MORAIS LEITÃO
GALVÃO TELES, SOARES DA SILVA
& ASSOCIADOS

LEGAL ALERT

NOVAS REGRAS DE RESILIÊNCIA OPERACIONAL DIGITAL NO SETOR FINANCEIRO

DIGITAL OPERATIONAL RESILIENCE ACT – REGULAMENTO (UE) 2022/2554 DO PARLAMENTO EUROPEU E DO CONSELHO, DE 14 DE DEZEMBRO DE 2022

Entrou em vigor, no passado dia 16 de janeiro de 2023, o *Digital Operational Resilience Act* – o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, publicado no Jornal Oficial da União Europeia no dia 27 de dezembro de 2022 ("Regulamento DORA").

Atualmente, o risco associado a ataques informáticos e violações de dados não conhece limites quantificáveis, podendo ter consequências reputacionais, e não só, imprevisíveis e irreparáveis. Tal realidade respeita a empresas que operam transversalmente no setor financeiro, sejam eles incumbentes tradicionais (*e.g.*, bancos), *fintechs* ou prestadores de serviços tecnológicos.

O Regulamento DORA estabelece requisitos e regras uniformes, no que respeita à segurança dos sistemas de rede e de informação que apoiam os processos operacionais das entidades financeiras, relacionado com matérias de tecnologias da informação e comunicação (TIC), de forma a alcançar um maior nível de segurança no ciberespaço, em especial de resiliência operacional digital no setor financeiro.
O diploma será diretamente aplicável a partir de 17 de janeiro de 2025, data na qual as entidades abrangidas pelo referido terão de ter assegurado o cumprimento das obrigações regulatórias relativas à resiliência operacional digital.

Assim, um dos grandes projetos a desenvolver pelas entidades financeiras e pelos fornecedores de tecnologia ao setor financeiro será a reformulação de todo o modelo de governo das áreas tecnológicas e sistemas de segurança e de gestão de risco tecnológico.

Objetivos do Regulamento DORA

Com o objetivo de harmonizar as regras em torno da resiliência operacional e regulamentação da cibersegurança na União Europeia (UE), o Regulamento DORA estabelece requisitos uniformes para a segurança da rede e sistemas de informação de empresas que operam no setor financeiro, bem como de terceiros que prestam serviços críticos relacionados com TIC.

O Regulamento DORA cria um quadro regulamentar sobre a resiliência operacional digital através do qual todas as entidades precisam de garantir que podem **resistir, responder e recuperar de todos os tipos de perturbações relacionadas com as TIC** (As TIC são definidas de forma ampla para incluir serviços digitais e de dados prestados através de sistemas de TIC para um ou mais sistemas internos ou utilizadores externos, numa base contínua).

Âmbito de aplicação – quem está abrangido?

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*);

- VASP – *Virtual Asset Service Providers*/CASP – *Crypto Asset Service Provider* e emitentes de *tokens* referenciados a ativos (*stablecoins*), autorizados nos termos do Regulamento MiCA.

Empresas tecnológicas, prestadoras de serviços TIC às Entidades Financeiras.

A aplicação das normas previstas no diploma deverá ter em conta a dimensão e o perfil de risco de cada entidade abrangida, nomeadamente em relação à sua natureza, à sua escala e à complexidade dos serviços, das atividades e das operações.

Principais Obrigações – Entidades Financeiras

As obrigações aplicáveis às Entidades Financeiras dividem-se nas seguintes:

Governance

As Entidades Financeiras devem implementar um quadro de *governance* e controlo interno a fim de detetar rapidamente, mitigar e responder aos riscos associados às TIC, de modo a se conformarem com as disposições do Regulamento DORA.

Gestão de Risco

O órgão de gestão da Entidade Financeira deve ser responsável pela definição, pela aprovação e pela supervisão e estar continuamente responsável pela gestão de risco inerente às TIC, no quadro de gestão de risco global da entidade.

Nesta medida, elencamos os principais deveres e obrigações que daí decorrem:

- Os membros do órgão de gestão devem desenvolver e manter conhecimentos relativamente aos riscos das TIC;
- Deve ser implementado um sistema de gestão da segurança da informação, reconhecido internacionalmente;

- Deve haver manutenção de programas e avaliações de gestão de risco;
- Deve identificar-se a tolerância da entidade ao risco das TIC e manter-se um quadro abrangente de gestão desse risco;
- Deve existir uma monotorização e um controlo constante da segurança, dos funcionamentos dos sistemas e das ferramentas de TIC.

Reporte de Incidentes

O Regulamento DORA pretende instituir um mecanismo de reporte de incidentes, incluindo um processo de gestão para detetar, gerir e notificar incidentes relacionados com as TIC.
Os incidentes considerados "graves" deverão ser comunicados às autoridades competentes em prazos rigorosos.

Testes de resiliência

Como parte do quadro de gestão de risco associado às TIC, o diploma prevê que as Entidades Financeiras adotem um sistema robusto de testagem que abranja ferramentas, sistemas e processos TIC.

As ferramentas, sistemas e processos críticos devem ser testados anualmente, sendo que certas entidades são obrigadas a realizar "testes de penetração" de três em três anos.

Partilha de informação

O Regulamento DORA contém disposições que facilitam a partilha, entre Entidades Financeiras, de informação relativamente a ameaças cibernéticas, incluindo indicadores de compromisso, táticas, técnicas e procedimentos, alertas de cibersegurança, *inter alia*, com o intuito de reforçar a resiliência operacional digital das mesmas, desde que realizada em conformidade com a legislação aplicável (*e.g.*, proteção de dados, concorrência).

Riscos e Obrigações Contratuais – Empresas Tecnológicas

No escopo do risco respeitante às Empresas Tecnológicas, as matérias mais relevantes do Regulamento DORA dizem respeito a *procurement* e *outsorcing*.

O diploma vem regular, em concreto e entre outros, os requisitos para a cessação de contratos e a imposição de diversas disposições contratuais obrigatórias que devem constar nos contratos celebrados com prestadores de serviços TIC.

Quando estejam em causa serviços TIC críticos, as imposições contratuais e os deveres do prestador de serviços são mais exigentes, destacando-se:

- A definição de metas de desempenho quantitativas e qualitativas para os níveis de serviços acordados;
- A adoção de medidas corretivas;
- A execução e a testagem de planos de contingência operacional;
- A obrigação de notificação às Entidades Financeiras quanto a serviços que possam ter impacto material nas atividades dessas;
- A existência de medidas, ferramentas e políticas de segurança no domínio das TIC que assegurem segurança na prestação dos serviços;
- A permissão de monitorização à sua atividade e às suas instalações pelas Entidades Financeiras;
- A definição de estratégias de *exit* e respetiva transição para outro prestador de serviços.

Moving Forward…

Apesar de a aplicação do Regulamento estar prevista apenas para daqui a dois anos, prevemos que seja uma disrupção em face do panorama atual, dado que este **impõe novas obrigações**, para além de absorver algumas das regras já constantes nas Orientações da EBA em matéria de subcontratação (entre outras *guidelines* semelhantes, como as da ESMA), pelo que **será importante acautelar as mudanças atempadamente**.

David Silva Ramalho [+info]
Nicole Fortunato [+info]
Ashick Remetula [+info]