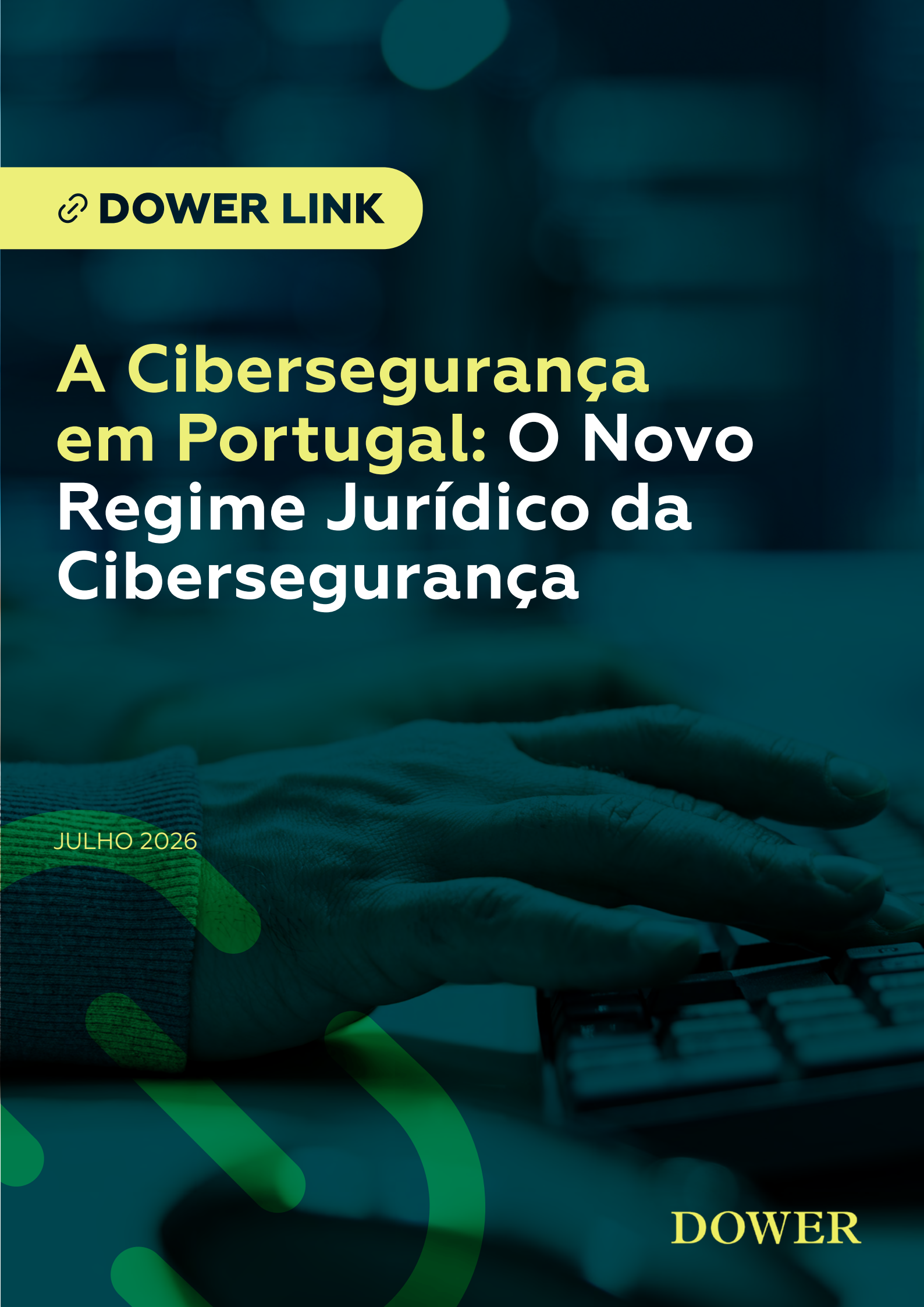
DOWER LINK

A Cibersegurança em Portugal: O Novo Regime Jurídico da Cibersegurança



JULHO 2026

DOWER

Entrou em vigor, no passado mês de abril, o Decreto-Lei n.º 125/2025, que transpõe a Diretiva NIS2 para Portugal e estabelece o novo Regime Jurídico da Cibersegurança.

