THE DIGITAL RESILIENCE DUTIES UNDER THE DORA REGULATION (REGULATION (EU) 2022/2554)

Isabella Silveira Lima

João Brotas Pinto

Working Paper N.º 05/2025
Setembro 2025

This paper can be downloaded without charge from the Governance Lab website at: www.governancelab.org.
The contents of this paper are the sole responsibility of their authors.

Keywords: DORA Regulation; digital resilience; operational risk; ICT risk management; financial services; regulatory compliance; cybersecurity; incident reporting; third-party risk; governance duties.

Palavras-chave: Regulamento DORA; resiliência digital; risco operacional; gestão de riscos das TIC; serviços financeiros; conformidade regulatória; cibersegurança; reporte de incidentes; risco de terceiros; deveres de governação.

THE DIGITAL RESILIENCE DUTIES UNDER THE DORA REGULATION (REGULATION (EU) 2022/2554)

Abstract

This paper analyses the paradigm shift in the provision of financial services brought about by digitalization and the resulting regulatory challenges. After a brief overview of the main normative sources on digital resilience, the study focuses on the DORA Regulation (Regulation (EU) 2022/2554). It examines DORA's structure, purpose, and scope of application, as well as key concepts such as operational risk, digital resilience, and Information and Communication Technologies (ICT). The core of the paper is dedicated to analyzing the digital resilience duties imposed on financial entities, namely obligations regarding ICT risk management, internal governance, incident reporting, operational resilience testing, and third-party risk management. Finally, a critical reflection is offered on the impact of DORA in strengthening the robustness and security of the financial sector in the digital age.

Resumo

O presente trabalho analisa a mudança de paradigma na prestação de serviços financeiros decorrente da digitalização e os novos desafios regulatórios que dela resultam. Após uma breve abordagem às principais fontes normativas sobre resiliência digital, centra-se no estudo do Regulamento DORA (Regulamento (UE) 2022/2554). São examinados a estrutura, a finalidade e o âmbito de aplicação do DORA, bem como conceitos fundamentais como risco operacional, resiliência digital e Tecnologias da Informação e Comunicação (TIC). O foco principal recai sobre a análise dos deveres de resiliência digital impostos às entidades financeiras, nomeadamente as obrigações de gestão de riscos das TIC, de governação interna, de reporte de incidentes, de realização de testes de resiliência operacional e de gestão de riscos de terceiros. Por fim, procede-se a uma reflexão crítica sobre o impacto do DORA no reforço da robustez e da segurança do setor financeiro na era digital.

ÍNDICE

I) INTRODUÇÃO: A MUDANÇA DE PARADIGMA NA PRESTAÇÃO DE SERVIÇOS FINANCEIROS 4

1. A TRANSIÇÃO PARA O DIGITAL E OS NOVOS DESAFIOS REGULATÓRIOS 4

2. FONTES NORMATIVAS SOBRE RESILIÊNCIA DIGITAL 5

II) O REGULAMENTO DORA: ESTRUTURA, FINALIDADE E ÂMBITO DE APLICAÇÃO 7

1. CONCEITOS FUNDAMENTAIS 7

1.1. RISCO OPERACIONAL 7

1.2. RESILIÊNCIA DIGITAL 7

1.3. TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO (TIC) 8

2. O REGIME JURÍDICO ESTABELECIDO PELO DORA 9

2.1. ESTRUTURA DO REGULAMENTO 9

2.2. FINALIDADE E ÂMBITO SUBJETIVO DO REGULAMENTO 10

2.3. O PRINCÍPIO DA PROPORCIONALIDADE NA APLICAÇÃO DO REGULAMENTO 11

2.4. LIMITES PRÁTICOS À EFETIVIDADE DO PRINCÍPIO DA PROPORCIONALIDADE 12

III) OS DEVERES DE RESILIÊNCIA DIGITAL NO ÂMBITO DO REGULAMENTO DORA 14

1. DEVERES DE GESTÃO DE RISCO DE TIC 14

1.1. IDENTIFICAÇÃO DO RISCO 14

1.2. AVALIAÇÃO DO RISCO 15

1.3. MITIGAÇÃO E MONITORIZAÇÃO DE AMEAÇAS ÀS TIC 15

2. DEVERES DE GOVERNAÇÃO DAS ENTIDADES REGULADAS 17

2.1. OBRIGAÇÃO DE IMPLANTAÇÃO DE UM QUADRO INTERNO DE GOVERNAÇÃO 17

2.2. A RESPONSABILIDADE DOS ADMINISTRADORES 18

2.3. ATUALIZAÇÃO CONTÍNUA DAS COMPETÊNCIAS DOS ADMINISTRADORES 20

3. DEVER DE GERIR, CLASSIFICAR E COMUNICAR INFORMAÇÕES SOBRE INCIDENTES RELACIONADOS COM AS TIC 20

3.1. GESTÃO E CLASSIFICAÇÃO DE INCIDENTES RELACIONADOS COM AS TIC 20

3.2. DEVER DE REPORTAR INCIDENTES RELACIONADOS COM AS TIC 22

4. DEVER DE REALIZAR TESTES DE RESILIÊNCIA OPERACIONAL DIGITAL 27

4.1. TESTES REGULARES DE AVALIAÇÃO DE RESILIÊNCIA 28

4.2. TESTES DE PENETRAÇÃO BASEADO EM AMEAÇAS (TLPT) 29

5. DEVER DE GERIR RISCOS DE TERCEIROS NO DOMÍNIO DAS TIC 30

5.1. FASE PRÉ-CONTRATUAL 32

5.2. DISPOSIÇÕES OBRIGATÓRIAS DOS CONTRATOS 33

IV) CONCLUSÃO 36

BIBLIOGRAFIA: 38

I) INTRODUÇÃO: A MUDANÇA DE PARADIGMA NA PRESTAÇÃO DE SERVIÇOS FINANCEIROS

1. A TRANSIÇÃO PARA O DIGITAL E OS NOVOS DESAFIOS REGULATÓRIOS

Neste trabalho, propomo-nos analisar os capítulos II, III, IV e da secção I do capítulo V do Regulamento DORA, que estabelecem os principais deveres de resiliência operacional digital aplicáveis às entidades financeiras. Para uma melhor compreensão destes deveres, começamos por apresentar os conceitos fundamentais que sustentam o diploma, bem como a sua estrutura, finalidade e âmbito de aplicação. Segue-se a exposição dos deveres específicos de resiliência operacional digital consagrados no regulamento.

A importância da resiliência financeira tornou-se particularmente evidente após as crises financeiras, que expuseram as vulnerabilidades estruturais ao nível da gestão, da fiscalização e da governação interna das instituições financeiras.

