Cerejeira Namora Marinho Falcão
an auren member firm

# Novo Regime Jurídico da Cibersegurança

Legal Update

Abril 2026

shaping the **future**

## 1. Enquadramento

O Decreto-Lei n.º 125/2025, de 4 de Dezembro, procede à transposição para a ordem jurídica portuguesa da Directiva (UE) 2022/2555, do Parlamento Europeu e do Conselho, de 14 de Dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de Cibersegurança na União (NIS2), aprovando o Regime Jurídico da Cibersegurança (RJC).

Importa, desde logo, notar que o RJC vem substituir o regime anteriormente aplicável em matéria de segurança do ciberespaço, aprovado pela Lei n.º 46/2018, de 13 de Agosto, que transpôs a Directiva (UE) 2016/1148 (NIS1), bem como a regulamentação constante do Decreto-Lei n.º 65/2021, de 30 de Julho.

O novo regime reforça significativamente os mecanismos de prevenção, gestão de riscos e responsabilização em matéria de cibersegurança, ampliando de forma substancial o universo de entidades abrangidas e reforçando as competências do Centro Nacional de Cibersegurança (CNCS).

## 2. Âmbito de aplicação

O regime aplica-se, em regra, a entidades públicas ou privadas que, cumulativamente:

**i.** integrem um dos tipos previstos nos Anexos I ou II do diploma

**ii.** prestem serviços ou exerçam actividade na União Europeia, e

**iii.** satisfaçam os critérios de dimensão previstos para médias ou grandes empresas, sem prejuízo das situações em que o legislador afasta expressamente esse critério

Para efeitos de delimitação do âmbito sectorial, o Anexo I do RJC identifica os sectores de importância crítica, abrangendo, designadamente:

- energia
- transportes
- sector bancário
- infra-estruturas do mercado financeiro
- saúde
- água
- infra-estruturas digitais
- serviços de tecnologias de informação e comunicação

Por sua vez, o Anexo II enumera outros sectores críticos, incluindo, entre outros:

- serviços postais e de estafeta
- gestão de resíduos
- produção e distribuição de produtos químicos
- indústria alimentar
- indústria transformadora
- prestação de serviços digitais e investigação

A integração de uma entidade num dos sectores acima referidos constitui o primeiro pressuposto para a aplicação do RJC, sendo posteriormente necessário aferir a verificação dos critérios de dimensão ou, quando aplicável, a existência de circunstâncias especiais que determinem a aplicação do regime independentemente da dimensão.

A aplicação do regime depende, em regra, de a entidade se qualificar como **média ou grande empresa,** nos termos da Recomendação 2003/361/CE da Comissão. Com efeito, uma empresa será considerada média ou grande se empregar **mais de 250 trabalhadores** e apresentar um **volume de negócios** anual igual ou superior a **50 milhões de euros** ou um balanço total anual igual ou superior 43 milhões de euros.

### 2.1 Subqualificação das entidades abrangidas

No âmbito do modelo regulatório instituído pelo RJC, as entidades abrangidas são qualificadas como entidades essenciais, **entidades importantes** ou **entidades públicas relevantes,** sendo essa qualificação determinante para a definição do alcance das obrigações aplicáveis e do modelo de supervisão a que ficam sujeitas. O diploma consagra os seguintes critérios de subqualificação:

**a) Entidades essenciais**

São qualificadas como entidades essenciais as entidades que integrem os sectores constantes do Anexo I e que excedam os limiares previstos para as médias empresas.

Independentemente da dimensão, são também qualificadas como entidades essenciais:

» Os prestadores de serviços de confiança qualificados, os registos de nomes de domínio de topo e os prestadores de serviços de sistemas de nomes de domínio

» As empresas que ofereçam redes públicas de comunicações electrónicas ou serviços de comunicações electrónicas acessíveis ao público que sejam consideradas médias empresas

» As entidades da Administração Pública com atribuições na prestação de serviços nas áreas do desenvolvimento, manutenção e gestão de infra-estruturas de tecnologias de informação e comunicação, ou que apresentem um grau particularmente elevado de integração digital

» As entidades identificadas como críticas nos termos do Decreto-Lei n.º 22/2025, de 19 de Março, que transpõe a Directiva (UE) 2022/2557, relativa à resiliência das entidades críticas

» Qualquer outra entidade que seja qualificada como essencial pela autoridade competente, atendendo ao grau de exposição a riscos, à probabilidade de ocorrência de incidentes e à respectiva gravidade, incluindo o impacto socioeconómico

**b) Entidades importantes**

São qualificadas como entidades importantes as entidades que, não sendo consideradas entidades essenciais, correspondam a um dos tipos referidos nos Anexos I ou II.

