Todas as instituições · Em vigor

DORA, resiliência operacional digital

O regulamento DORA aplica-se desde 17 de janeiro de 2025. Enquadra a gestão do risco informático, a comunicação de incidentes, os testes de resiliência e o recurso a prestadores. O BCE faz dele um eixo dos seus controlos para 2027-2029.

DATA DE APLICAÇÃO	QUEM O EXIGE	A QUEM RESPONDE	NATUREZA DA EXIGÊNCIA
17 jan. 2025	Legislador europeu (regulamento DORA)	BCE, ACPR, AMF	Supervisão prudencial

INSTITUIÇÕES ABRANGIDAS

- Grande grupo bancário
- Banco de média dimensão
- Financiamento especializado
- Banco privado
- Sociedade gestora
- Seguradora
- Mútua e previdência
- Instituição financeira pública

Fundo cheio: abrangido. Tracejado: consoante o estatuto ou a atividade.

MARCOS

O calendário do texto.

27 dez. 2022	16 jan. 2023	17 jan. 2025	19 nov. 2026
Publicação do Regulamento (UE) 2022/2554	Entrada em vigor	Aplicação	Prioridades de supervisão 2027-2029 do BCE

EM DETALHE

O que muda.

Quatro pilares

EM APLICAÇÃO DESDE 17 DE JANEIRO DE 2025

RISCO INFORMÁTICO	INCIDENTES	TESTES	PRESTADORES
• Quadro de gestão do risco associado às tecnologias	• Comunicação dos incidentes ao supervisor	• Testes de resiliência • Testes de intrusão baseados em ameaças	• Gestão do risco de terceiros • Dependências da cloud

Programa do BCE para 2027-2029: duas campanhas de inspeções, sobre a cibersegurança e sobre o risco de terceiros.

O Regulamento (UE) 2022/2554 relativo à resiliência operacional digital do setor financeiro é aplicável desde 17 de janeiro de 2025. Abrange quatro pilares: a gestão do risco informático, a comunicação de incidentes, os testes de resiliência e a gestão do risco associado aos prestadores de serviços informáticos.

As prioridades de supervisão 2027-2029 do BCE, publicadas em 19 de novembro de 2026, preveem duas campanhas de inspeções, sobre a cibersegurança e sobre o risco de terceiros, testes de intrusão

baseados em ameaças realizados nos termos do DORA e uma revisão das dependências da cloud.

A NOSSA LEITURA

Desde a entrada em aplicação, a questão já não é a conformidade no papel, mas provar que o dispositivo funciona: registo de prestadores atualizado, incidentes comunicados dentro dos prazos, testes seguidos de ações. As mudanças de sistema, como uma migração de core banking ou uma passagem para a cloud, são os momentos em que este dispositivo está mais exposto.

O QUE FAZEMOS

Consideração dos requisitos do DORA nos projetos de migração e de transformação dos sistemas, manutenção dos dados do registo de prestadores, documentação dos controlos.

DORA | Risco de terceiros | Cloud

CORE BANKING→

PARA SABER MAIS

Fontes oficiais.

BCE, prioridades de supervisão 2027-2029	https://www.bankingsupervision.europa.eu/framework/supervisory-policy/html/ssm.supervisory_priorities202611.en.html
ACPR, dossiê DORA	https://acpr.banque-france.fr/fr/reglementation/focus-sur-la-reglementation/transverse/digital-operational-resilience-act-dora
AMF, dossiê DORA	https://www.amf-france.org/fr/actualites-publications/dossiers-thematiques/dora
EIOPA, dossiê DORA	https://www.eiopa.europa.eu/digital-operational-resilience-act-dora_en

Ligações verificadas em 23 de novembro de 2026.