JUN. 26

NOTA INFORMATIVA

TECNOLOGIA, MEDIA E TELECOMUNICAÇÕES

Regulamento do Regime Jurídico da Cibersegurança

Enquadramento

Foi publicado no Diário da República o "Regulamento do Regime Jurídico da Cibersegurança" (Regulamento n.º 756/2026, de 22 de junho de 2026 – o "Regulamento"), que concretiza as matérias do Regime Jurídico da Cibersegurança (Decreto-Lei n.º 125/2025, de 4 de dezembro – "RJC[1]") cometidas ao Centro Nacional de Cibersegurança ("CNCS").

O projeto de Regulamento havia sido previamente submetido a consulta pública entre março e abril, da qual resultaram dezenas de contribuições, algumas delas integradas na versão final.

Âmbito de Aplicação

O Regulamento aplica-se às entidades essenciais, importantes e públicas relevantes, nos termos do RJC, e disciplina, designadamente:

O Regulamento aplica-se às entidades essenciais, importantes e públicas relevantes, nos termos do RJC.

- O funcionamento da plataforma eletrónica, nomeadamente quanto ao procedimento de auto-identificação e qualificação das entidades;
- As notificações obrigatórias de incidentes de cibersegurança e as notificações voluntárias de informações pertinentes;
- As comunicações entre entidades e a autoridade de cibersegurança competente;
- O Quadro Nacional de Referência de Cibersegurança (QNRCS);
- A produção da Matriz de Risco;
- A gestão do risco residual;

Pedro Lomba
Marta Salgado Areias
Mafalda de Brito Fernandes
Equipa de Tecnologia, Media e Telecomunicações

1 Diploma que transpôs para o ordenamento jurídico português a Diretiva (UE) 2022/2555 ("Diretiva NIS 2"),

- Os níveis de conformidade e medidas de cibersegurança mínimas obrigatórias para as entidades abrangidas;
- As regras relativas à comunicação do responsável de cibersegurança e do ponto de contacto permanente;
- As matérias cuja aplicação dependa de instruções técnicas ou de outros normativos da autoridade de cibersegurança competente, incluindo critérios técnicos e mecanismos operacionais relativos à plataforma e às notificações.

Plataforma eletrónica "MyCiber"

A plataforma eletrónica "MyCiber", desenvolvida e gerida pelo CNCS e disponível em myciber.gov.pt, centraliza o registo, a qualificação, as comunicações obrigatórias, a notificação de incidentes e a divulgação de informação pelas autoridades competentes.

Aplica-se o princípio da declaração única, com dispensa de informação já disponível, conta única por entidade, área reservada, recibos de entrega e autenticação por Cartão de Cidadão, Chave Móvel Digital ou mecanismos equivalentes, incluindo meios emitidos noutros Estados-Membros da UE. As notificações são feitas para a área reservada, com alerta por email, sem prejuízo do envio postal de citações e decisões finais contraordenacionais; está ainda disponível um simulador indicativo, sem efeito vinculativo para o CNCS.

Auto-identificação e qualificação

O registo deve ser feito no prazo de 60 dias após a disponibilização da plataforma, para entidades já em atividade, ou em 30 dias após o início de atividade.

As entidades sujeitas ao RJC devem identificar-se na plataforma mediante o preenchimento de um formulário eletrónico, do qual devem constar dados como o nome, o NIF, o(s) setor(es) e subsetor(es) de atividade, o tipo de entidade, o endereço e os dados de contacto atualizados, o número de trabalhadores e o CNCS, em conjunto com a autoridade setorial competente, quando aplicável, determina se a entidade está abrangida pelo RJC. A entidade dispõe de 10 dias úteis para se pronunciar; na ausência de pronúncia, é emitido o Ato de Qualificação, a partir do qual se aplicam as obrigações do RJC, sem prejuízo dos meios impugnatórios previstos no Código do Procedimento Administrativo.

O registo deve ser feito no prazo de 60 dias após a disponibilização da plataforma, para entidades já em atividade, ou em 30 dias após o início de atividade, sob pena de sanções contraordenacionais. Os dados e informações submetidos na plataforma são da responsabilidade de cada entidade, que deve mantê-los permanentemente atualizados.

A qualificação pode ser alterada a qualquer momento pela autoridade competente, em função de alteração das circunstâncias.

A comunicação do responsável de cibersegurança e do ponto de contacto permanente deve ser feita mediante formulário disponível na área reservada da plataforma eletrónica.

Quando se conclua que a entidade não está abrangida pelo RJC, o registo provisório é cancelado no prazo máximo de 90 dias. A autoridade de cibersegurança competente mantém, contudo, a conservação do formulário de auto-identificação e da respetiva notificação de exclusão, por outros meios e pelo período que considere necessário.

Entidades Financeiras

As entidades financeiras abrangidas simultaneamente pelo RJC, pelo Regulamento (UE) 2022/2554 (DORA) e pela Lei n.º 73/2025, de 23 de dezembro, realizam, após registo e qualificação, as comunicações e notificações de resiliência operacional digital junto das autoridades previstas na legislação especial aplicável. Devem, no entanto, assegurar as obrigações do RJC em matéria de designação do responsável de cibersegurança, ponto de contacto permanente e notificação de incidentes.

Comunicação de documentos

As entidades essenciais devem comunicar anualmente à autoridade de cibersegurança competente, por meio da sua área reservada na plataforma eletrónica, o relatório anual previsto no artigo 30.º do RJC. As entidades importantes, por sua vez, remetem o relatório anual ao CNCS sempre que este lhes seja solicitado.

