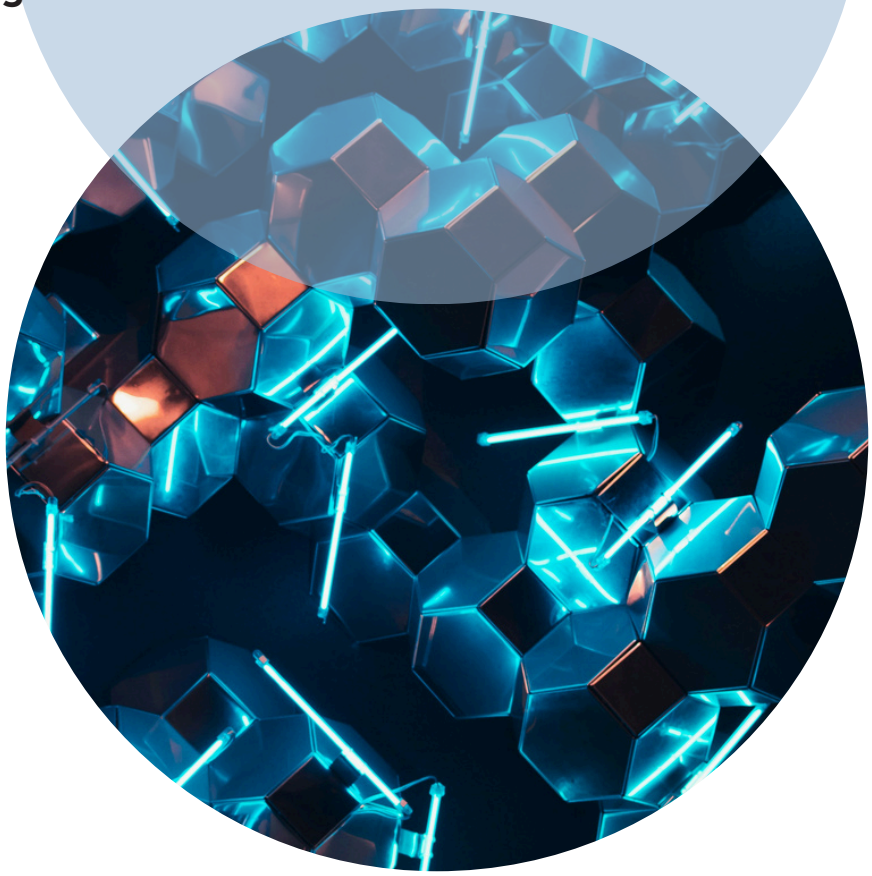
Regulamento de Execução do Regime Jurídico da Cibersegurança

info@abreuadvogados.com
abreuadvogados.com



No dia 22 de junho de 2026 foi publicado o Regulamento n.º 756/2026, que concretiza a aplicação do Regime Jurídico da Cibersegurança ("RJC"), aprovado pelo Decreto-Lei n.º 125/2025, de 4 de dezembro, estabelecendo regras operacionais essenciais para as entidades essenciais, entidades importantes e entidades públicas relevantes.

O Regulamento define, entre outras matérias, o funcionamento da nova plataforma eletrónica do Centro Nacional de Cibersegurança ("CNCS"), os procedimentos de autoidentificação e qualificação das entidades abrangidas, as regras de notificação de incidentes de cibersegurança e os instrumentos estruturantes que servirão de referência para a implementação das obrigações previstas no RJC.