Hoje, os desafios são distintos, e decorrem da evolução das tecnologias da informação e comunicação (TIC), que levaram não apenas a uma alteração das expectativas dos consumidores quanto à forma de prestação dos serviços financeiros, mas também à automatização dos próprios processos internos das entidades, em busca de maior eficiência.

Esta transição tornou as entidades financeiras fortemente dependentes das novas tecnologias para a prestação dos serviços – uma dependência que, longe de ser negativa, faz surgir um conjunto de novas vulnerabilidades para as entidades financeiras, bem como para o sistema económico no seu todo. Entre os principais riscos, destaca-se a externalização das funções a terceiros prestadores de serviços TIC.

Perante estes novos riscos, tornou-se clara a necessidade de um regime que reforçasse a resiliência operacional digital em todo o setor financeiro. O Regulamento (UE) 2022/2554 (Regulamento DORA), inserido no pacote legislativo europeu para as finanças digitais, veio responder a essa necessidade. Até à sua aprovação, as regras existentes encontravam-se dispersas por diferentes instrumentos legislativos nacionais e europeus, dificultando respostas coerentes e transversais a todas as entidades do setor financeiro.

Com este diploma, passam a ser estabelecidos deveres claros em áreas fundamentais como a gestão do risco das TIC, tanto da própria entidade como dos terceiros externos

que lhe prestam serviços, a comunicação de incidentes e a realização de testes de resiliência operacional digital. Além disso, o diploma introduz uma novidade, ao alargar, pela primeira vez, o perímetro de supervisão dos reguladores financeiros às empresas prestadoras de serviços de TIC.

2. FONTES NORMATIVAS SOBRE RESILIÊNCIA DIGITAL

A regulamentação da resiliência operacional digital no setor financeiro europeu integra o Pacote de Finanças Digitais[1], iniciativa da União Europeia para promover a inovação segura e fortalecer a estabilidade do mercado. Neste contexto, destaca-se o Regulamento (UE) 2022/2554 (DORA), que estabelece um quadro setorial específico para a gestão dos riscos de TIC, funcionando como regime especial face à Diretiva NIS (UE) 2016/1148.

Além do DORA, o pacote legislativo inclui instrumentos complementares como o Regulamento (UE) 2023/1114 (MiCA), relativo aos criptoativos, e o Regulamento (UE) 2022/858, que cria um regime-piloto para infraestruturas de mercado baseadas em tecnologia de registo distribuído (DLT Pilot Regime).

As fontes normativas sobre resiliência digital estruturam-se principalmente em dois níveis:

– Medidas de Nível 1: Regulamento (UE) 2022/2554 (DORA), que define as obrigações gerais de governação, gestão de riscos e continuidade operacional.

– Medidas de Nível 2: Composto por regulamentos delegados que complementam o DORA, especificando aspetos técnicos:

- Regulamento (UE) 2024/2956: Trata da resiliência digital e da classificação de incidentes tecnológicos.
- Regulamento (UE) 2024/1772: Define critérios para a classificação de incidentes TIC e requisitos de relatórios.
- Regulamento (UE) 2024/1773: Regula os arranjos contratuais com fornecedores de serviços TIC críticos.
- Regulamento (UE) 2024/1774: Estabelece diretrizes para a gestão de riscos TIC e um *framework* simplificado de gestão.

[1] RODRIGUES, André Alfar, 2023, "*Manual de Inovação Financeira – Uma introdução ao universo das Criptomoedas e da Blockchain*", pp. 167-168.

- Regulamento (UE) 2025/532: Estabelece normas técnicas regulamentares em subcontratação.

Para além destes, importa ressaltar as medidas de nível 3, que fornecem orientações adicionais sobre a aplicação prática das medidas de níveis 1 e 2. Embora não tenham caráter vinculativo, essas diretrizes, emitidas pelas autoridades de supervisão ajudam as organizações a implementar as exigências de resiliência operacional digital, alinhando-se às melhores práticas do setor.

II) O REGULAMENTO DORA: ESTRUTURA, FINALIDADE E ÂMBITO DE APLICAÇÃO

1. CONCEITOS FUNDAMENTAIS

1.1. RISCO OPERACIONAL

O setor financeiro está exposto a diversos tipos de risco, como o risco de crédito, risco de mercado, risco de liquidez e risco operacional. Este último ganha especial relevância no âmbito do Regulamento DORA, que tem como objetivo mitigar os riscos operacionais relacionados com as tecnologias da informação e comunicação (TIC) de modo a promover a chamada resiliência digital[2].

O Risco operacional foi definido pelo Comité de Basileia para Supervisão Bancária como "o risco de perda resultante de processos internos inadequados ou falhos, pessoas e sistemas, ou de eventos externos"[3]. Trata-se, portanto, de riscos tanto decorrentes da própria atividade das instituições financeiras quanto de fatores externos. Entre os exemplos possíveis estão: perdas provocadas por falhas de TIC, erros em transações ou eventos externos como inundações, terramotos ou incêndios[4].

Nesse contexto, é fundamental uma gestão eficaz do risco operacional, tanto para prevenir perdas inesperadas como para mitigar os danos quando eventos adversos forem inevitáveis.

1.2. RESILIÊNCIA DIGITAL

A resiliência, no campo da física, é a propriedade de um corpo de recuperar a sua forma original após sofrer choque ou deformação. Figuradamente, refere-se à capacidade de superar adversidades.

O Regulamento DORA, porém, define a resiliência operacional digital como a capacidade das entidades financeiras para criar, assegurar e reavaliar a sua integridade e fiabilidade operacionais, garantindo, inclusive com o apoio de terceiros, a continuidade e a segurança dos serviços financeiros, em situações de perturbação[5].

---

[2] Regulamento DORA, Considerandos (5) e (12).
[3] Comité de Supervisão Bancária de Basileia, Acordo de Capital de Basileia II, 2001, Documento Complementar "Risco Operacional", p. 2.
[4] KARAM, Elias/PLANCHET, Frédéric, 2012, "Operational risks in financial sectors", p. 2.
[5] Regulamento DORA, Artigo 3.º, (1).

Ao contrário da conceção comum, que se limita à capacidade de resistir ao impacto e recuperar o estado anterior, o conceito do DORA postula comportamentos proativos, contínuos e integrados, exigindo a capacidade de prevenir, resistir, adaptar-se e recuperar-se. Essa abordagem aproxima-se do conceito de antifragilidade, desenvolvido por Nassim Taleb, segundo o qual alguns sistemas não apenas resistem ao choque, mas melhoram com este[6]. Esta leitura torna-se ainda mais relevante ao considerar que o DORA não se limita a impor medidas defensivas, mas obriga a uma dinâmica de melhoria contínua, como veremos melhor nos próximos capítulos. A regulação, portanto, estimula um comportamento antifrágil, mesmo que não o nomeie como tal.

