Radar NIS 2

Consulta Pública do Centro Nacional de Cibersegurança

abreuadvogados.com

O Centro Nacional de Cibersegurança (CNCS) lançou para consulta pública, até 22 de abril de 2026, um projeto de Regulamento do Regime Jurídico de Cibersegurança ("**Projeto de Regulamento**"). Este Projeto desenvolve e densifica o Decreto-Lei n.º 125/2025, de 4 de dezembro, que transpõe a Diretiva NIS2 para o direito nacional.

1. **Plataforma Eletrónica**

Todas as entidades abrangidas devem registar-se e interagir com a autoridade competente através de uma plataforma eletrónica centralizada. Através desta plataforma, as entidades deverão: (i) proceder à autoidentificação, qualificação e registo; (ii) designar um Responsável pela Cibersegurança e um Ponto de Contacto Permanente; (iii) submeter relatórios anuais; e (iv) notificar incidentes de cibersegurança. A autenticação exige identificação eletrónica portuguesa de nível elevado, nomeadamente Cartão de Cidadão ou Chave Móvel Digital. As notificações oficiais consideram-se recebidas no terceiro dia após o envio para a área reservada.

2. **Matriz de Risco e Níveis de Conformidade**

O Projeto estabelece um quadro referencial com valores de risco para cenários que recaem sobre cada setor e subsetor de atividade. Este modelo conduz a um sistema de classificação de conformidade em três níveis: Básico, Substancial e Elevado. Os níveis são cumulativos: uma entidade no nível Substancial deve implementar todas as medidas Básicas mais as Substanciais adicionais, enquanto uma entidade no nível Elevado deve implementar medidas nos três níveis. Esta abordagem proporcional garante que as obrigações são calibradas para refletir o perfil de risco inerente ao setor da entidade, a sua dimensão e importância sistémica.

3. **Medidas Mínimas de Cibersegurança**

As medidas mínimas aplicam-se às entidades essenciais e importantes consoante os três níveis de conformidade, e às entidades públicas relevantes consoante a sua qualificação como A ou B. As medidas abrangem as seguintes áreas: identificação de serviços críticos; processos de gestão de risco; inventário de ativos; plano de resposta a incidentes e recuperação; tratamento de incidentes e continuidade das atividades; segurança da cadeia de abastecimento; aquisição, desenvolvimento e manutenção das redes e sistemas; práticas de ciber-higiene e formação; políticas de criptografia e autenticação multifator; e gestão de ativos e controlo de acessos.

4. **Procedimentos de Notificação de Incidentes**

As organizações devem notificar incidentes significativos através da Plataforma Eletrónica, cumprindo as seguintes fases: (i) notificação inicial imediatamente após deteção; (ii) comunicação da cessação do impacto significativo; e (iii) relatórios finais ou intercalares após a resolução do incidente.

5 **Certificação Voluntária**

O Projeto prevê uma presunção de conformidade para organizações titulares de certificados válidos ao abrigo de: QNRCS Certification Scheme; ISO/IEC 27001; DNP TS 4577-1 (Digital

Maturity Seal) para entidades públicas; e outros esquemas aprovados pelo CNCS. As alterações ao estado do certificado (revogação, suspensão ou caducidade) devem ser comunicadas no prazo de 20 dias úteis.

6. **Lista de Ativos Publicamente Acessíveis**

As entidades essenciais, importantes e públicas relevantes devem elaborar, manter atualizada e comunicar à autoridade competente uma lista de todos os ativos essenciais para a prestação dos respetivos serviços que estejam diretamente acessíveis através da Internet.

7. **Datas e Próximos Passos**

Marco	**Data**
Período de consulta pública	Até 22 de abril de 2026
Entrada em vigor	5.º dia após publicação em Diário da República

A Equipa da Abreu Advogados está disponível para apoiar na análise e aplicação destas matérias, nomeadamente prestando assistência no âmbito do processo de consulta pública.

Thinking about tomorrow? Let's talk today.

Ricardo Henriques – Sócio
ricardo.henriques@abreuadvogados.com

Catarina Mascarenhas – Consultora
catarina.mascarenhas@abreuadvogados.com

Marta Boura – Consultora
marta.boura@abreuadvogados.com