A) Plataforma MyCiber e Qualificação das Entidades

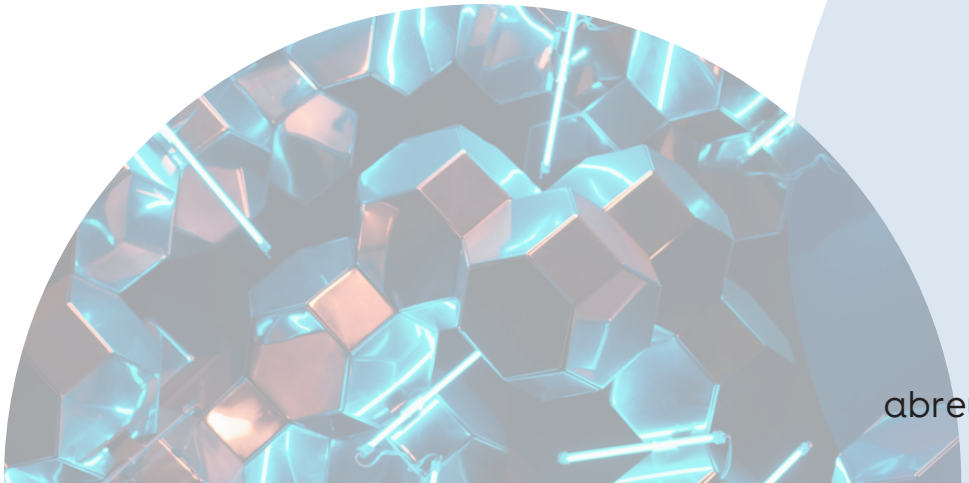
Uma das principais novidades do Regulamento consiste na operacionalização da plataforma eletrónica do CNCS, já disponível com a funcionalidade de simulação – MyCiber –, que passa a constituir o canal privilegiado de interação entre as entidades abrangidas e a autoridade de cibersegurança competente.
A plataforma assegurará, designadamente:

- A autoidentificação das entidades abrangidas;
- O procedimento de qualificação das entidades como essenciais, importantes ou públicas relevantes;
- A comunicação do Responsável de Cibersegurança e do Ponto de Contacto Permanente;
- A submissão de notificações obrigatórias e voluntárias;
- A receção de notificações eletrónicas do CNCS;
- A entrega de relatórios e demais elementos exigidos no âmbito dos poderes de supervisão.

Procedimento de Autoidentificação e Qualificação

O processo inicia-se através do preenchimento de formulário eletrónico na plataforma MyCiber, do qual resultará um registo provisório. Após análise pelo CNCS, será desencadeado o procedimento de qualificação da entidade.

Na sequência do processo de consulta pública, foi consagrado o direito de audiência prévia das entidades visadas, exercido mediante notificação pelo CNCS, que dispõem de um prazo de 10 dias úteis para se pronunciarem sobre o projeto de decisão. Decorrido esse prazo, o CNCS proferirá a decisão final de qualificação, da qual constará, quando aplicável:



- A categoria da entidade;
- O nível de conformidade aplicáve
- As medidas de cibersegurança obrigatórias a implementar.

Após a qualificação, o registo provisório converte-se em registo definitivo, passando a entidade a estar sujeita às obrigações permanentes previstas no RJC e no Regulamento.

B) Responsável de Cibersegurança e Ponto de Contacto Permanente

O Regulamento concretiza igualmente os requisitos relativos à designação e comunicação do Responsável de Cibersegurança e do Ponto de Contacto Permanente, que deverão ser comunicados através da área reservada da plataforma MyCiber.

C) Notificação de Incidentes

A Plataforma será igualmente o ponto central para a submissão das notificações obrigatórias de incidentes com impacto significativo.

As entidades abrangidas deverão apresentar:

- Notificação inicial;
- Notificação de fim do impacto significativo;
- Relatório final ou intercalar.

A plataforma permitirá acompanhar o estado das notificações, associar diferentes comunicações relativas ao mesmo incidente e receber alertas automáticos relativos aos prazos legais de reporte.

O Regulamento prevê ainda a possibilidade de apresentação de notificações voluntárias relativas a incidentes, ciberameaças, vulnerabilidades ou quase-incidentes, mesmo por entidades ou pessoas não registadas na plataforma.

De acordo com a redação final do Regulamento, será divulgada na Plataforma informação relativa à ocorrência de incidentes significativos.

D) Instrumentos Estruturantes

O Regulamento aprova um conjunto de instrumentos fundamentais para a implementação do novo quadro regulatório de cibersegurança.

i. Quadro Nacional de Referência para a Cibersegurança (QNRCS)

O QNRCS passa a constituir o instrumento nacional de referência para identificação de normas, padrões e boas práticas em matéria de gestão da cibersegurança e segurança da informação.

ii. Matriz de Risco

A Matriz de Risco estabelece os cenários de risco aplicáveis aos diferentes setores e subsetores de atividade e determina os respetivos níveis de conformidade:

- Básico;
- Substancial;
- Elevado.