Complementarmente, o DORA centra-se nas tecnologias da informação e comunicação (TIC), cuja gestão eficaz é essencial para alcançar esse nível de resiliência operacional digital.

1.3. TECNOLOGIAS DA INFORMAÇÃO E COMUNICAÇÃO (TIC)

As tecnologias da informação e comunicação (TIC) constituem um conceito central no DORA. Englobam os sistemas, infraestruturas, aplicações e processos tecnológicos que sustentam o funcionamento digital das entidades financeiras. Incluem desde redes e servidores até *softwares*, plataformas digitais, sistemas de armazenamento, gestão de dados, cibersegurança, e comunicações internas e externas — tudo o que permite o processamento e a troca de informação digital.

O DORA reconhece que a crescente dependência das TIC expõe o setor financeiro a novos riscos operacionais, frequentemente interligados, sistémicos e de origem externa (como ciberataques, falhas de *software* ou interrupções nos serviços de prestadores terceiros). Assim, um dos seus objetivos centrais é mitigar os riscos associados às TIC, assegurando que as instituições mantêm um nível elevado de resiliência operacional digital, mesmo perante falhas tecnológicas graves[7].

Em suma, o Regulamento DORA visa não apenas responder aos desafios impostos pelas TIC, mas também estabelecer um modelo de resiliência contínua, dinâmico e adaptável, essencial para a estabilidade e confiança do sistema financeiro num ambiente cada vez mais digitalizado e vulnerável.

---

[6] TALEB, Nassim Nicholas, 2014, *Antifragile: Things That Gain from Disorder.* Taleb distingue três categorias de sistemas: o frágil, que se quebra com o choque; o resiliente, que resiste e retorna ao estado anterior; e o antifrágil, que se fortalece com o impacto, evoluindo a partir da perturbação.

[7] Regulamento DORA, Considerandos (1) e (2).

O risco associado às TIC é definido pelo Regulamento DORA como sendo "qualquer circunstância razoavelmente identificável relacionada com a utilização de sistemas de rede e informação que, caso se materialize, pode comprometer a segurança dos sistemas de rede e informação, de qualquer instrumento ou processo dependente de tecnologia, do funcionamento e da execução de processos ou da prestação de serviços, causando efeitos adversos no ambiente digital ou físico"[8].

Dessa forma, o risco associado às TIC configura-se como uma subespécie do risco operacional, nos termos já referidos, ao incidir sobre falhas, vulnerabilidades ou ameaças relacionadas com os ativos tecnológicos das instituições financeiras. Este tipo de risco possui a particularidade de se propagar com elevada rapidez e amplitude, quando comparado com outros riscos operacionais, sendo potencialmente gerador de efeitos sistémicos que podem comprometer a estabilidade de todo o sistema financeiro[9].

A sua autonomização conceitual no Regulamento DORA não exclui a sua natureza operacional, mas antes evidencia a sua relevância e complexidade crescentes, exigindo uma abordagem regulatória distinta, alinhada com a transformação digital do setor e com os riscos sistémicos dela decorrentes.

2. O REGIME JURÍDICO ESTABELECIDO PELO DORA

2.1. ESTRUTURA DO REGULAMENTO

O Regulamento (UE) 2022/2554 (DORA) estrutura-se em nove capítulos, estabelecendo de forma sistemática o quadro jurídico da resiliência operacional digital no setor financeiro. Após as disposições gerais (Cap. I), os capítulos seguintes centram-se nos principais deveres impostos às entidades reguladas: governação e gestão de risco das TIC (Cap. II), reporte de incidentes (Cap. III), testes de resiliência operacional (Cap. IV) e gestão dos riscos decorrentes de prestadores terceiros (Cap. V) — deveres estes que constituem o núcleo do presente trabalho. Os capítulos VI a IX complementam este regime, abordando a partilha de informação, os mecanismos de supervisão, o poder regulamentar da Comissão e as disposições transitórias. Esta estrutura normativa orientará a análise desenvolvida nos capítulos seguintes, com especial enfoque nos deveres concretos impostos às instituições financeiras para garantir a resiliência digital no novo paradigma tecnológico.

[8] Regulamento DORA, artigo 3.º, (5).
[9] DUGGAN, Derek, 2024, "The impact of the Digital Operational Resilience Act on financial market infrastructures in Europe", p. 345.

2.2. FINALIDADE E ÂMBITO SUBJETIVO DO REGULAMENTO

Na era digital em que vivemos, o Regulamento (UE) 2022/2554 (DORA) foi criado com o objetivo de harmonizar, de maneira coerente, as regras relativas à resiliência operacional digital e à segurança no domínio das tecnologias da informação e comunicação (TIC). Pretende-se, com isso, colmatar lacunas e eliminar sobreposições existentes, além de reforçar a supervisão das autoridades competentes[10], permitindo-lhes supervisionar de forma eficaz a gestão do risco associado às TIC no setor financeiro. O objetivo final é proteger a integridade e a eficiência do mercado interno, assegurando o seu funcionamento ordenado.[11].

O Regulamento DORA aplica-se, em geral, às entidades financeiras sujeitas à supervisão prudencial e, em alguns aspetos, aos seus terceiros prestadores de serviços de TIC[12]. O artigo 2.º define claramente o seu âmbito subjetivo de aplicação[13], abrangendo uma vasta gama de instituições financeiras e prestadores de serviços essenciais, incluindo instituições de crédito, empresas de investimento, plataformas de negociação, prestadores de serviços de criptoativos, entre outros.

No entanto, o artigo 2º, n.º 3 do regulamento também estabelece uma série de exceções, definindo determinadas entidades e categorias que ficam fora do seu alcance. As razões por trás dessas exclusões são diversas e refletem tanto a natureza e complexidade das entidades excluídas quanto o objetivo do regulamento de focar as suas exigências nas entidades com maior impacto sistémico no setor financeiro.

Importa destacar a exclusão das empresas de auditoria, que, embora tenham grande impacto no setor financeiro, não são consideradas entidades financeiras propriamente ditas. Por não estarem sujeitas à supervisão das autoridades financeiras competentes, estas empresas ficam fora do escopo do Regulamento DORA[14].

