Regulamento DORA e o risco tecnológico – a maior transformação para a infraestrutura do setor financeiro depois do RGPD

abreuadvogados.com/

A. Contexto do DORA

Na era digital, as tecnologias da informação e comunicação (TIC) mantêm em funcionamento setores fundamentais da economia, nomeadamente o setor financeiro.

A intensificação da digitalização, a interligação entre sistemas informáticos e a utilização em larga escala de dados pessoais amplifica o risco associado às TIC, tornando a sociedade no seu conjunto e, em particular, o sistema financeiro, vulneráveis a ciberameaças ou perturbações no domínio das TIC.

Hoje em dia o risco associado a ataques informáticos e eventos de violação de dados não conhece limites quantificáveis, podendo ter consequências reputacionais imprevisíveis e irreparáveis.

Esta realidade respeita a empresas que operam transversalmente no setor financeiro, sejam operadores tradicionais, — Bancos, Seguradoras e Empresas de Investimento —, FinTech ou empresas tecnológicas. Foi nesse âmbito que a Comissão Europeia apresentou, em 20 de setembro de 2020, o *digital finance package* com vista a fomentar o desenvolvimento tecnológico e assegurar a estabilidade do mercado financeiro e proteção dos consumidores.

Esse pacote legislativo, que acompanha a estratégia para a as finanças digitais, integrava a proposta de Regulamento Mercados de Criptoativos europeu (Regulamento MiCA), que aguarda para breve a sua aprovação final, e uma proposta de Regulamento relativo à resiliência operacional digital do setor financeiro (Digital Operational Resilience Act ou "DORA"), que foi já adotado e publicado no Jornal Oficial da UE no passado dia 27 de dezembro de 2022.

O DORA está em vigor desde 16 de janeiro de 2023 e iniciará a sua aplicação em todos o espaço da União Europeia, sem necessidade de transposição, no dia 17 de janeiro de 2025, data em que as entidades abrangidas terão de ter assegurado o cumprimento das novas obrigações regulatórias relativas à resiliência operacional digital.

Nos próximos dois anos a reformulação de todo o modelo de governo das áreas tecnológicas e sistemas de segurança da informação, e de gestão do risco tecnológico, será um dos grandes projetos a desenvolver por todas as entidades que recorrem à tecnologia para a prestação de serviços financeiros e por todos os fornecedores de tecnologia ao setor financeiro.

B. O que se pretende com o DORA?

Reconhecendo a existência de um risco sistémico para o setor financeiro, que é, em grande medida, digital, com uma interligação e dependências no interior do próprio setor e em relação a infraestruturas e serviços prestados por terceiros, o DORA visa reforçar a resiliência do setor aos riscos associados a essas TIC, introduzindo requisitos específicos idênticos que serão aplicáveis em todos os Estados-Membro da UE.

O objetivo é o de que as entidades financeiras que recorrem a tecnologia sejam capazes de resistir, responder e recuperar do impacto dos incidentes relacionados com as TIC, continuando a providenciar os serviços críticos, mesmo em alturas de crise, e minimizando a perturbação para os clientes e para o próprio sistema financeiro. Tal apenas será possível através da instituição de medidas e controlos robustos sobre sistemas, ferramentas e terceiros.

Assim o Regulamento DORA estabelece requisitos uniformes para a segurança das redes e sistemas de informação de empresas e organizações que operam no sector financeiro, bem como de terceiros que lhes prestam serviços relacionados com as TIC. Tais requisitos respeitam a:

- gestão do risco no domínio das tecnologias da informação e comunicação (TIC);
- notificação de incidentes de caráter severo relacionados com as TIC e notificação, numa base voluntária, de ciberameaças significativas às autoridades competentes;
- notificação de incidentes de caráter severo operacionais ou de segurança, relacionados com pagamentos, às autoridades competentes pelas entidades financeiras;
- realização de testes de resiliência operacional digital;
- partilha de dados e informações sobre as ciberameaças e as vulnerabilidades;
- medidas para a boa gestão do risco associado às TIC devido a fornecedores;
- Requisitos referentes aos acordos contratuais celebrados entre terceiros prestadores de serviços de TIC e entidades financeiras;
- Regras para o estabelecimento e execução do quadro de superintendência dos terceiros prestadores de serviços de TIC críticos na prestação desses serviços a entidades financeiras.