A classificação obtida influenciará diretamente as obrigações de cibersegurança aplicáveis a cada entidade.

iii. Medidas de Cibersegurança Mínimas

Os Anexos III e IV estabelecem os conjuntos de medidas mínimas de cibersegurança aplicáveis:

- Às entidades essenciais e importantes;
- Às entidades públicas relevantes.

Estas medidas passam a constituir o referencial mínimo obrigatório para efeitos de conformidade com o RJC.

Próximos Passos

A entrada em vigor do Regulamento no dia 23 de junho marca o início da fase operacional do novo Regime Jurídico da Cibersegurança.

As entidades potencialmente abrangidas deverão, desde já:

- Avaliar se se encontram no âmbito subjetivo do RJC;
- Preparar a respetiva autoidentificação na plataforma MyCiber;
- Rever os mecanismos de governação da cibersegurança;
- Designar o Responsável de Cibersegurança e o Ponto de Contacto Permanente;
- Avaliar o respetivo nível de conformidade e as medidas de cibersegurança aplicáveis;
- Preparar os processos internos de gestão e reporte de incidentes.

A implementação atempada destas medidas será determinante para assegurar o cumprimento das novas obrigações regulatórias e reduzir o risco de supervisão e de responsabilidade contraordenacional.

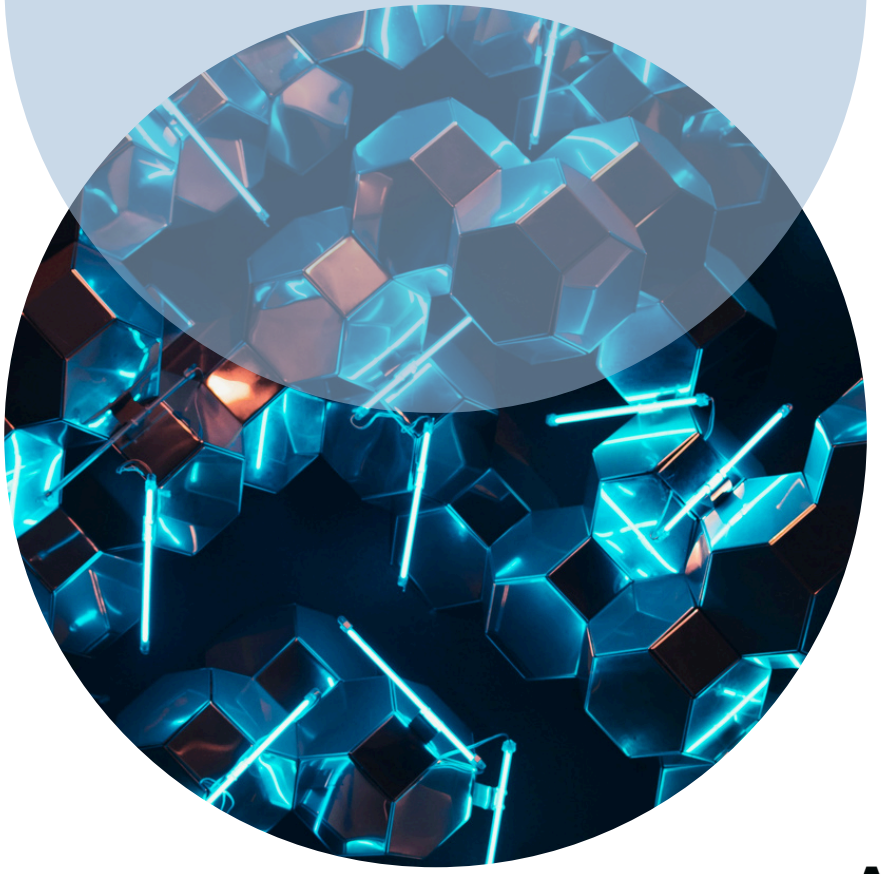
Para mais informações, contacte o nosso Serviço de Proteção de Dados e Cibersegurança.

Thinking about tomorrow? Let's talk today.

Ricardo Henriques
ricardo.henriques@abreuadvogados.com

Catarina Mascarenhas
catarina.mascarenhas@abreuadvogados.com

Marta Boura
marta.boura@abreuadvogados.com



info@abreuadvogados.com
abreuadvogados.com

Abreu advogados