Além disso, entidades de menor dimensão, como mediadores de seguros a título acessório que sejam microempresas e planos de pensões com menos de 15 membros, são excluídas, uma vez que não representam riscos significativos no que diz respeito à

---

[10] BUTTIGIEG, Chistopher P./ZIMMERMANN, Beatriz Brunelli, 2024, "The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision", p. 4.
[11] Regulamento DORA, Considerandos (8) a (10).
[12] CARRILLO, Elena F. Pérez, 2023, "Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform", p. 1146.
[13] Regulamento DORA, Artigo 2.º, n.º 1.
[14] CLAUSMEIER, Dirk, 2023, "Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)", p. 82.

resiliência operacional digital, dado o tamanho e a simplicidade das suas infraestruturas. O Regulamento DORA, com seus requisitos complexos e exigentes, poderia ser desproporcional para estas entidades[15].

Por fim, o DORA concentra-se nas instituições de maior risco sistémico, como instituições de crédito, plataformas de negociação e outros agentes financeiros cujas falhas poderiam comprometer a estabilidade do sistema financeiro. As exclusões, portanto, permitem que o regulamento seja direcionado a entidades com maior dependência tecnológica e impacto potencial, assegurando que a regulação seja proporcional ao risco apresentado por cada organização.

2.3. O PRINCÍPIO DA PROPORCIONALIDADE NA APLICAÇÃO DO REGULAMENTO

O princípio da proporcionalidade é um conceito fundamental tanto no âmbito do direito administrativo quanto na regulação do setor financeiro[16]. O princípio da proporcionalidade, conforme destacado por alguns especialistas, determina que a regulação e a supervisão devem ser adequadas, necessárias e proporcionais ao contexto da entidade, respeitando a sua dimensão, complexidade e perfil de risco.

Em 2011, a Autoridade Bancária Europeia (EBA) reforçou a aplicação do princípio da proporcionalidade no setor financeiro nas suas orientações sobre Governo Interno (GL 44), segundo as quais as instituições abrangidas poderiam demonstrar de que forma a natureza, a escala e a complexidade das suas atividades permitiam alcançar o resultado visado por essas orientações[17]. Esta posição evidencia a relevância fundamental do princípio da proporcionalidade na regulação financeira.

Deste modo, ao consagrar o princípio da proporcionalidade no seu artigo 4.º, o Regulamento DORA visa assegurar uma supervisão que seja simultaneamente eficaz e ajustada à realidade concreta de cada entidade. Parte-se do reconhecimento de que "*one size does not fit all*", ou seja, que as exigências regulatórias devem ser calibradas de acordo com a dimensão, complexidade, perfil de risco e natureza das atividades da entidade em causa. Este princípio visa garantir que as exigências do regulamento sejam proporcionais à realidade de cada instituição, evitando sobrecargas desnecessárias para

[15] Regulamento DORA, Considerando (39), e artigo 2.º, n.º 3.
[16] Está previsto no artigo 266º da Constituição da República Portuguesa como um dos princípios fundamentais que orientam a Administração Pública, sendo este densificado pelo artigo 7.º do Código de Procedimento Administrativo. Para maiores desenvolvimentos, RAMALHO, Inês Palma, 2021, "O princípio da proporcionalidade no sector financeiro", p. 11.
[17] RAMALHO, Inês Palma, 2021, "O princípio da proporcionalidade no sector financeiro", p. 12.

entidades menores ou com menos risco associado enquanto aumenta a eficiência no alcance dos objetivos propostos pelo Regulamento[18].

O artigo 4.º estabelece que, nos capítulos II, III, IV e V, secção I, a aplicação das regras será feita com base nessas variáveis, permitindo que a regulação seja flexível e adaptada às diferentes realidades do setor financeiro. Para o princípio funcionar de forma adequada, é necessário que as entidades reguladoras possuam uma "fotografia" detalhada das instituições financeiras sob a sua supervisão, considerando a natureza, a escala e a complexidade das suas operações. A supervisão eficaz deve partir do reconhecimento das diferentes realidades de cada instituição, levando em conta fatores como geografia, fase de desenvolvimento e tipo de atividades desenvolvidas[19].

2.4. LIMITES PRÁTICOS À EFETIVIDADE DO PRINCÍPIO DA PROPORCIONALIDADE

Apesar do reconhecimento formal do princípio da proporcionalidade, a aplicação concreta deste no contexto do DORA revela limitações substanciais. O regulamento classifica genericamente as entidades entre micro, pequenas, médias e grandes, mas impõe, na prática, um conjunto de obrigações bastante homogéneo, com diferenças limitadas. As exceções previstas abrangem, em sua maioria, apenas microentidades ou pequenas entidades de determinados tipos específicos — como empresas de investimento ou instituições de realização de planos de pensões profissionais — conforme disposto no artigo 16.º. Assim, entidades de pequeno e médio dimensão continuam sujeitas à quase totalidade das exigências técnicas e organizacionais aplicáveis a instituições de grande dimensão, sem um ajustamento proporcional significativo.

Além disso, o DORA impõe uma quantidade extensa e altamente detalhada de obrigações normativas, que incluem desde requisitos de gestão de risco das TIC e classificação de incidentes, até a realização de testes de penetração baseados em ameaças (TLPT). Cumprir tais deveres pressupõe a existência de quadros técnicos especializados, o que, para pequenas entidades, implica a necessidade de contratação de pessoal adicional com competências em cibersegurança, gestão de riscos e conformidade regulatória.

---

[18] BIERECKI, Dominik, 2024, "Principle of Proportionality in the Application of the Digital Operational Resilience Act
(DORA)", p. 9.
[19] RAMALHO, Inês Palma, 2021, "O princípio da proporcionalidade no sector financeiro", p. 13.

A complexidade técnica do quadro normativo é agravada pelos regulamentos complementares de Nível 2. Por exemplo, o Regulamento Delegado (UE) 2024/1772 especifica critérios rigorosos para classificação de incidentes e ciberameaças; o Regulamento Delegado (UE) 2024/1774 define instrumentos técnicos exigentes para a gestão de risco TIC. Esses instrumentos exigem conhecimento técnico-jurídico elevado e familiaridade com padrões internacionais de cibersegurança, dificultando a implementação por entidades com estruturas enxutas.

Tal complexidade se manifesta de forma ainda mais aguda no Regulamento de Execução (UE) 2024/2956, que estabelece modelos normalizados para o registo de informações sobre contratos com prestadores de serviços de TIC. Estes modelos devem ser preenchidos com base em códigos e chaves relacionais, exigindo conhecimento específico em estruturas de dados, interoperabilidade documental e taxonomias digitais. Essa exigência representa uma barreira técnica significativa para instituições menores, que dificilmente possuem os recursos humanos ou tecnológicos necessários para estruturar e manter esse tipo de base de dados conforme o padrão regulatório.

