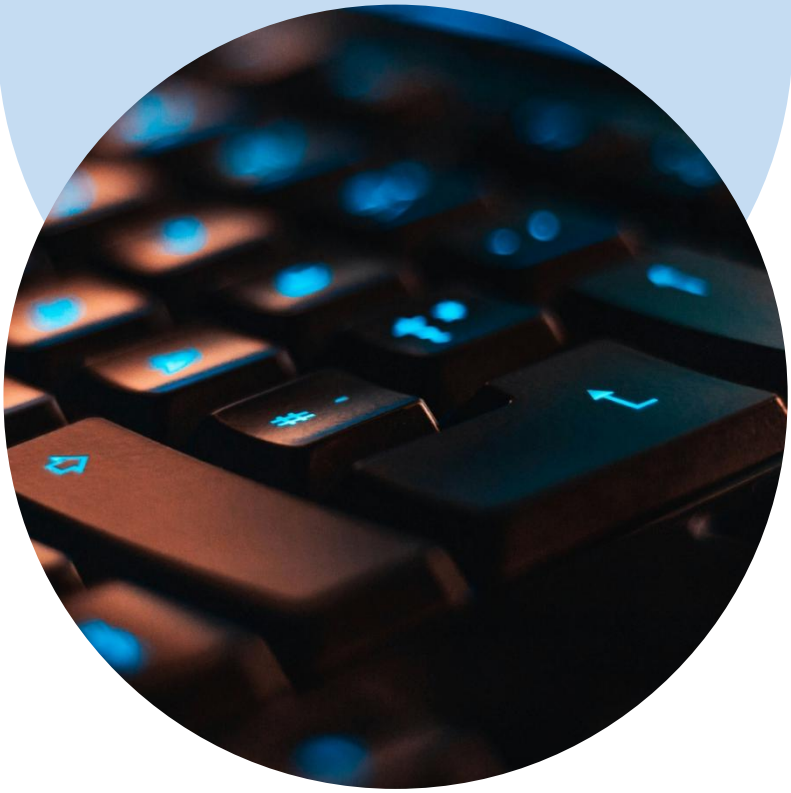
# DORA: regras de aplicação nacional

abreuadvogados.com



## 1. Objeto e âmbito de aplicação

Foi publicada no dia 23 de dezembro de 2025 a Lei n.º 73/2025, de 23 de dezembro ("**Lei 73/2025**"), que assegura a implementação de atos jurídicos europeus no ordenamento jurídico nacional relativos à resiliência operacional digital do setor financeiro, a saber o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022 ("Regulamento DORA") e a Diretiva (UE) 2022/2556 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022 ("**Diretiva DORA**").

A Lei 73/2025 tem por objetivos principais:

- Estabelecer as medidas de execução nacional do Regulamento DORA;
- Transpõe para a ordem jurídica interna a Diretiva DORA;
- Identificar as autoridades de supervisão competentes; e
- Definir o regime sancionatório aplicável

A Lei 73/2025 aplica-se a:

- Empresas de seguros e resseguros com sede em Portugal, às quais se aplica, respetivamente, o regime jurídico de acesso e exercício da atividade seguradora e resseguradora, aprovado pela Lei n.º 147/2015, de 9 de setembro
- Entidades gestoras de fundos de pensões autorizadas em Portugal, às quais se aplica o regime jurídico da constituição e do funcionamento dos fundos de pensões e das entidades gestoras de fundos de pensões, aprovado pela Lei n.º 27/2020, de 23 de julho.

- Demais entidades financeiras sujeitas ao Regulamento DORA: Excluem-se do seu âmbito as Caixas Económicas existentes a 1 de janeiro de 1985, salvo as que revestem a forma de sociedades anónimas.

## 2. Autoridades competentes e poderes de regulamentação

Para efeitos do Regulamento DORA, são três as entidades competentes, dispondo, no âmbito das respetivas atribuições, dos poderes e prerrogativas previstas na legislação referente à matéria de resiliência operacional digital:

(a) Banco de Portugal

- Entidades sujeitas à sua supervisão
- Autoridade única competente para a receção das comunicações dos incidentes de carácter severo relacionados com as tecnologias de informação e comunicação (TIC) e de notificações voluntárias de ciberameaças significativas no caso de instituições de crédito que exerçam atividades de distribuição de seguros e nos casos em que as instituições de crédito e instituições de pagamento prestem serviços de financiamento colaborativo

(b) ASF

- Entidades do setor segurador e fundos de pensões

(c) CMVM

- Entidades do setor dos valores mobiliários

Quando uma entidade seja supervisionada por mais de uma autoridade, prevalece a autoridade prudencial para efeitos de reporte e acompanhamento.

