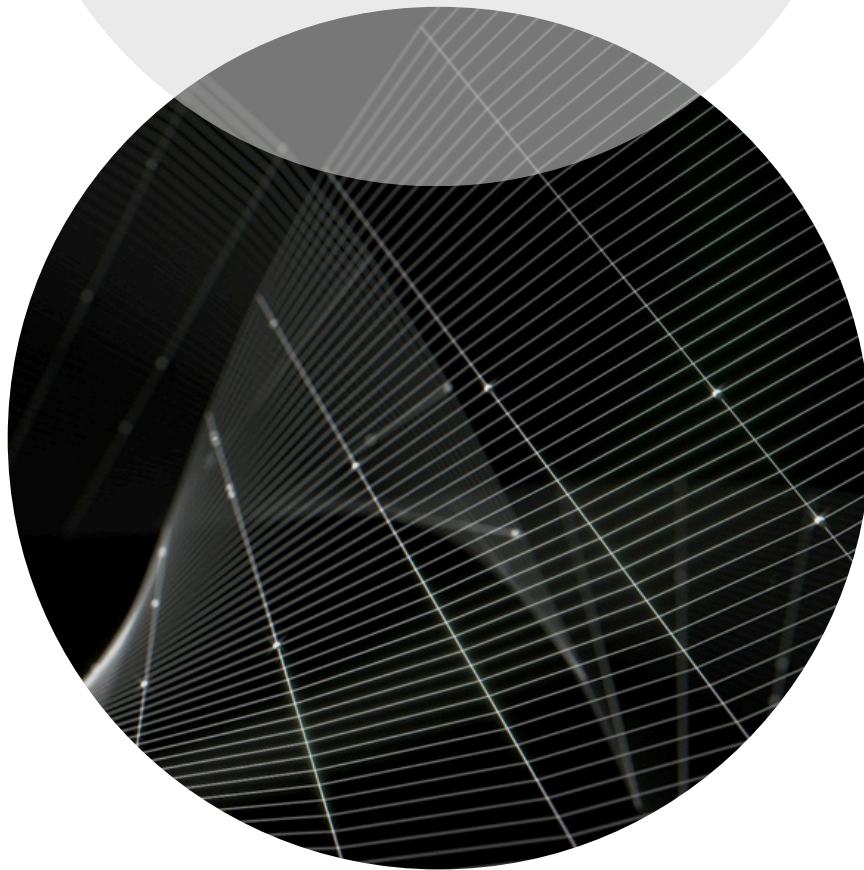


Avaliação Nacional de Risco e Estratégia Nacional para a Resiliência das Entidades Críticas

info@abreuadvogados.com
abreuadvogados.com



No passado dia 26 de junho de 2026 foi publicada, em Diário da República, a Resolução do Conselho de Ministros n.º 135/2026, que aprova a Avaliação Nacional de Risco e a Estratégia Nacional para a Resiliência das Entidades Críticas (“a Estratégia”). Estes instrumentos consubstanciam um passo essencial para a implementação coerente e eficaz do quadro jurídico nacional da resiliência das entidades e infraestruturas críticas, definido no Decreto-Lei n.º 22/2025, de 19 de março (o “Decreto-Lei”), que transpôs para a ordem jurídica interna a Diretiva (UE) 2022/2557, de 14 de dezembro.

Conforme previsto no Decreto-Lei, a Avaliação Nacional de Risco é classificada como “Reservada”, estando o seu acesso e análise condicionado. Por sua vez, a Estratégia é um documento público que define as medidas de política, os objetivos estratégicos e as linhas de ação para reforçar a resiliência das entidades críticas. A sua implementação é acompanhada por um Plano de Ação, que monitoriza e avalia a execução da Estratégia para o período de 2026-2029.

Antecipa-se que a aprovação e publicação destes instrumentos desencadeie o processo de designação das entidades críticas e respetivas infraestruturas críticas, as quais ficaram sujeitas ao cumprimento do Decreto-lei, bem como do Regime Jurídico de Cibersegurança, definido no Decreto-lei n.º 125/2025, de 4 de dezembro.

A) Enquadramento Estratégico

O Decreto-Lei estabelece o regime jurídico nacional em matéria de resiliência das entidades críticas, abrangendo os setores da energia, transportes, bancário, infraestruturas do mercado financeiro, saúde, água potável, águas residuais, infraestruturas digitais, Administração Pública, espaço, produção, transformação e distribuição de produtos alimentares, e seguros e fundos de pensões. A Estratégia surge como o instrumento político de enquadramento e operacionalização das obrigações nele previstas.

A Estratégia integra, assim, os seguintes elementos estruturantes:

- Objetivos estratégicos no intuito de reforçar a resiliência global das entidades críticas;
- Quadro de governação com descrição das funções e responsabilidades das entidades competentes, das entidades setoriais, das entidades críticas e de outras partes relevantes;
- Descrição das medidas de resiliência a implementar;
- Processo de identificação e designação das entidades críticas e respetivas infraestruturas;
- Medidas de coordenação com as autoridades competentes em matéria de cibersegurança;
- Medidas de apoio às entidades críticas, nomeadamente às que sejam pequenas e médias empresas.