Essa configuração normativa, apesar de invocar uma lógica baseada no risco, tende, na prática, a produzir um efeito oposto ao pretendido: um movimento de uniformização das exigências, independentemente da natureza ou dimensão da entidade. O resultado provável é a consolidação de um modelo de conformidade essencialmente formal, no qual os operadores económicos se preocupam mais em demonstrar documentalmente o cumprimento das exigências do regulamento do que em alcançar uma efetiva resiliência operacional. Em vez de incentivar melhorias estruturais adaptadas à realidade concreta de cada instituição, o regime atual pode conduzir a uma abordagem defensiva e burocrática, desvirtuando a função estratégica do princípio da proporcionalidade como elemento de eficiência regulatória.

III) OS DEVERES DE RESILIÊNCIA DIGITAL NO ÂMBITO DO REGULAMENTO DORA

1. DEVERES DE GESTÃO DE RISCO DE TIC

A gestão do risco associado às TIC exige um processo contínuo, estruturado e integrado de identificação, avaliação, mitigação, reporte e monitorização de ameaças tecnológicas. Mais do que mera prevenção de falhas, este processo visa melhorar os sistemas internos, apoiar decisões estratégicas, reduzir custos decorrentes de disrupções inesperadas e oferecer respostas coordenadas aos diferentes níveis de risco digital. Ao centrar-se na proteção e robustez das infraestruturas tecnológicas, a gestão do risco das TIC torna-se o pilar essencial da resiliência operacional digital exigida pelo DORA[20]. Trata-se de um dever com conteúdo multifacetado, que abrange e desdobra diversos outros deveres. Para fins didáticos, iremos dividi-los em subpontos, seguindo uma ordem lógica.

1.1. IDENTIFICAÇÃO DO RISCO

Nos artigos 5.º a 16.º do Regulamento DORA, são estabelecidos os deveres relativos à gestão do risco associado às TIC, complementado pelo Regulamento Delegado (UE) 2024/1774. Estes diplomas impõem que as entidades financeiras devem implementar um quadro robusto de gestão de risco[21] que permita uma resposta rápida e eficiente a eventuais riscos associados às TIC[22].

Integra-se neste dever, a gestão dos ativos de TIC[23], definidos como "ativos de programas informáticos ou de equipamentos informáticos nos sistemas de rede e informação utilizados pela entidade financeira"[24]. A sua gestão é de suma importância pois estes constituem o substrato técnico sobre o qual assenta toda a operação digital. A

[20] O AI Act (Regulamento (UE) 2024/1689) adota uma técnica regulatória muito próxima da que foi seguida no Regulamento DORA, ao exigir a classificação prévia dos sistemas de IA consoante o grau de risco e, no caso dos considerados de risco elevado, a implementação de mecanismos estruturados de gestão de risco e de governação de dados. Em ambos os casos, observa-se uma arquitetura normativa orientada pela proporcionalidade e pela adaptação dos deveres ao grau de criticidade dos sistemas, o que evidencia uma opção clara do legislador europeu por uma abordagem transversal e coerente na regulação dos riscos tecnológicos.
[21] THUAMA, Rois NI/COSTIGAN, Sean S., 2023, "DORA - Understanding the New Regulatory Framework on Digital Operational Resilience", p. 2.
[22] Artigo 5.º, n.º 1 do Regulamento DORA e artigo 2.º do Regulamento Delegado (UE) 2024/1774.
[23] Regulamento Delegado (UE) 2024/1774, artigos 4.º e ss.
[24] Regulamento DORA, artigo 3.º, (7).

sua má gestão pode comprometer a resiliência operacional, a integridade dos dados, a continuidade dos serviços e a própria segurança cibernética.

O referido quadro de gestão de risco deve começar por identificar, classificar e documentar adequadamente os riscos associados às TIC. Este processo inclui a avaliação de ciberameaças e vulnerabilidades, com especial atenção aos riscos provenientes de terceiros prestadores de serviços. Exige-se, por isso, que os administradores responsáveis pela implementação do quadro tenham uma visão ampla de todos os riscos relevantes, devendo aplicar os melhores esforços e a diligência necessária para a sua identificação, nomeadamente através da consulta a especialistas na área.

O artigo 16.º do Regulamento DORA estabelece um quadro simplificado de gestão de risco para as entidades de pequena dimensão como uma forma de assegurar que essas entidades, que não se enquadram nas disposições gerais do regulamento, também implementem práticas mínimas de gestão de risco. Embora não se aplicam as disposições gerais do regulamento a essas entidades, elas devem manter um sistema documentado de gestão de risco, monitorando a segurança e o funcionamento dos sistemas TIC, protegendo infraestruturas críticas e garantindo a continuidade das atividades essenciais.

1.2. AVALIAÇÃO DO RISCO

O quadro de gestão de risco deverá ainda indicar o nível de tolerância ao risco associado às TIC, em conformidade com a apetência para o risco da entidade financeira, assim como analisar a sua tolerância ao impacto de eventuais perturbações nos sistemas[25].

A avaliação do risco deve ser realizada com base numa metodologia específica, definida pela própria entidade, que identifique obrigatoriamente as vulnerabilidades e ameaças que afetem, ou possam vir a afetar, as funções operacionais suportadas, os sistemas de TIC e os ativos de TIC que lhes dão suporte. Essa metodologia deve ainda prever a utilização de indicadores — quantitativos ou qualitativos — capazes de medir o impacto e a probabilidade dessas vulnerabilidades e ameaças se concretizarem.

1.3. MITIGAÇÃO E MONITORIZAÇÃO DE AMEAÇAS ÀS TIC

O quadro de gestão de risco deve contemplar estratégias, políticas, procedimentos e ferramentas adequadas para garantir a proteção integral dos ativos de informação[26] e das

[25] Regulamento DORA, artigo 6.º, n.º 8, al. b) e Regulamento Delegado 2024/1774, Artigo 3.º, al. b).
[26] Definido no artigo 3.º, (7) do Regulamento DORA como "um conjunto de informações, tangível ou intangível, que deve ser protegido".

infraestruturas de TIC, assegurando assim a resiliência digital da organização no contexto do novo paradigma regulatório.

