DORA: o que muda na cibersegurança financeira?

itsecurity.pt/news/opinion/dora-o-que-muda-na-ciberseguranca-financeira

IT Security

Nos últimos anos, temos acompanhado várias organizações do setor financeiro na adaptação a novas exigências regulatórias. Mas poucas geraram tanta resistência — e, simultaneamente, tanta urgência — como o DORA. Talvez porque nos obriga a olhar de frente para uma realidade que muitos ainda encaram como um detalhe técnico: a dependência total da tecnologia.

O DORA (Regulamento de Resiliência Operacional Digital) quer garantir que bancos, seguradoras, fintechs, fundos de investimento e respetivos fornecedores tecnológicos consigam continuar a operar mesmo quando os sistemas falham. E falham. Não é uma hipótese teórica: entre ciberataques, erros humanos e falhas de terceiros, os incidentes com impacto operacional multiplicam-se todos os anos.

Segundo a Agência da União Europeia para a Cibersegurança (ENISA), só em 2023, o setor financeiro foi alvo de mais de 25% dos ataques reportados. Um em cada quatro. Já não se trata apenas de proteger dados: trata-se de garantir continuidade, resiliência e confiança num setor que não pode parar.

Entre os principais requisitos, destaco aqui cinco pilares: **1) Governança e controlo de risco**: a gestão de risco tecnológico passa a ser parte da estratégia, com responsabilidade clara ao nível da administração; **2) Gestão de incidentes**: as organizações devem ter processos de deteção, resposta e reporte rápido de incidentes — com envio obrigatório às autoridades; **3) Testes de resiliência digital**: serão exigidos testes regulares aos sistemas críticos, incluindo simulações de ataques, para avaliar a capacidade de resposta; **4) Gestão de terceiros**: os fornecedores que prestam serviços tecnológicos críticos passam a estar sujeitos a obrigações contratuais específicas e a maior supervisão; e **5) Partilha de informação**: fomenta-se a cooperação entre entidades sobre ciberameaças, com mecanismos para partilhar alertas relevantes.

Pese embora a aplicação plena do regulamento apenas tenha entrado em vigor em janeiro de 2025, tendo o referido diploma sido publicado em dezembro de 2022, na prática, constatou-se que o mesmo originou desafios reais e imediatos, aquando da sua publicação. Aliás, um estudo das Autoridades Europeias de Supervisão (ESAs) indica que menos de 30% das instituições têm hoje uma gestão madura do risco tecnológico. Em Portugal, o Banco de Portugal e a ASF já emitiram orientações de preparação — e a maioria dos contratos com fornecedores ainda não refletem os requisitos do DORA.

O impacto é estrutural: DORA não é mais um documento para assinar e arquivar. Vai obrigar a rever políticas internas, exigir inventários rigorosos de ativos tecnológicos, estabelecer fluxos claros de comunicação e, sobretudo, testar — e provar — que a organização está preparada para o inesperado.
A boa notícia? Quem cumprir o DORA estará mais bem preparado para resistir a falhas e ataques, proteger os seus clientes e manter a confiança no setor financeiro.

Mais do que uma obrigação, encaro este regulamento como uma oportunidade. Para criar estruturas mais robustas, relações mais transparentes com fornecedores e, acima de tudo, um setor financeiro europeu mais resistente. E isso interessa a todos — não apenas a quem trabalha no setor, mas a qualquer pessoa que utiliza um cartão, efetua uma transferência ou depende da estabilidade financeira. Como em tudo, resiliência não se improvisa. Constrói-se.

Francisca Marques