

Digital Operational Resilience Act (DORA)

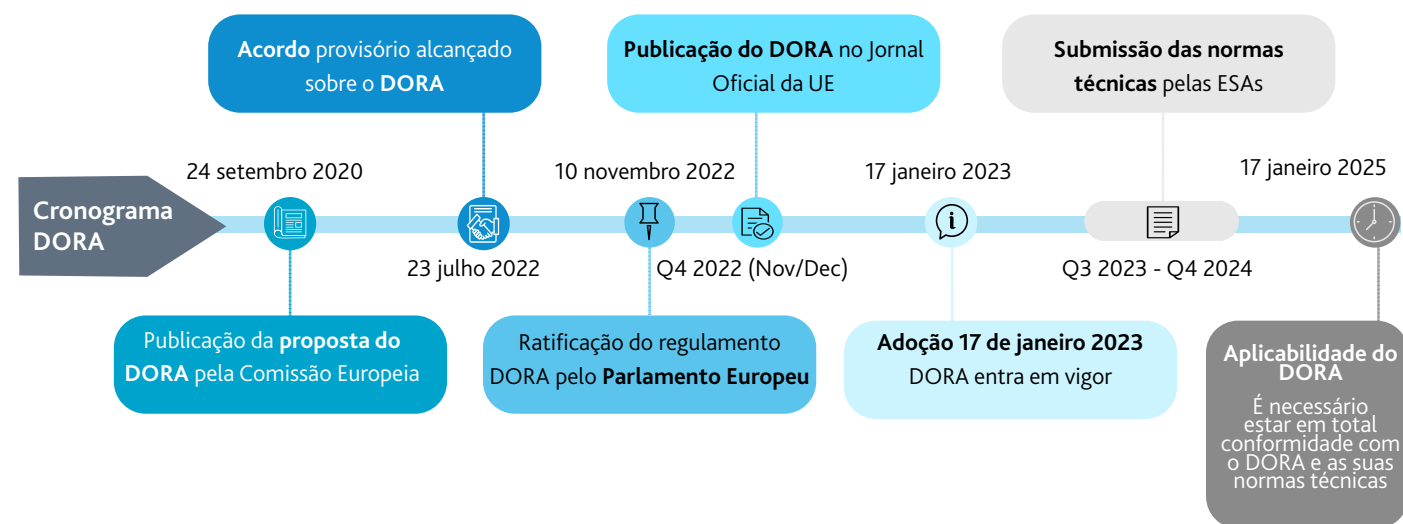
Explore com confiança os caminhos do DORA

VISÃO GERAL DO DORA

O objetivo do DORA é melhorar a cibersegurança e a resiliência operacional de todas as instituições financeiras regulamentadas na Europa e dos prestadores de serviços críticos relacionados com as tecnologias da informação e comunicação (TIC).

O Digital Operational Resilience Act (Lei de Resiliência Operacional Digital) estabelece um conjunto unificado de requisitos para a segurança de redes e sistemas de informação de empresas e organizações que operam no setor financeiro, bem como de terceiros que fornecem serviços relacionados com as TIC a essas entidades (por exemplo, plataformas cloud ou serviços de análise de dados). Além disso, o DORA estabelece um enquadramento regulamentar para a resiliência operacional digital, no qual todas as empresas necessitam de garantir que conseguem resistir, responder e recuperar de todos os tipos de perturbações e ameaças relacionadas com as tecnologias da informação e comunicação. Os requisitos são os mesmos em todos os Estados-Membros da UE, uma vez que visam prevenir e mitigar o crescente número de ameaças cibernéticas.

O cronograma de implementação do DORA



ENTIDADES SUJEITAS

As entidades sujeitas terão de implementar o regulamento e estar totalmente em conformidade até 17 de janeiro de 2025.

O DORA aplica-se a uma vasta gama de organizações, incluindo instituições financeiras, como bancos, companhias de seguros, empresas de investimento, bolsas de valores, fintechs, etc., e fornecedores externos de serviços destas entidades na que operam na área das tecnologias da informação e comunicação, tais como serviços de computação cloud, software, serviços de análise de dados e centros de dados.

O DORA coloca a relação entre as instituições financeiras e os seus fornecedores de tecnologia sob uma nova perspetiva para abordar em conjunto os requisitos regulamentares.