O procedimento para o tratamento do risco associado às TIC exige que a entidade financeira implemente medidas que garantam que os riscos identificados sejam mantidos dentro dos níveis de tolerância estabelecidos. Após a implementação dessas medidas, alguns riscos residuais podem permanecer, e a entidade deve identificá-los e justificar sua aceitação quando estes ultrapassam os níveis de tolerância. A aceitação desses riscos deve ser documentada em um inventário, com revisões anuais para garantir que as razões para a sua aceitação ainda sejam válidas e que as medidas de mitigação sejam adequadas[27].

A monitorização contínua é essencial para detetar alterações no panorama de riscos e ciberameaças, tanto internas quanto externas. A entidade deve estar atenta a quaisquer mudanças que possam afetar seu perfil de risco, garantindo uma resposta rápida. Além disso, qualquer alteração na estratégia empresarial ou de resiliência operacional digital deve ser considerada na gestão de riscos, para assegurar que as medidas adotadas estejam sempre alinhadas com os objetivos da organização.

O Regulamento DORA estabelece que as entidades financeiras devem adotar mecanismos eficazes para a identificação rápida de atividades anómalas em seus sistemas de TIC[28]. Para isso, é necessário implementar uma política robusta de continuidade de negócios no âmbito digital. Além disso, como parte integrante da gestão de riscos operacionais, exige-se a criação de procedimentos claros de *backup* e estratégias de recuperação de dados, visando reduzir ao máximo o tempo de indisponibilidade e minimizar perdas. Também se espera que essas entidades tenham planos de comunicação bem definidos para situações de crise[29]. Embora o regulamento seja detalhado em seus requisitos, a aplicação prática dependerá do perfil de risco específico de cada instituição, tornando essencial a orientação técnica das Autoridades Europeias de Supervisão para uma implementação eficiente[30].

Por fim, é crucial monitorizar a eficácia das medidas de mitigação de risco, avaliando se os níveis de tolerância ao risco são respeitados e se ações corretivas são necessárias quando as medidas não são eficazes.

---

[27] Regulamento Delegado 2024/1774, Artigo 3.º, al. d), n.º. iv).
[28] Regulamento DORA, artigo 9.º e 10.º.
[29] Regulamento DORA, artigo 11.º.
[30] CLAUSMEIER, Dirk, 2023, "Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)", p. 84.

2. DEVERES DE GOVERNAÇÃO DAS ENTIDADES REGULADAS

2.1. OBRIGAÇÃO DE IMPLANTAÇÃO DE UM QUADRO INTERNO DE GOVERNAÇÃO

O artigo 5.º do Regulamento DORA inaugura, logo no seu n.º 1, uma exigência fulcral para a arquitetura interna das entidades financeiras: a constituição de um quadro de governação e controlo que assegure uma gestão eficaz e prudente do risco tecnológico associado às TIC.

Trata-se de uma obrigação que reflete uma mudança paradigmática na cultura regulatória da União Europeia. Se antes o foco recaía quase exclusivamente sobre parâmetros prudenciais clássicos — como solvabilidade, liquidez e risco de crédito — agora exige-se das entidades uma abordagem holística e transversal da resiliência operacional, onde o risco tecnológico é elevado à categoria de risco sistémico, comparável aos riscos financeiros tradicionais. Nesse sentido, há quem fale em "*cyber* risco sistémico", reconhecendo o potencial disruptivo que incidentes tecnológicos de larga escala podem ter sobre o funcionamento do sistema financeiro como um todo[31].

Concretamente, tal obrigação implica a criação de funções e unidades organizacionais dedicadas à gestão do risco de TIC, com competências bem delimitadas e hierarquias de reporte formalizadas. Isto inclui, nomeadamente, a obrigação de criar um cargo responsável por monitorizar os acordos celebrados com terceiros prestadores de serviços de TIC ou, alternativamente, a designação de um membro da direção de topo incumbido de fiscalizar a exposição ao risco conexo e a documentação pertinente[32].

Impõe-se, ainda, a segregação de funções críticas, em linha com os princípios de controlo interno já consagrados na supervisão prudencial para os bancos (como os Princípios de *Corporate Governance* emitidos pelo Comité de Basileia[33]), bem como, a existência de canais internos de comunicação e coordenação que assegurem uma resposta célere e eficiente perante incidentes tecnológicos.

A existência de processos claros e bem definidos para lidar com ameaças cibernéticas, bem como a criação de um comité dedicado ao risco no quadro de governação da empresa, pode contribuir de forma significativa para a redução dos riscos de ciberataques. Uma

[31] CARRILLO, Elena F. Pérez, 2023, "Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform", p. 1138.
[32] Regulamento DORA, artigo 5.º, n.º 3.
[33] Basel Committee on Banking Supervision Guidelines: corporate governance principle for banks, July 2015.

proposta particularmente relevante seria a instituição de um comité de risco segregado, composto por especialistas em risco cibernético, com a função de apoiar as decisões dos administradores e reforçar a capacidade da entidade em antecipar, avaliar e responder a incidentes tecnológicos[34].

A clareza na distribuição de responsabilidades e a capacidade de atuação coordenada entre as várias funções ligadas às TIC não constituem assim, uma exigência meramente formal, mas uma condição estrutural para a resiliência digital da instituição. Essa resiliência, contudo, não deve ser entendida apenas como o cumprimento de obrigações regulatórias, mas como um objetivo estratégico e cultural de longo prazo. O caminho para alcançá-la começa na definição da visão, dos valores e das prioridades da organização, refletindo o seu propósito corporativo. Cabe, por isso, ao órgão de gestão estabelecer os pilares que sustentam essa cultura de resiliência operacional, através da aprovação de políticas, da alocação de recursos adequados e da promoção de uma liderança ativa e consciente ("*tone from the top*")[35].

Por fim, importa destacar que a estrutura de governação interna deve ser concebida de modo a permitir ajustes rápidos diante das mudanças regulatórias e tecnológicas, assegurando a preservação da integridade operacional da entidade[36]. O cumprimento desta obrigação não se esgota na criação do quadro de governação, devendo este ser continuamente mantido, atualizado e adaptado, em consonância com os riscos emergentes e a constante evolução do panorama tecnológico. Neste contexto, a governação assume um papel central, servindo como eixo estruturante da resiliência digital e elemento catalisador de uma mudança cultural que permita superar a fragmentação interna e integrar efetivamente a gestão do risco de TIC em toda a organização[37].

2.2. A RESPONSABILIDADE DOS ADMINISTRADORES

Nesse contexto de gestão de riscos das TIC, o órgão de administração da entidade financeira tem um papel fundamental, uma vez que é responsável por aprovar, fiscalizar e assegurar a aplicação de todas as disposições relacionadas com o anteriormente referido quadro de gestão do risco associado às TIC[38].

