NOVO REGIME JURÍDICO DE CIBERSEGURANÇA

Decreto – Lei n.º 125/2025, de 4 de dezembro

O Decreto - Lei n.º 125/2025, de 4 de dezembro, concretiza a transposição da Diretiva (UE) 2022/2555 para o ordenamento jurídico português, introduzindo um conjunto de medidas destinadas a fortalecer e harmonizar o quadro de cibersegurança no âmbito da União Europeia.

ENTIDADES ABRANGIDAS

Para responder ao agravamento das ciberameaças, capazes de comprometer a segurança nacional de diversas entidades, em múltiplos setores, o novo regime amplia o conjunto de entidades abrangidas, ajustando as obrigações à sua dimensão e relevância.

Com efeito, o regime é aplicável a:

- **Entidades da Administração Pública,** incluindo organismos e serviços dependentes do Estado, salvo aqueles com funções especificamente excluídas no diploma (segurança nacional, defesa e serviços de informações, investigação criminal e órgãos de polícia criminal)
- **Entidades privadas consideradas essenciais ou relevantes** para a segurança do ciberespaço, designadamente:
  - operadores de serviços essenciais,
  - operadores de infraestruturas críticas,
  - prestadores de serviços digitais,
  - entidades cuja dimensão ou natureza da atividade determine risco elevado para a continuidade de serviços

essenciais ou para a segurança nacional.

- **Demais entidades abrangidas por critérios setoriais específicos**, a definir pelas autoridades competentes no âmbito do Quadro Nacional de Referência para a Cibersegurança.

MEDIDAS

Por outro lado, **o regime reforça igualmente três instrumentos centrais da política pública de cibersegurança**:

- a **Estratégia Nacional de Segurança do Ciberespaço**, que fixa prioridades e objetivos estratégicos;
- o **Plano Nacional de Resposta a Crises e Incidentes de grande escala**, que aprimora a gestão destes eventos; e,
- o **Quadro Nacional de Referência para a Cibersegurança**, que sistematiza e difunde normas, padrões e boas práticas.

Este regime **alarga ainda o quadro institucional existente, reforçando o papel do Centro Nacional de Cibersegurança como autoridade nacional** e criando autoridades de supervisão setoriais e especiais, as quais contribuem para uma distribuição mais equilibrada das funções de supervisão.

Paralelamente, **estabelece-se um modelo de cooperação e interoperabilidade entre as entidades públicas com competências em cibersegurança e segurança interna e externa**, promovendo a circulação eficaz de informação e a coordenação na prevenção, deteção e resposta a incidentes.

Entre as **principais medidas**, destaca-se:

- Definição de critérios para identificação das entidades abrangidas pelo regime e ampliação do conjunto de entidades abrangidas pelo mesmo;
- Diferenciação entre entidades essenciais, entidades importantes e entidades públicas relevantes, para efeitos da aplicação do regime jurídico da cibersegurança aprovado;
- Definição dos instrumentos estruturantes da segurança do Ciberespaço, como sejam a Estratégia Nacional de Segurança do Ciberespaço, o Plano Nacional de resposta a crises e incidentes de cibersegurança em grande escala, o Quadro Nacional de Referência para a Cibersegurança, a Estratégia Nacional de Ciberdefesa e o Conceito Estratégico de Defesa Nacional;
- Regulação do *ethical hacking*, mais concretamente, a atividade destinada a conhecer as vulnerabilidades inerentes aos sistemas das empresas, para efeitos de reporte;
- Reforço da supervisão, com o Centro Nacional de Cibersegurança a alcançar o estatuto de autoridade nacional de cibersegurança;
- Cooperação das entidades integrantes do quadro institucional da segurança do

ciberespaço, com o setor privado, para efeitos de partilha de informação, adoção de boas práticas, desenvolvimento e/ou melhoria de sistemas de classificação quanto a medidas de gestão dos riscos de cibersegurança, indicadores de exposição a riscos ou ciberameaças, procedimentos de tratamento de incidentes, gestão de crises e divulgação de vulnerabilidades;

- Dever de elaboração de um relatório anual por parte das entidades essenciais e importantes, que apresente, de forma sintética, as principais atividades desenvolvidas em matéria de segurança das redes e sistemas de informação, incluindo estatísticas trimestrais de incidentes e uma análise agregada dos incidentes significativos — abrangendo utilizadores afetados, duração, distribuição geográfica e eventual impacto transfronteiriço;
- Notificação obrigatória de qualquer incidente significativo, por parte das entidades essenciais, importantes e públicas, à autoridade de cibersegurança competente;
- Previsão de contraordenações muito graves, graves e leves, perante o incumprimento de determinadas disposições previstas no Decreto-Lei.

ENTRADA EM VIGOR

O presente decreto-lei entra em vigor 120 dias após a sua publicação.

Inês Ferreira Lourenço
ines.fl@caldeirapires.pt
.