As entidades financeiras e os fornecedores externos de serviços de TIC devem aumentar a sua colaboração para dar resposta aos requisitos desta nova regulamentação.

Quem é responsável?

Globalmente, a responsabilidade por este enquadramento, e outras obrigações de governação impostas pelo DORA, recae sobre o órgão de administração da entidade, que será responsável por rever, aprovar, implementar e atualizar o enquadramento da gestão de riscos.

A gestão deverá ter plena consciência e compreensão do uso, serviços e perfil de risco das TIC da instituição financeira. Esta poderá ser a altura ideal para as empresas avaliarem como as linhas de reporte do seu departamento de tecnologias da informação para a gestão operam na prática diária.

As instituições financeiras sujeitas ao DORA devem nomear um membro da direção de topo pela resiliência operacional digital e reportar incidentes às autoridades competentes.

Entidades afetadas pelo DORA conforme o Artigo 2 - Âmbito de aplicação

Entidades financeiras

- ▶ Instituições de crédito
- ▶ Instituições de pagamento
- ▶ Prestadores de serviços de informação sobre contas
- ▶ Instituições de moeda eletrónica
- ▶ Empresas de investimento
- ▶ Prestadores de serviços de criptoativos e emitentes de tokens referenciadas a ativos
- ▶ Centrais de valores mobiliários
- ▶ Contrapartes centrais
- ▶ Plataformas de negociação
- ▶ Repositórios de transações
- ▶ Gestoras de fundos de investimento alternativos
- ▶ Sociedades gestoras
- ▶ Prestadores de serviços de comunicação de dados
- ▶ Empresas de seguros e resseguros

Terceiros prestadores de serviços de TIC*

- ▶ Prestadores de serviços de computação em cloud
- ▶ Software
- ▶ Serviços de análise de dados
- ▶ Prestadores de serviços de centros de dados
- ▶ Empresas que fazem parte de um grupo financeiro e fornecem serviços de TIC predominantemente à sua casa-mãe, ou às subsidiárias ou sucursais da sua casa-mãe
- ▶ Entidades financeiras que fornecem serviços de TIC a outras entidades financeiras
- ▶ Participantes no ecossistema de serviços de pagamento, que prestam atividades de processamento de pagamentos ou operam infra-estruturas de pagamento

* As entidades enumeradas são exemplos de prestadores externos de serviços de TIC.



IMPACTO DO DORA

Embora o DORA permita um período de transição até 17 de janeiro de 2025, a conformidade pode ser desafiadora e demorada para as entidades abrangidas.

Alcançar a conformidade com as exigentes obrigações do DORA dentro do prazo estipulado será desafiador e demorado. Embora o DORA permita um período de transição até 17 de janeiro de 2025, a BDO recomenda que as organizações abrangidas iniciem imediatamente os preparativos.

A BDO recomenda a adoção de uma abordagem faseada, em que as entidades abrangidas devem delinear um programa de conformidade com o DORA com o objetivo de atingir a conformidade até o final do período de transição.

A falta de conformidade pode resultar em multas severas a partir de janeiro de 2025.

Conformidade

As respetivas autoridades nacionais competentes (no caso Português, será a entidade de supervisão de cada tipo de entidade, i.e., o Banco de Portugal, CMVM ou ASF, conforme o caso) farão cumprir o regulamento conforme necessário. Os Estados-Membros da UE terão o direito de impor penalidades por violação de obrigações.

As penalidades significativas assumirão a forma de um pagamento periódico de 1% do volume de negócios global diário médio da organização no ano comercial anterior. Isso será aplicado pela entidade de supervisão, diariamente, até que a conformidade seja alcançada, por um período não superior a seis meses.

A nossa recomendação

Recomendamos os seguintes pontos de ação:

- ▶ Faça uma avaliação de maturidade relacionada com os requisitos DORA, com análise de lacunas e respectivo plano de mitigação para alcançar a conformidade até o final de 2024.
- ▶ Melhore o seu programa de gestão de riscos de TIC certificando-se de que tem uma visão completa dos seus sistemas críticos e medidas em vigor para mitigar ou minimizar o risco.
- ▶ Crie um registo de fornecedores de serviços críticos de TIC e realize avaliações de riscos de terceiros.