---

[34] CORTEZ, Elif Kiesow/DEKKER, Martijn, 2022, "A Corporate Governance Approach to Cybersecurity Risk Disclosure", p. 42.
[35] REIS, Laura/TEIXEIRA, Maria Emília, 2022, "A transformação digital na banca e a crescente relevância da resiliência operacional", p. 206.
[36] ESENER, Esen, 2024, "Adaptive Governance for Blockchain Networks", pp. 77-78.
[37] BEGOZZI, Valerio/OLDANI, Matteo/TERRIZZANO, Francesca, 2023, "The growing importance of digital risk & governance", p. 27.
[38] Regulamento DORA, artigo 5.º, n.º 2.

É de suma importância que o órgão de administração garanta a utilização de sistemas, protocolos e ferramentas de TIC adequados, capazes de lidar com a dimensão das operações da entidade financeira e de responder adequadamente a picos de transações ou situações adversas. Estes devem ser fiáveis e resilientes, com capacidade suficiente para tratar dados de forma eficiente, assegurando a continuidade dos serviços mesmo em momentos de grande pressão ou falhas tecnológicas[39].

O Regulamento DORA atribui ao órgão de administração a responsabilidade última pela gestão do risco associado às TIC da entidade financeira[40], cabendo a estes um dever contínuo de acompanhamento e revisão das políticas estabelecidas em matéria de resiliência operacional digital[41].

Esta solução resulta do tradicional dever de diligência imposto aos administradores, comum a diversos ordenamentos jurídicos. No ordenamento jurídico inglês, é abordado no *Companies Act* de 2006, secção 174; nos Estados Unidos, é tratado largamente nos precedentes judiciais[42]; e em França, está previsto no artigo L225-251 do *Code de commerce*. No ordenamento jurídico português, esse dever está previsto no artigo 64.º do Código das Sociedades Comerciais, sendo que a sua violação pode dar origem à responsabilidade civil dos administradores, nos termos do artigo 72.º/1, segundo o qual a culpa é presumida.

A responsabilização expressa dos administradores prevista no Regulamento DORA revela-se particularmente relevante, na medida em que reforça e harmoniza deveres já consagrados nos ordenamentos jurídicos nacionais, promovendo o cumprimento reforçado das políticas e dos procedimentos de gestão do risco associado às TIC, tal como densificados pelo Regulamento Delegado (UE) 2024/1774[43], por parte dos administradores.

---

[39] Regulamento DORA, artigo 7.º.

[40] A responsabilidade atribuída ao órgão de administração na governação das instituições financeiras não é uma inovação do DORA. Já nas "Orientações da EBA sobre a governação interna", de 2021, se destacava que compete a este órgão compreender a estrutura organizacional e os riscos operacionais específicos da entidade, bem como assegurar o cumprimento do respetivo quadro de gestão de riscos (parágrafo 71 e ss.).

[41] Nos termos do artigo 8.º, n.º 1 e 2 *in fine* do Regulamento DORA, as entidades financeiras devem rever periodicamente, e pelo menos uma vez por ano os cenários de risco suscetíveis de as afetar e a adequação da classificação das funções operacionais apoiadas pelas TIC e de toda a documentação pertinente.

[42] THUAMA, Rois NI/COSTIGAN, Sean S., 2023, "DORA - Understanding the New Regulatory Framework on Digital Operational Resilience", p. 2.

[43] Para maiores desenvolvimentos, conferir o artigo 3.º e ss. do Regulamento Delegado (UE) 2024/1774.

2.3.ATUALIZAÇÃO CONTÍNUA DAS COMPETÊNCIAS DOS ADMINISTRADORES

O Regulamento DORA impõe às entidades reguladas o dever de assegurar que os membros do órgão de administração atualizem ativamente os seus conhecimentos e competências relativamente ao risco associado às TIC. Trata-se de um reforço da exigência de idoneidade técnica, que vai além da tradicional avaliação da honorabilidade e da experiência dos administradores, colocando a formação contínua como elemento estruturante da resiliência operacional.

Para cumprir esta obrigação, os administradores devem não apenas compreender os riscos tecnológicos emergentes, mas ser capazes de os avaliar criticamente e tomar decisões informadas sobre a sua gestão. O regulamento especifica, inclusive, a necessidade de frequência regular de formações específicas, ajustadas ao perfil e grau de exposição da instituição ao risco TIC[44].

Esta previsão evidencia que a governação digital não pode ser delegada exclusivamente a equipas técnicas, devendo estar integradamente incorporada na atuação da alta administração. A especificidade do setor financeiro impõe, ainda, exigências reforçadas de governação, com foco na qualificação dos conselhos e na mitigação de riscos sistémicos[45].

3. DEVER DE GERIR, CLASSIFICAR E COMUNICAR INFORMAÇÕES SOBRE INCIDENTES RELACIONADOS COM AS TIC

3.1. GESTÃO E CLASSIFICAÇÃO DE INCIDENTES RELACIONADOS COM AS TIC

A gestão eficaz dos incidentes relacionados com as TIC constitui um elemento essencial da estratégia de resiliência operacional digital preconizada pelo Regulamento DORA. Antes mesmo da obrigação de reporte às autoridades competentes, o regime estabelece um conjunto de deveres internos de deteção, registo, classificação e resposta a incidentes, fundamentais para assegurar uma atuação tempestiva e proporcional por parte das entidades financeiras.

Os artigos 17.º e 18.º do Regulamento DORA enquadram esta dimensão, impondo às entidades financeiras a adoção de processos organizados e contínuos de gestão de

[44] Regulamento DORA, artigo 5.º, n.º 4.
[45] KLAUS, J. Hopt, 2021, "Corporate Governance of Banks and Financial Institutions", pp. 14-16.

incidentes, bem como a aplicação de critérios uniformes para a sua classificação, com vista à avaliação do seu grau de severidade[46].

Através da criação de processos de gestão do risco pretende-se que as entidades financeiras possam responder de forma mais célere e eficaz aos riscos tecnológicos. Todavia, para alcançar esse objetivo, o legislador europeu optou por não impor um modelo único ou rígido de gestão. Optou antes por permitir que as entidades adotem abordagens próprias, desde que capazes de assegurar as seguintes funções: identificação, proteção, prevenção, deteção, resposta, recuperação, aprendizagem, evolução, e notificação dos riscos associados às TIC[47], conferindo assim uma abordagem flexível e proporcional à dimensão e ao perfil de risco de cada entidade financeira.

