



DORA

High Level Snapshot

1. BREVE VISÃO GERAL

O **Digital Operational Resilience Act** (“**DORA**”)¹ é um Regulamento da União Europeia destinado a garantir que as **entidades financeiras** possam resistir, responder e recuperar-se de incidentes cibernéticos e outros eventos relacionados com interrupções operacionais.

Âmbito subjetivo: Aplica-se a uma ampla gama de entidades financeiras, incluindo, mas sem limitar, a instituições de crédito, empresas de investimento, gestores de fundos de investimento alternativos, sociedades gestoras, empresas de seguros e fornecedores de serviços de tecnologia da informação.

Objetivo: Manutenção, por parte das entidades financeiras de uma elevada resiliência operacional digital compatível com os recursos disponíveis e com o seu perfil de risco, através de uma gestão eficaz dos riscos de tecnologias de informação e comunicação (“**TIC**”), testes rigorosos de resiliência, monitorização de terceiros e partilha de informações sobre ameaças e incidentes.

¹ **REGULAMENTO (UE) 2022/2554**, do Parlamento Europeu e do Conselho de 14 de dezembro de 2022, relativo à resiliência operacional digital do setor financeiro e que altera os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/10.



2. IMPORTÂNCIA DA RESILIÊNCIA OPERACIONAL DIGITAL

Com o aumento das ameaças cibernéticas (como *ransomeware*, *phishing*, *hacking* e violação de dados) e a crescente dependência das tecnologias digitais nos mercados de capitais, a resiliência operacional tornou-se um fator crítico para a segurança e estabilidade do setor financeiro.

Por isso, há que:

- Proteger os Clientes e os seus interesses, garantindo a continuidade dos serviços financeiros.
- Mitigar os Riscos de perdas financeiras significativas e danos reputacionais, reduzindo a vulnerabilidade a ciberataques e outras interrupções operacionais.
- Promover a Conformidade Regulamentar e o cumprimento das exigências do DORA, evitando penalidades e sanções.

Vantagem Competitiva: Entidades financeiras com uma forte resiliência operacional digital estão melhor posicionadas para se adaptar a novas ameaças e mudanças no mercado.

3. PILARES DO DORA

3.1. GOVERNO SOCIETÁRIO

O DORA estabelece requisitos específicos de governo societário, como a atribuição de papéis claros às funções relacionadas com as TIC. Compete ao órgão de administração a manutenção de um papel fulcral e ativo na orientação e adaptação do quadro de gestão destes riscos.

3.2. GESTÃO DO RISCO TIC

Esta gestão do risco inclui estratégias, políticas e procedimentos, protocolos e ferramentas de TIC que possam assegurar proteção, prevenção e deteção *end-to-end*, para limitar os danos e priorizar a recuperação rápida e segura das atividades.



3.3. REPORTE DE INCIDENTES TIC

O DORA vem estabelecer obrigações de harmonização e racionalização da comunicação de incidentes relacionados com as TIC, através de um mecanismo de reporte de comunicações uniforme.

3.4. TESTE DE RESILIÊNCIA OPERACIONAL DIGITAL

Os quadros de gestão de riscos das empresas no domínio das TIC devem ser periodicamente testados para identificar quaisquer deficiências e avaliados criticamente. Se forem assinaladas deficiências, as instituições devem implementar e documentar medidas corretivas.

3.5. PARTILHA DE INFORMAÇÃO E INTELIGÊNCIA

A obrigação de promoção da partilha de informação relativa a ameaças cibernéticas entre entidades financeiras pode reduzir o impacto dos incidentes e representa uma vantagem na mitigação dos riscos.

3.6. GESTÃO DO RISCO DE TERCEIROS DE TIC

O DORA vem exigir às empresas, que para além da monitorização do grau de dependência operacional que possa existir com os prestadores de serviços TIC terceiros, passem a incluir a informação relativa a este grau de dependência nos contratos celebrados com estes prestadores de serviços.

4. BREVE CRONOLOGIA

27/12/2022

· Publicação do DORA.



16/01/2023

· Entrada em vigor do DORA.



17/01/2024

· Publicação do *First Batch*, que inclui normas técnicas e normas de implementação.



17/07/2024

· Publicação do *Second Batch*, que inclui normas técnicas, normas de implementação e orientações.



17/01/2025

· Aplicação do DORA.



MARIA
CARVALHO MARTINS



ANA RITA
LOURENÇO