.
- Definir um plano de implementação com prazos, responsabilidades e métricas de controlo.
- Promover formação contínua e uma verdadeira cultura de segurança digital. CS