C. A quem se aplica?

O Regulamento é aplicável a:

Entidades financeiras, tais como:

- instituições de crédito;
- instituições de pagamento;
- instituições de moeda eletrónica;
- empresas de investimento;
- sociedades gestoras de organismos de investimento coletivo em valores mobiliários e de organismos de investimento alternativo;
- empresas e mediadoras de seguros e resseguros;
- prestadores de serviços de financiamento colaborativo (*crowdfunding*) e
- prestadores de serviços de criptoativos e emitentes de *tokens* referenciados a ativos (*stablecoins*), autorizados nos termos do Regulamento MiCA;

Empresas tecnológicas, prestadoras de serviços de TIC às Entidades Financeiras.

D. Todas as empresas ficam automaticamente sujeitas ao DORA?

Não. O Regulamento exclui do âmbito de aplicação, com algumas exceções, as empresas que com menos de 10 trabalhadores e cujo volume de negócios anual e/ou balanço total anual não exceda 2 milhões de euros ("Microempresas").

Apesar da ampla cobertura pretendida, a aplicação das regras de resiliência operacional digital deverá ter em conta a dimensão e o perfil de risco de cada entidade financeira, designadamente em função da natureza, escala e complexidade dos serviços, atividades e operações.

É, assim, instituído um princípio da proporcionalidade, de acordo com o qual o estabelecimento de estruturas de governação e requisitos mais complexos só é imposto às Entidades Financeiras que não sejam Microempresas, visto que as entidades financeiras de maior dimensão dispõem de mais recursos e conseguem mais rapidamente mobilizar fundos para se conformarem às exigências impostas pelo diploma, sem com isso colocarem em causa a sustentabilidade do seu negócio.

As Microempresas e entidades financeiras abrangidas pelo quadro simplificado de gestão do risco veem, dessa forma, as obrigações reduzidas.

E. A partir de quando?

Atenta a natureza jurídica do diploma, o Regulamento será aplicável sem necessidade de transposição por diploma legal nacional. As entidades abrangidas têm até 17 de janeiro de 2025 para se adaptar e assegurar o cumprimento das novas obrigações impostas pelo DORA.

F. Quais são as principais obrigações para as Entidades Financeiras?

Os requisitos e obrigações abrangidas pelo DORA dividem-se pelas seguintes áreas principais:

o Governação

As entidades financeiras, pela atuação do seu órgão de administração, estão obrigadas a implantar um quadro de governação interna e de controlo que garanta uma gestão eficaz e prudente do risco associado às TIC, a fim de alcançar um elevado nível de resiliência operacional digital.

Este quadro de governação deve estar articulado com o sistema de controlo interno, em especial a função de gestão de risco, e funcionará como uma segunda linha de defesa.

o Gestão de Risco

Os órgãos de administração têm a responsabilidade final pela gestão do risco associado às TIC. Para o efeito, o DORA estabelece um elenco de deveres e obrigações a que a administração está sujeita dos quais se destacam:

- obrigação para os membros da gestão de desenvolverem e manterem conhecimentos sobre os riscos das TIC;
- identificação da sua tolerância ao risco das TIC, em linha com a apetite ao risco da Entidade, e manutenção de um quadro abrangente de gestão do risco das mesmas, orientando o trabalho relacionado com essa gestão;
- manutenção de programas e avaliações de gestão de risco;
- obrigação de implementar um sistema de gestão da segurança da informação reconhecido internacionalmente.

Para efeitos da gestão do risco referido, mostrar-se-á necessário proceder a implementação de um quadro dispositivo, com diversas políticas e protocolos que prevejam, designadamente, uma boa gestão da rede e das infraestruturas baseada no risco, sistemas correções de anomalias e atualizações de *software*, mecanismos de autenticação fortes, a limitação do acesso físico e virtual aos recursos e dados dos sistemas TIC, a prevenção de fugas de informação, entre outras.

As Entidades Financeiras abrangidas ficam ainda obrigadas a adotar e rever regularmente uma estratégia sobre o risco de terceiros prestadores de serviços de TIC e manter um registo que descreva todas as posições contratuais com os mesmos.

o Classificação e reporte de Incidentes

As entidades abrangidas são obrigadas a pôr em prática um processo de gestão de incidentes relacionados com as TIC e a desenvolver capacidades para monitorizar, tratar e acompanhar esses incidentes, incluindo procedimentos para "detetar, gerir e notificar com as TIC e criar indicadores de alerta precoce como alertas".

Os incidentes devem ser obrigatoriamente classificados de acordo com fatores tais como a distribuição geográfica e duração de incidente, criticidade dos serviços efetuados, entre outros, devendo ser comunicados à autoridade setorial competente sempre que qualificados como graves.

o Testes de Resiliência Operacional Digital

O DORA define uma obrigação de implementar um programa de teste de resiliência operacional digital proporcional e baseado no risco. O programa deve prever a execução de uma gama completa de testes apropriados por entidades externas e qualificadas, tais como avaliações e scans de vulnerabilidade, análises de *open source* e avaliações de segurança de rede.