Responsável de cibersegurança e ponto de contacto permanente

A comunicação do responsável de cibersegurança e do ponto de contacto permanente deve ser feita mediante formulário disponível na área reservada da plataforma eletrónica. Para as entidades já existentes à data de entrada em vigor do RJC, o prazo de 20 dias úteis conta-se a partir da notificação da qualificação da entidade.

Notificação obrigatória de incidentes

As notificações obrigatórias de incidentes previstas nos artigos 40.º a 44.º do RJC são submetidas por formulário na área reservada, com alertas automatizados sobre prazos. O impacto significativo é definido pelo Regulamento de Execução (UE) n.º 2024/2690 para as entidades aí previstas e por instrução técnica do CNCS para as restantes. Admite-se ainda a submissão de notificações voluntárias de incidentes, ciberameaças, quase incidentes ou vulnerabilidades, sem autenticação na plataforma.

Quadro Nacional de Referência de Cibersegurança (QNRCS)

O QNRCS, constante do Anexo I, é o instrumento nacional de referência para normas, padrões e boas práticas de gestão da cibersegurança, estruturado em objetivos, categorias e controlos. Deve ser aplicado numa perspetiva de melhoria contínua, é atualizado pelo CNCS pelo menos de cinco em cinco anos e a sua utilização facultativa deve ser conjugada com as medidas mínimas do Anexo III.

Certificação Voluntária

As entidades essenciais, importantes e públicas relevantes podem beneficiar de uma presunção de cumprimento das medidas de cibersegurança mediante certificado emitido por organismo acreditado, incluindo EC QNRCS, ISO/IEC 27001 com âmbito integral sobre os sistemas relevantes ou outro esquema aprovado. Alterações ao certificado devem ser comunicadas em 72 horas, em caso de revogação, ou em 10 dias úteis nas restantes situações. A autoridade competente pode ainda exigir certificação nacional, europeia ou internacional em casos fundamentados.

Níveis de conformidade e medidas de cibersegurança mínimas

O Regulamento estabelece três níveis de conformidade – básico, substancial e elevado – resultantes da Matriz de Risco (Anexo II), que considera o setor, dimensão e risco associado. As entidades abrangidas devem aplicar, pelo menos, as medidas mínimas dos Anexos III e IV, incluindo as dos níveis inferiores quando sujeitas aos níveis substancial ou elevado; em caso de sobreposição, aplica-se o nível mais exigente. As medidas abrangem, entre outros domínios, ativos, identidades e acessos, dados, infraestrutura tecnológica, monitorização, incidentes, formação e cadeia de abastecimento.

A análise de riscos deve ser realizada pelo menos anualmente ou após notificação do CNCS relativa a uma ameaça ou vulnerabilidade emergente.

Gestão de Riscos

A análise de riscos deve ser realizada pelo menos anualmente ou após notificação do CNCS relativa a uma ameaça ou vulnerabilidade emergente, considerando histórico de incidentes, utilizadores afetados, duração, distribuição geográfica e dependências intersectoriais. As entidades devem comunicar a lista inicial de ativos publicamente acessíveis relevantes até 31 de janeiro do ano seguinte à notificação de qualificação ou no prazo de seis meses após essa notificação, consoante o que se vencer primeiro, e atualizá-la anualmente, tratando-a como informação sensível.

Entrada em vigor e produção de efeitos

O Regulamento entrou em vigor em 23 de junho de 2026, produzindo efeitos imediatos quanto às disposições que não constem do regime transitório específico e que não dependam de instruções técnicas ou atos complementares, incluindo as regras de funcionamento da plataforma eletrónica, de auto-identificação, qualificação e comunicações com a autoridade de cibersegurança competente, na medida em que sejam imediatamente operacionalizáveis.

PLMJ

Quanto ao regime transitório de 24 meses previsto pelo RJC, ficam abrangidas por este período, em especial, as seguintes obrigações e anexos:

- A implementação das medidas de cibersegurança mínimas previstas no Anexo III (entidades essenciais e importantes, nos níveis básico, substancial e elevado) e no Anexo IV (entidades públicas relevantes, Grupos A e B), ao abrigo dos artigos 26.º e 33.º do RJC.

- A aplicação da Matriz de Risco constante do Anexo II, enquanto instrumento de determinação dos níveis de conformidade aplicáveis às entidades essenciais e importantes.

- As obrigações de análise e gestão periódica dos riscos e riscos residuais, incluindo a realização de análises de risco com periodicidade mínima anual e a análise do risco residual após a adoção das medidas de cibersegurança.

- A notificação obrigatória de incidentes com impacto significativo, incluindo a notificação inicial, a notificação de fim do impacto significativo e o relatório final ou intercalar, sem prejuízo de eventuais obrigações que já resultem diretamente do RJC ou de regulamentação europeia aplicável.

- A comunicação da lista de ativos publicamente acessíveis e respetiva atualização periódica, na medida em que a obrigação dependa da qualificação da entidade e da operacionalização dos mecanismos regulamentares aplicáveis.

Ações Recomendadas

Recomenda-se que as entidades potencialmente abrangidas adotem, em especial, as seguintes medidas:

- Confirmar o enquadramento no RJC e proceder à auto-identificação na MyCiber, reunindo a informação necessária ao formulário.

- Identificar as obrigações já exigíveis e as abrangidas pelo período transitório de 24 meses, incluindo os prazos associados à qualificação.

- Designar o responsável de cibersegurança e o ponto de contacto permanente, preparando a respetiva comunicação na plataforma.

- Realizar uma avaliação de lacunas (*gap analysis*) face às medidas mínimas aplicáveis e rever procedimentos de gestão e notificação de incidentes.

- Assegurar a conformidade em matéria de proteção de dados, ponderar certificação voluntária e monitorizar instruções técnicas, orientações ou outros normativos do CNCS. ■