No âmbito dos seus poderes, cabe a estas entidades regulamentar as seguintes matérias:

a) Os canais e processos operacionais concretos para fins da comunicação às autoridades competentes da informação referente a incidentes de carácter severo relacionados com as TIC e à notificação voluntária de ciberameaças significativas;

b) Os canais e processos operacionais concretos para fins da comunicação às autoridades competentes da informação referente ao registo de informações em relação a todos os acordos contratuais relativos à utilização dos serviços de TIC prestados por terceiros prestadores de serviços de TIC;

c) Modelos normalizados, formulários e procedimentos para fins da comunicação às autoridades competentes da informação referente a acordos contratuais planeados de funções de TIC críticas ou importantes ou que se tornem críticas ou importantes;

d) A periodicidade, o conteúdo mínimo esperado e os modelos normalizados para fins da elaboração e comunicação à autoridade competente, se necessário e a pedido desta, da informação relativa ao relatório sobre a revisão do quadro de referência sobre o risco das TIC;

e) Os canais e processos operacionais concretos e as condições para fins da comunicação às autoridades competentes da informação referente à estimativa dos custos e perdas anuais agregados causados por incidentes de carácter severo relacionados com as TIC;

f) Modelos normalizados, formulários e procedimentos para fins da comunicação às autoridades competentes da informação referente a testes avançados através da realização de TLPT;

g) Os canais e processos operacionais concretos e as condições para fins da notificação às autoridades competentes da participação em acordos de partilha de informações específicas e sensíveis relativas a ciberataques

**3**. **Regime sancionatório**

O processamento dos ilícitos de mera ordenação social, a aplicação de coimas e sanções acessórias são competência da ASF, do Banco de Portugal ou da CMVM, consoante a autoridade competente.

Constituem contraordenações:

a) A prestação de informação à autoridade competente ou aos clientes que não seja completa, verdadeira, atual, clara, objetiva e lícita ou a omissão dessa prestação;

b) A não colaboração com as autoridades competentes no âmbito de exercícios de gestão de crises e contingência que envolvam cenários de ciberataques;

c) A violação de um conjunto de deveres, sem prejuízo de outros estabelecidos no Regulamento DORA, tais como, e a título ilustrativo, não exaustivo:

   (i) de implementar um quadro de governação interna e de controlo que garanta uma gestão eficaz e prudente do risco associado às TIC;

   (ii) de atribuir a responsabilidade pela gestão e supervisão do risco associado às TIC a uma função de controlo,

   (iii) de assegurar a segregação e independência das funções responsáveis pela gestão, controlo e de auditoria interna do risco associado às TIC;

   (iv) relativos ao exercício de funções, competências e responsabilidades de membro dos órgãos de administração e dos quadros superiores responsáveis pelas TIC das entidades financeiras;

   (v) de estabelecer estruturas de gestão de redes e infraestruturas, políticas, controlos e procedimentos no domínio das TIC

   (vi) de sujeição periódica a auditorias internas do quadro de gestão do risco associado às TIC e dos planos de resposta e recuperação em matéria de TIC;

   (vii) de realizar a análise do impacto na atividade das exposições a perturbações graves; de manter um local de tratamento de dados secundários; de ter uma função de gestão de crises;

(viii) de estabelecer um processo formal de acompanhamento das conclusões da análise da auditoria interna no quadro da gestão do risco associado às TIC; e

(ix) de desenvolver programas de sensibilização para a segurança das TIC, bem como de formação em matéria de resiliência operacional digital;

Este regime prevalece sobre os regimes sancionatórios setoriais, salvo se outro regime previr sanção mais grave. As contraordenações previstas na presente lei são equiparadas às contraordenações especialmente graves e às contraordenações muito graves para efeitos da aplicação do Regime Geral das Instituições de Crédito e Sociedades Financeiras, do Código dos Valores Mobiliários, aos crimes especiais do setor segurador e dos fundos de pensões e às contraordenações cujo processamento compete à ASF, de acesso e exercício da atividade seguradora e resseguradora, da constituição e do funcionamento dos fundos de pensões e das entidades gestoras de fundos de pensões, da distribuição de seguros e de resseguros

A tentativa e negligência são puníveis, sendo que em caso de negligência o limite máximo da coima é reduzido a metade, e na tentativa a sanção é especialmente atenuada.

Às contraordenações previstas na presente lei são aplicáveis as seguintes coimas:

| Tipo de Entidade | Pessoas Coletivas | Pessoas Singulares |
|---|---|---|
| Instituições de crédito, centrais de valores mobiliários,<br>Prestadores de serviços de pagamento<br>Instituições de moeda eletrónica,<br>Empresas de seguros e resseguros,<br>Prestadores de serviços de criptoativos,<br>Administradores de índices de referência críticos<br>Fundos de pensões | €10.000 a €5.000.000 | €5.000 a €2.500.000 |
| Mediadores de seguros, resseguros e a título acessório | €3.000 a €2.500.000 | €1.000 a €500.000 |
| Prestadores de serviços de financiamento colaborativo | €2.500 a €500.000 | €400 a €500.000 |
| O limite máximo das coimas pode ser agravado até:<br>• **3 vezes** o benefício económico obtido (incluindo perdas evitadas); ou<br>• **10%** do volume de negócios anual (para pessoas coletivas do primeiro grupo) | | |