Uma entidade poderá ainda ser qualificada como importante quando:

Seja o único prestador de um serviço essencial para a manutenção de actividades sociais ou económicas críticas;

» A perturbação dos serviços prestados seja susceptível de afectar significativamente a segurança pública, a saúde pública ou a continuidade de serviços essenciais

» A perturbação possa gerar riscos sistémicos relevantes, incluindo impactos transfronteiriços

» A entidade assuma particular importância para o sector em causa ou para sectores interdependentes

**c) Entidades públicas relevantes**

São entidades públicas relevantes as entidades públicas que, não sendo enquadradas como essenciais ou importantes, se integrem num dos dois grupos seguintes:

» Grupo A: entidades públicas de maior dimensão ou relevância institucional, abrangendo serviços da administração directa e indirecta do Estado com 250 ou mais trabalhadores, entidades públicas empresariais que excedam os limiares de médias empresas, entidades administrativas independentes e serviços de órgãos de soberania;

» Grupo B: entidades públicas de média dimensão, designadamente serviços da administração directa e indirecta do Estado com quadros de pessoal entre 50 e 249 trabalhadores, bem como entidades públicas empresariais qualificadas como médias empresas.

A **qualificação** numa destas três categorias é determinante, na medida em que define o alcance das obrigações aplicáveis e o regime de supervisão a que cada entidade fica adstrita.

## 3. Obrigações

Ainda que a intensidade da supervisão varie consoante a qualificação da entidade, a generalidade dos deveres de organização interna, gestão de riscos e notificação aplica-se tanto às entidades essenciais como às entidades importantes. Sem prejuízo das especificidades aplicáveis a cada categoria, destacam-se as seguintes obrigações transversais:

**a) Autoidentificação, qualificação e registo**

As entidades abrangidas pelo âmbito de aplicação do regime devem proceder à sua autoidentificação junto do CNCS, através da plataforma electrónica disponibilizada para o efeito.

No caso de entidades já em funcionamento à data da entrada em vigor do RJC, a autoidentificação deve ser efectuada no prazo de 60 dias a contar da disponibilização da plataforma electrónica.

Após a autoidentificação, cabe à autoridade competente proceder à qualificação da entidade como essencial, importante ou pública relevante, com base nos elementos fornecidos, na análise documental e, quando aplicável, na audição de autoridades sectoriais.

Para além da autoidentificação e qualificação, as entidades ficam sujeitas a um dever permanente de registo, obrigando-se a manter actualizadas, junto da autoridade competente, as informações relevantes para efeitos de supervisão, comunicação de incidentes e articulação institucional.

**b) Obrigações de informação e cooperação**

A política pública de segurança do ciberespaço assenta num conjunto de instrumentos estruturantes, designadamente a Estratégia Nacional de Segurança do Ciberespaço, o plano nacional de resposta a crises e incidentes de cibersegurança em grande escala e o Quadro Nacional de Referência para a Cibersegurança.

As entidades abrangidas devem acompanhar as orientações da autoridade de cibersegurança e cooperar nas avaliações de segurança.

Adicionalmente, as entidades essenciais e importantes devem designar um ponto de contacto permanente assegurando a existência de uma estrutura de comunicação contínua com a autoridade nacional de cibersegurança, especialmente em matéria de incidentes significativos e situações de crise. O ponto de contacto

deve ter disponibilidade permanente (24h /7 dias).

**c) Obrigações dos órgãos de gestão**

O RJC estabelece deveres específicos dos órgãos de gestão, direcção e administração das entidades essenciais e importantes, reforçando a sua responsabilidade directa na governação da cibersegurança.

Compete, designadamente, a esses órgãos aprovar e supervisionar as medidas de gestão de riscos, assegurar o cumprimento das obrigações legais e promover acções regulares de formação destinadas a garantir uma cultura organizacional adequada em matéria de segurança da informação.