REQUISITOS

O DORA é composto por 58 artigos e está estruturado em torno de cinco pilares-chave:



Gestão do risco associado às TIC

(Artigos 5 a 16)

- ▶ Governação: órgão de administração responsável
- ▶ Quadro de gestão de riscos e atividades associadas (identificação, proteção, deteção, resposta e recuperação, aprendizagem e evolução, comunicação de crise)



Gestão, classificação e comunicação de incidentes relacionados com as TIC

(Artigos 17 a 23)

- ▶ Classificação padronizada de incidentes
- ▶ Reporte obrigatório e padronizado de incidentes de carácter severo
- ▶ Relatórios padronizados a nível da UE de forma anonimizada



Teste de resiliência operacional digital

(Artigos 24 a 27)

- ▶ Programa de testes proporcional e baseado no risco
- ▶ Testes de ameaças em grande escala efetuados por testadores independentes a cada 3 anos



Gestão de risco de terceiros nas TIC

(Artigos 28 a 44)

- ▶ Estratégia, política e registo padronizado de prestadores de serviços de TIC
- ▶ Orientações para a avaliação pré-contratual, conteúdo do contrato, rescisão e a saída em situação de stress



Disposições de partilha de informações

(Artigo 45)

- ▶ As instituições financeiras são encorajadas a partilhar informações sobre ciberameaças e cibersegurança, indicadores de comprometimento dos sistemas ou dos dados, táticas, técnicas e procedimentos.



A NOSSA SOLUÇÃO





Os ciberataques têm dominado o panorama de riscos para organizações em todo o mundo ao longo dos anos. Setores críticos para a nossa sociedade, como finanças, saúde, transporte e energia, estão cada vez mais dependentes da tecnologia, tornando esses setores vulneráveis a interrupções graves se os riscos tecnológicos não forem mitigados adequadamente.

Consequentemente, as empresas e outras instituições têm vindo a aumentar os seus investimentos para ampliar significativamente a sua resiliência e maturidade ao nível da segurança da informação.

É importante compreender que todos estes investimentos em boa governação e em infraestruturas digitais seguras não se perdem, antes são, por si só, pedras angulares de regulamentos anteriores e futuros em matéria de cibersegurança, como o DORA e o NIS2.

Na BDO, reconhecemos esses esforços e estamos aqui para ajudar a avaliar o seu nível atual de conformidade e necessidades de desenvolvimento de uma forma eficiente e controlada.

De que forma a BDO poderá ajudar?

-  1 Avaliar até que ponto o regulamento DORA se aplica à sua organização.
-  2 Realizar uma gap analysis da implementação do DORA e avaliar o seu atual nível de maturidade e resiliência cibernética.
-  3 Definir um plano de segurança prioritizado que inclua requisitos específicos do DORA para a sua organização, mas que também esteja em conformidade com outras legislações e regulamentos aplicáveis.
-  4 Auxiliar na gestão de projetos e/ou execução prática do plano de segurança, por exemplo, através da implementação de políticas e procedimentos-chave, da realização de testes de resiliência, da gestão testes de intrusão e implementação de recomendações subsequentes, de avaliações de risco de fornecedores na área das TIC, etc.



PARA MAIS INFORMAÇÕES:

MÁRIO SILVESTRE NETO

Partner
+351 937 997 003
silvestre.neto@bdo.pt

ANTÓNIO JORGE PINTO

Manager
+351 937 990 031
antonio.pinto@bdo.pt

RICARDO VIDAL MOREIRA

Manager
+351 912 942 258
ricardo.moreira@bdo.pt

A BDO & Associados, SROC, Lda., BDO Consulting, Lda., BDO Outsourcing, Serviços de Contabilidade e Organização, Lda., BDO Outsourcing, Serviços de Contabilidade e Organização II, Lda. e BDO II Advisory S.A., sociedades registadas em Portugal, são membros da BDO International Limited, sociedade inglesa limitada por garantia, e fazem parte da rede internacional BDO de firmas independentes. BDO é a marca da rede internacional BDO e para cada uma das Firmas Membro BDO.

Copyright © dezembro, 2023, BDO Portugal. Todos os direitos reservados. Publicado em Portugal.

www.bdo.pt