## 4. Alterações Legislativas

No âmbito da transposição da Diretiva DORA, e de forma a assegurar uma aplicação coerente da matéria de resiliência operacional digital, a Lei 73/2025 procede à alteração (total ou parcialmente) de oito diplomas fundamentais:

(i) Regime Geral das Instituições de Crédito e Sociedades Financeiras:

- Banco de Portugal pode, sempre que seja necessário para a supervisão em base consolidada das instituições de crédito, proceder ou mandar proceder a verificações e exames periciais nas companhias financeiras, companhias mistas ou nas companhias financeiras mistas e nas respetivas filiais, bem como nas sociedades de serviços auxiliares, incluindo terceiros prestadores de serviços de TIC;
- A explicação da forma como as funções críticas e as linhas de negócio estratégicas podem ser jurídicas, económica e operacionalmente separadas, na medida do necessário, de outras funções, para assegurar a sua continuidade, e a resiliência operacional digital, em caso de insolvência da instituição de crédito;
- Identificação dos proprietários dos sistemas identificados na alínea anterior, acordos de nível de serviço associados e programas, sistemas ou licenças informáticas, incluindo uma discriminação das respetivas entidades jurídicas, das funções críticas e linhas de negócio estratégicas, bem como uma identificação dos terceiros prestadores de serviços de TIC críticos.

(ii) Código dos Valores Mobiliários.

(iii) Decreto-Lei n.º 357-C/2007, de 31 de outubro (Transposição da Diretiva dos Mercados de Instrumentos Financeiros).

(iv) Regime jurídico de acesso e exercício da atividade seguradora e resseguradora.

(v) Regime Jurídico dos Serviços de Pagamento e Moeda Eletrónica.

(vi) Regime jurídico da constituição e funcionamento dos fundos de pensões e entidades gestoras.

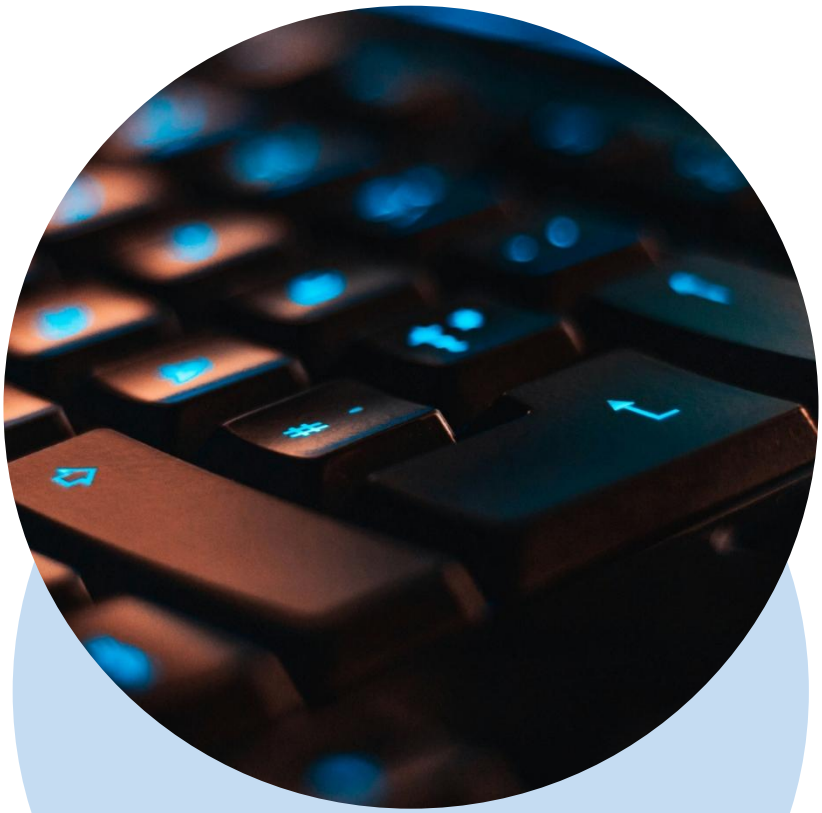
(vii) Regime das Empresas de Investimento.

(viii) Regime da Gestão de Ativos.

## 5. Próximos Passos

As entidades abrangidas devem:

- Avaliar o impacto da Lei 73/2025 nos atuais processos.
- Proceder à revisão e atualizar políticas e procedimentos de resiliência operacional digital.
- Assegurar conformidade com os requisitos de governação e gestão de risco de TIC.
- Implementar programas de formação e sensibilização.



**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

**Catarina Rodrigues Rocha** – Advogada Estagiária
catarina.r.rocha@abreuadvogados.com