Os sistemas e aplicações TIC críticas devem ser testados anualmente e certas entidades abrangidas são obrigadas a realizar "testes de penetração" conduzidos por ameaças avançadas uma vez de três em três anos.

o Partilha de Informação

As entidades abrangidas podem partilhar entre si informação sobre ameaças cibernéticas, desde que essa partilha de informações tenha por objetivo reforçar a resiliência operacional digital das entidades abrangidas, tenha lugar no seio de comunidades de confiança e seja realizado em conformidade com a legislação aplicável (e.g. proteção de dados, concorrência).

G. Risco de terceiros, *procurement*, *outsourcing*, e *contract lifecycle*

Para gerir o risco de terceiros relacionado com as TIC, o governo do *procurement* e de contratação com prestadores de serviços é um dos aspetos mais relevantes do DORA.

À semelhança do que tem ocorrido no *outsourcing* no setor financeiro, em especial no que respeita à contratação de serviços de computação em nuvem, (i) a aquisição de serviços e produtos de TIC; (ii) os requisitos para a cessação de contratos; e (iii) a imposição de diversas disposições contratuais obrigatórias que devem constar dos contratos com prestadores de serviços de TIC, são algumas das matérias reguladas pelo DORA.

No caso particular do fornecimento de serviços de TIC críticos ou importantes à Entidade Financeira, os deveres e obrigações do prestador de serviços previstos, a definir contratualmente, serão de maior exigência, encontrando-se o mesmo adstrito aos seguintes deveres e obrigações:

- aceitar a definição de metas de desempenho quantitativas e qualitativas rigorosas para os níveis de serviços acordados;
- adotar medidas corretivas;
- cumprir os períodos e as obrigações de notificação à entidade financeira quanto a serviços que possam ter impacto material na sua atividade;
- assegurar a execução e testagem de planos de contingência operacional;
- garantir a existência de medidas, ferramentas e políticas de segurança no domínio das TIC que assegurem um nível adequado de segurança na prestação de serviços;
- permitir a monitorização à sua atividade e instalações pela entidade financeira numa base contínua;
- assegurar a definição das estratégias de saída e respetiva transição para outro prestador de serviços de TIC.

Os prestadores de serviços de comunicação de dados devem manter, além disso, recursos adequados e dispor de equipamentos de salvaguarda e de restauração, a fim de poderem oferecer e manter os seus serviços em qualquer momento.

H. Quais as sanções para o incumprimento?

O DORA atribui competências e confere poderes de supervisão, investigação e sancionatórios às autoridades nacionais, incluindo a possibilidade de abranger a vertente penal.

As referidas autoridades poderão aplicar sanções e medidas corretivas em caso de violação do DORA, como por exemplo:

- exigir a cessação temporária ou permanente de qualquer prática contrária às disposições do regulamento e evitar a sua repetição, ou mesmo, abstenção;
- adotar medidas de natureza pecuniária que visem assegurar que as entidades financeiras continuem a cumprir os requisitos legais;
- emitir comunicações ao público que indiquem a identidade do infrator e a natureza da violação.

As autoridades competentes publicarão nos respetivos sítios *Web* oficiais qualquer decisão que imponha uma sanção administrativa não passível de recurso depois de o destinatário da sanção ter sido notificado dessa decisão.

I. Como podemos ajudar?

A Abreu Advogados tem ampla experiência no acompanhamento da administração de Instituições de Crédito em funções de supervisão e do seu sistema de controlo interno. Nesse âmbito, temos assessorado na definição de políticas e procedimentos relativos a todos o tipo de riscos, incluindo o risco operacional.

Para além disso, temos experiência na implementação do RGPD em instituições de crédito, na gestão do risco de *outsourcing* e na modelação de políticas de segurança de informação adaptadas aos mais exigentes standards internacionais, como a norma ISO 27001.

Temos uma equipa multidisciplinar que conjuga competências de Direito Financeiro e TMT e que é especializada em tecnologias emergentes, e que poderá auxiliar na implementação de soluções compatíveis com o DORA que se traduzam num valor acrescentado para o negócio dos clientes.

Este artigo foi escrito por Rafael Silva Teopisto, João Lupi e Diogo Pereira Duarte.

Contactos Abreu Advogados

Diogo Pereira Duarte – Sócio
diogo.p.duarte@abreuadvogados.com

João Lupi – Associado Sénior
joao.lupi@abreuadvogados.com

Rafael Silva Teopisto – Associado
rafael.s.teopisto@abreuadvogados.com