Por forma a reforçar a obrigação de diligência, o regime determina a obrigatoriedade de designação de um responsável pela cibersegurança, que deve integrar os órgãos de gestão, direcção ou administração, ou a estes reportar de forma directa, assegurando a articulação entre a estratégia de cibersegurança e a governance corporativa.

A designação deve ser comunicada ao CNCS no prazo de 20 dias úteis após o início da actividade ou, para entidades já em funcionamento, até **4 de Maio de 2026.**

**d) Medidas de cibersegurança e gestão dos riscos**

As entidades essenciais e importantes são responsáveis por garantir a segurança das redes e dos sistemas de informação que utilizam, devendo adoptar medidas técnicas, operacionais e organizativas adequadas para gerir os riscos e minimizar o impacto de incidentes.

O regime exige uma abordagem sistémica e proporcional ao risco, prevendo a adopção de políticas de gestão de riscos, procedimentos de resposta a incidentes, medidas de continuidade de actividade e mecanismos de monitorização e avaliação contínua.

As medidas concretas a adoptar serão detalhadas no Regulamento do RJC, cuja publicação se aguarda após o encerramento da consulta pública.

Em matéria de cadeia de abastecimento, o regime impõe que as entidades avaliem as vulnerabilidades específicas dos seus fornecedores e prestadores de serviços, bem como a qualidade e prácticas de Cibersegurança adoptadas por estes.

**e) Certificação em cibersegurança**

A autoridade competente pode exigir às entidades essenciais, importantes e públicas relevantes a obtenção de certificação de cibersegurança, nacional, europeia ou internacional, destinada a comprovar a adequação das medidas adoptadas. Pode ainda ser exigida a utilização de produtos e serviços de TIC certificados.

**f) Obrigações de notificação**

O regime prevê deveres específicos de comunicação e notificação destinados a assegurar a monitorização contínua da segurança do ciberespaço. As entidades essenciais e importantes devem notificar a autoridade competente da sua participação em acordos de partilha de informações sobre cibersegurança.

Para além desta obrigação, o regime prevê a comunicação de vulnerabilidades e a notificação obrigatória de incidentes significativos.

## 4. Consequências do incumprimento

### a) Coimas

O incumprimento das obrigações previstas no RJC constitui contra-ordenação, punível com coimas que podem atingir €10 milhões ou 2% do volume de negócios anual mundial do exercício anterior (conforme o que for mais elevado). A qualificação da infracção (muito grave, grave ou leve), conjugada com a categoria da entidade (essencial, importante ou pública relevante), determina a moldura abstracta aplicável.

O RJC qualifica como muito graves os incumprimentos que afectem os deveres estruturantes do regime, designadamente a não adopção das medidas de gestão de riscos, a omissão de notificação de incidentes significativos, o incumprimento da obrigação de designação de responsável de Cibersegurança e a não implementação de ponto de contacto permanente.

Os limites máximos das coimas variam consoante a categoria da entidade:

» Entidades essenciais: até €10 milhões ou 2% do volume de negócios anual mundial (conforme o que for mais elevado)

» Entidades importantes: até €7 milhões ou 1,4% do volume de negócios anual mundial (conforme o que for mais elevado)

» Entidades públicas relevantes: até €500.000 (Grupo A) ou €100.000 (Grupo B)

A determinação da medida concreta da coima atende, entre outros factores, à gravidade da infracção, à duração do incumprimento, aos antecedentes da entidade, ao grau de cooperação com as autoridades e às medidas adoptadas para atenuar os danos.

Para além das coimas, o RJC prevê sanções acessórias, incluindo:

» Publicação da decisão sancionatória

» Interdição temporária do exercício de funções de administração ou direcção

» Suspensão de certificações ou autorizações

» Sanções pecuniárias compulsórias, para compelir ao cumprimento de determinações da autoridade competente

### b) Responsabilização pessoal dos gestores

O RJC consagra expressamente a responsabilização pessoal dos membros dos órgãos de gestão. O incumprimento dos deveres de supervisão e garantia do cumprimento das obrigações de cibersegurança pode determinar responsabilidade civil dos titulares desses órgãos, nos termos gerais da lei, quando se verifique actuação dolosa ou com culpa grave. Trata-se de uma inovação relevante face ao regime anterior, com impacto directo na governação das entidades abrangidas.