B) Eixos de Intervenção e Objetivos Estratégicos

Os objetivos estratégicos decorrem da análise do contexto nacional e internacional e estão agrupados em três eixos de intervenção:

- Eixo I – Reforço da Resiliência das Entidades Críticas: engloba os objetivos relativos à identificação e designação criteriosa das entidades e infraestruturas críticas, à avaliação sistemática de riscos e à adoção de medidas de resiliência adequadas e proporcionais;
- Eixo II – Cooperação, Supervisão e Coordenação Institucional: visa reforçar a cooperação nacional e internacional;
- Eixo III – Investigação, Formação, Comunicação e Cultura de Resiliência: centra-se no reforço de capacidades técnicas e operacionais das entidades críticas, na realização de exercícios e na promoção de uma cultura nacional de resiliência.

C) Medidas de Resiliência: Identificação e Designação de Entidades e Infraestruturas Críticas

Uma das medidas centrais do Eixo I será a aprovação, pelo Conselho Nacional de Planeamento Civil de Emergência (“CNPCE”), dos critérios e metodologia aplicáveis para identificar e designar as entidades críticas e respetivas infraestruturas críticas.

D) Processo de Designação das Entidades Críticas

O processo de designação articula-se nas seguintes fases sequenciais:

- Proposta das entidades setoriais: as entidades setoriais submetem ao CNPCE uma proposta com a densificação dos critérios de identificação e os limiares aplicáveis, identificando as entidades candidatas à designação;
- Notificação das entidades candidatas: o CNPCE notifica as entidades candidatas da sua possível designação, concedendo-lhes um prazo não inferior a 10 dias para apresentarem pronúncia;
- Análise das pronúncias: em caso de pronúncia desfavorável, o CNPCE remete-a à entidade setorial, que dispõe de 60 dias para reanalisar e, se necessário, adequar a proposta;
- Designação formal pelo CNPCE: concluído o procedimento, o CNPCE designa formalmente as entidades críticas e respetivas infraestruturas críticas, no prazo máximo de 30 dias;
- Notificação da designação: a entidade crítica é formalmente notificada no prazo máximo de 10 dias.

E) Obrigações das Entidades Críticas

Após a notificação da sua designação, as entidades críticas ficam sujeitas a um conjunto de obrigações nos termos do Decreto-Lei que se sistematizam no quadro seguinte:

Obrigação	Prazo
Avaliação de risco	9 meses após notificação da designação
Plano de resiliência	10 meses após notificação; revisto de 4 em 4 anos
Agentes de ligação	10 dias após a designação como entidade crítica
Auto-identificação como entidade essencial na Plataforma MyCiber	30 dias após designação caso a entidade não estivesse já abrangida pelo Decreto-lei n.º 125/2025, de 4 de dezembro – Sem prejuízo de futuras orientações das autoridades competentes

F) Plano de Ação

O Plano de Ação compreende 42 medidas distribuídas pelos três eixos de intervenção, com início previsto para janeiro de 2026 e prazo de implementação que se estende, na maioria dos casos, até dezembro de 2029.

Merecem destaque as seguintes medidas:

- Densificação dos critérios de identificação pelas entidades setoriais, cujo prazo de implementação se estende até julho de 2026;
- Aprovação dos critérios e metodologia de identificação e designação das entidades críticas e respetivas infraestruturas críticas pelo CNPCE, com prazo de implementação igualmente até julho de 2026;
- O Plano de Ação prevê ainda o desenvolvimento de uma plataforma digital comum de notificação de incidentes, a implementar conjuntamente pelo Secretário-Geral do Sistema de Segurança Interna e pelas autoridades competentes em matéria de cibersegurança. Esta plataforma abrangerá tanto os incidentes relativos à resiliência das entidades críticas como os incidentes no âmbito do Regime Jurídico da Cibersegurança, estabelecido pelo Decreto-lei n.º 125/2025, de 4 de dezembro.

G) Próximos Passos

A aprovação da Avaliação Nacional de Risco e da Estratégia Nacional para a Resiliência das Entidades Críticas marca o início da fase operacional do regime jurídico de resiliência das entidades críticas, antecipando-se a designação destas entidades e respetivas infraestruturas críticas para a segunda metade do ano de 2026.

Para mais informações, contacte o nosso Serviço de Proteção de Dados e Cibersegurança.

Thinking about tomorrow? Let's talk today.



Ricardo Henriques

ricardo.henriques@abreuadvogados.com



Catarina Rodrigues Rocha

catarina.r.rocha@abreuadvogados.com

info@abreuadvogados.com
abreuadvogados.com

Abreu:
advogados