A Diretiva NIS2 surge para reforçar a cibersegurança na União Europeia.

Os seus principais objetivos são:

i. Aumentar a resiliência digital das organizações;
ii. Harmonizar regras entre Estados-Membros;
iii. Reforçar a resposta a incidentes de cibersegurança.

Quem fica abrangido pelo RJC?

Entidades essenciais: Entidades que operam em setores de elevada criticidade para a sociedade e para a economia, como a energia, os transportes, a saúde, as infraestruturas digitais, as comunicações eletrónicas, a banca e determinados serviços financeiros, entre outros previstos na lei.

Entidades importantes: Entidades abrangidas pelo RJC que não sejam classificadas como essenciais. A respetiva classificação depende da atividade desenvolvida em setores críticos, da dimensão da entidade e demais critérios legalmente previstos.

Entidades públicas relevantes: Entidades que, não se enquadrando como essenciais ou importantes, preenchem os pressupostos específicos previstos no RJC, tendo em conta, designadamente, o âmbito das funções que exercem ou a sua dimensão.

Embora o regime se aplique, em regra, **a médias e grandes empresas**, pode também abranger **entidades de menor dimensão quando preencham critérios específicos** previstos na lei, atendendo, designadamente, à natureza crítica ou à relevância dos serviços prestados.

Mas, afinal, o que muda para as organizações?

1. Novas responsabilidades para a gestão

Os órgãos de topo passam a ter um papel ativo na cibersegurança. Devem:

i. Aprovar medidas de gestão de riscos;
ii. Supervisionar a sua implementação;
iii. Garantir formação adequada;
iv. Assegurar o cumprimento das obrigações legais.

2. Gestão de riscos não é opcional

As entidades essenciais e importantes devem implementar medidas de cibersegurança, relacionadas com diversas áreas, entre as quais:

i. Tratamento de incidentes;
ii. Continuidade de atividades;
iii. Segurança da cadeia de abastecimento;
iv. Práticas básicas de ciber-higiene e formação em cibersegurança;
v. Segurança dos recursos humanos;
vi. Entre outras.

As entidades públicas relevantes devem adotar as medidas de cibersegurança estabelecidas pelo CNCS no Regulamento n.º 756/2026, de 22 de junho.

3. Responsável de Cibersegurança

As entidades essenciais e importantes devem assegurar a existência de um responsável pela cibersegurança, que terá como funções, entre outras:

i. Propor medidas de gestão de riscos de cibersegurança;
ii. Prestar informação sobre as medidas de gestão de riscos de cibersegurança;
iii. Auxiliar no cumprimento das medidas de supervisão e execução;

iv. Promover uma cultura de cibersegurança;
v. Gerir risco residual;
vi. Garantir a elaboração do relatório anual;
vii. Coordenar as ações do ponto de contacto permanente.

4. Notificação de incidentes

As entidades abrangidas devem comunicar à autoridade de cibersegurança competente os incidentes significativos.

O regime prevê:

i. Notificação inicial;
ii. Relatórios intercalares, quando aplicável;
iii. Notificação do fim do impacto significativo;
iv. Relatório final.

E se houver incumprimento?

O novo regime prevê coimas que podem atingir:

- **10 milhões de euros** ou **2% do volume de negócios anual mundial**, quando superior, para as pessoas coletivas;
- **200 mil euros** para as pessoas singulares.

Podem ainda ser aplicadas:

i. **Sanções acessórias**, incluindo restrições à atividade e implementação de planos em matéria de cibersegurança; e
ii. **Sanções pecuniárias compulsórias**.

O Decreto-Lei encontra-se em vigor desde 3 de abril de 2026.

Até 3 de abril de 2027, as entidades abrangidas pelo RJC podem, mediante pedido fundamentado, solicitar a dispensa de coimas aplicadas.

A 23 de junho de 2026 entrou em vigor o Regulamento n.º 756/2026 que vem concretizar a aplicação prática do Regime Jurídico da Cibersegurança, em domínios como notificação de incidentes e comunicação com a autoridade de cibersegurança competente.

A sua organização está preparada?

A identificação atempada das obrigações aplicáveis e a preparação da organização são essenciais para assegurar a conformidade e reforçar a resiliência digital.

Equipa de Privacidade e Compliance
dower@dower.pt