### c) Autoridade competente

O procedimento contra-ordenacional é instaurado e instruído pela autoridade de cibersegurança competente (o CNCS).

Importa, todavia, salientar que o legislador previu um período de adaptação durante o primeiro ano após a entrada em vigor do RJC. Assim, até **3 de Abril de 2027,** a aplicação do regime sancionatório será modulada, permitindo às entidades abrangidas ajustarem-se progressivamente às novas obrigações em matéria de Cibersegurança, sem ficarem imediatamente expostas à aplicação plena das coimas e sanções acessórias previstas.

## 5. Considerações finais

O RJC, aprovado pelo Decreto-Lei n.º 125/2025, de 4 de dezembro, entrou em vigor a 3 de abril de 2026, inaugurando um novo paradigma na regulação da cibersegurança em Portugal. A entrada em vigor foi precedida de desenvolvimentos institucionais relevantes, designadamente o protocolo de cooperação entre a CNPD e o CNCS para articulação com o RGPD, bem como a Circular n.º 2/2025 da ASF, em articulação com o Regulamento DORA.

Em março de 2026, o CNCS lançou a consulta pública sobre o projeto de Regulamento, que encerra a 22 de abril de 2026. Este diploma regulamentar estabelecerá, de forma integrada:

» **As regras de funcionamento da plataforma eletrónica**, que constituirá o canal principal para autoidentificação e registo de entidades, comunicação com as autoridades setoriais de cibersegurança, submissão de relatórios anuais e notificações eletrónicas

» **Os procedimentos de notificação de incidentes,** definindo as notificações e relatórios obrigatórios, bem como as condições para notificações voluntárias relativas a ciberameaças, quase incidentes ou vulnerabilidades

» **As normas de comunicação** entre entidades e a autoridade competente, incluindo a designação do responsável de cibersegurança e do ponto de contacto permanente

» **A matriz de risco** (Anexo II), que estabelece o quadro referencial dos valores de risco por setor e subsetor de atividade, atribuindo um de três níveis de conformidade: básico, substancial ou elevado

» **As medidas de cibersegurança mínimas** (Anexos III e IV), que especificam critérios, controlos e medidas de verificação para efeitos de auditorias e certificações

» **A metodologia de gestão de risco residual,** relativa aos ativos que garantam a continuidade das redes e sistemas de informação

O **Quadro Nacional de Referência de Cibersegurança** (Anexo I), instrumento de referência para identificação de normas, padrões e boas práticas em gestão da cibersegurança, e a **Matriz de Risco** (Anexo II) encontram-se já disponíveis, embora não estejam sujeitos a consulta pública.

Sem prejuízo das especificidades de cada situação concreta e da aprovação da versão final do Regulamento, todas as entidades potencialmente abrangidas devem:

» **Verificar o enquadramento no regime,** aferindo se integram um dos setores constantes dos Anexos I ou II do Decreto-Lei, se preenchem os critérios de dimensão e qual a qualificação aplicável (entidade essencial ou importante) Para verificar se a entidade será abrangida pelo RJC, o CNCS disponibilizou um simulador na plataforma MyCiber, a plataforma eletrónica referida no n.º 1 do artigo 8.º do Decreto-lei n.º 125/2025 que será usada, futuramente, para registo das entidades. É possível aceder ao simulador através deste link.

» **Designar o responsável de Cibersegurança** e preparar a comunicação ao CNCS, atendendo ao prazo de 4 de maio de 2026

- **Realizar um diagnóstico de conformidade,** identificando lacunas nas políticas, procedimentos, *governance* e medidas técnicas face às obrigações gerais do RJC
- **Elaborar um inventário de ativos,** identificando redes, sistemas de informação e ativos críticos, bem como mapeando interdependências
- **Avaliar a cadeia de abastecimento,** revendo contratos com fornecedores de serviços TIC e identificando riscos associados
- **Rever os planos de continuidade de negócio** e de recuperação de desastres
- **Iniciar programas de sensibilização e formação em cibersegurança p**ara colaboradores e órgãos de gestão

Recorde-se que, durante o primeiro ano de vigência do RJC, o regime sancionatório não produzirá efeitos plenos, constituindo este período uma oportunidade para que todas as entidades assegurem, progressivamente, a conformidade com o novo quadro regulatório.

Privacidade, Digital e Tecnologia