Para que os processos de gestão do risco cumpram eficazmente os seus objetivos, é essencial que as entidades financeiras disponham de mecanismos de classificação de incidentes relacionados com as TIC e de ciberameaças significativas. O conceito de incidente relacionado com as TIC é central neste enquadramento e corresponde, a "*uma ocorrência ou uma série de ocorrências conexas não previstas pelas entidades financeiras que comprometem a segurança dos sistemas de rede e informação e têm um impacto adverso na disponibilidade, autenticidade, integridade ou confidencialidade dos dados ou nos serviços prestados pela entidade financeira*"[48]. Entre estes, o Regulamento confere particular relevo aos incidentes de carácter severo, ou seja, aqueles que apresentam um impacto negativo elevado sobre funções críticas ou importantes da entidade financeira[49]. Já as ciberameaças significativas correspondem a "*uma ciberameaça cujas características técnicas indicam que tem potencial de resultar num incidente de carácter severo relacionado com as TIC ou num incidente de carácter severo operacional ou de segurança relacionado com pagamentos*"[50].

Assim, as entidades financeiras têm de possuir mecanismos que as permitam classificar adequadamente os incidentes ocorridos e as ciberameaças identificadas. Esta classificação é essencial, por um lado, para que as entidades financeiras possam dar respostas proporcionais à gravidade dos acontecimentos e, por outro, para permitir a avaliação da eventual obrigatoriedade de reporte às autoridades competentes ou aos clientes.

[46] Art. 17.º, n.º 1 do Regulamento DORA.
[47] Considerando 47 do Regulamento DORA.
[48] Art. 3.º (8) do Regulamento DORA.
[49] Art. 3.º (10) do Regulamento DORA.
[50] Art. 3.º (13) do Regulamento DORA.

Para assegurar que a classificação dos incidentes é feita de uma forma objetiva e uniforme em toda a União, o Regulamento DORA estabelece um conjunto de critérios que devem ser considerados pelas entidades financeiras. Esses critérios, previstos no artigo 18.º/1, permitem avaliar a gravidade do incidente com base nos seus impactos concretos, nomeadamente: o número e a relevância dos clientes (al. a)), a duração do incidente (al. b)), a distribuição geográfica (al. c)), a perda de dados (al. d)), a criticidade dos serviços afetados (al. e)) e as perdas económicas resultantes desse acontecimento (al. f)). Estes critérios são especificados mais pormenorizadamente no Regulamento Delegado (UE) 2024/1772 da Comissão, de 13 de março de 2024.

Assim, embora todas as entidades estejam obrigadas a gerir e classificar internamente todos os incidentes relacionados com as TIC, o reporte obrigatório às autoridades competentes apenas se impõe quando o incidente for qualificado como severo. Por isso, a classificação do risco assume um papel determinante, pois é esta classificação que permite aferir se os requisitos formais do reporte estão preenchidos.

3.2. DEVER DE REPORTAR INCIDENTES RELACIONADOS COM AS TIC

O dever de reporte de incidentes relacionados com as TIC constitui um dos pilares fundamentais do Regulamento DORA[51]. Esta obrigação visa garantir a proteção da integridade do sistema financeiro e a confiança dos investidores. Num setor altamente interligado como o financeiro, um incidente isolado pode desencadear um efeito de contágio com implicações sistémicas, pelo que a deteção atempada e a comunicação adequada são fulcrais para mitigar impactos negativos e salvaguardar a estabilidade do sistema.

Neste contexto, os destinatários das comunicações são, em primeiro lugar, as autoridades competentes pertinentes, responsáveis pela supervisão e coordenação institucional. Em certos casos, poderá também haver lugar à comunicação aos clientes, sempre que os seus interesses financeiros tenham sido diretamente afetados. Deste modo, promove-se a transparência e reforça-se a confiança nas entidades financeiras.

Como já se avançou no subcapítulo anterior, de acordo com o Regulamento DORA, apenas estão sujeitos ao dever de reporte os incidentes severos relacionados com as TIC[52] e as ciberameaças significativas[53]. Esta lógica funda-se na ideia se proporcionalidade

[51] CLAUSMEIER, Dirk, "Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)", pp. 85-86.
[52] Art. 19.º, n.º 1, 1.º parágrafo e art. 19.º, n.º 3, 1.º parágrafo do Regulamento DORA.
[53] Art. 19.º, n.º 2, 1.º parágrafo e art. 19.º, n.º 3, 2.º parágrafo do Regulamento DORA.

subjacente ao diploma, ficando sujeitos ao reporte os incidentes que apresentam mais riscos para a estabilidade financeira e para os clientes.

Para qualificar um incidente relacionado com as TIC como severo, é necessário atender aos critérios já enunciados no subcapítulo anterior, previstos no artigo 18.º/1 do Regulamento DORA, em conjugação com as regras de classificação estabelecidas nos artigos 8.º e 9.º do Regulamento Delegado (EU) 2024/1772.

O artigo 8.º estabelece duas vias para a classificação de um incidente de carácter severo:

- Uma primeira (8.º/1), que exige a verificação de duas condições, estarmos perante um incidente que afete um serviço crítico e de serem atingidos determinados limites de materialidade. Estes limites de materialidade correspondem a limiares quantitativos e qualitativos aplicáveis aos critérios previstos no artigo 18.º, n.º 1 do Regulamento DORA, densificados no artigo 9.º do Regulamento Delegado, cuja superação determina a qualificação do incidente como severo. Assim, o incidente relacionado com TIC será severo caso ultrapasse o limiar mínimo previsto no artigo 9.º, n.º 5, al. b) do Regulamento Delegado (UE) 2024/1772[54], ou caso atinja dois ou mais dos outros limiares de materialidade a que se refere o artigo 9.º, n.ºs 1 a 6 do Regulamento Delegado (UE) 2024/1772.

- Uma segunda via (8.º/2), que permite que todos os incidentes recorrentes que, individualmente, não reúnam os requisitos para serem qualificados como de carácter severo nos termos do n.º 1 possam ser classificados como tal: caso ocorram pelo menos duas vezes num período de 6 meses; tenham a mesma causa profunda aparente, como referido no artigo 20.º, al. b), primeiro parágrafo do Regulamento (UE) 2022/2554; e preencham, na sua globalidade, os requisitos do n.º 1, permitindo a sua qualificação conjunta como um único incidente de carácter severo.

Com a classificação do incidente relacionado com as TIC como severo, as entidades financeiras ficam obrigadas a comunicar o incidente às autoridades competentes[55/56], permitindo-lhes avaliar com maior profundidade a gravidade do incidente e determinar

[54] Art. 8.º/1/a) do Regulamento Delegado (UE) 2024/1772.
[55] Art. 19.º, n.º 1 do Regulamento DORA.
[56] Caso estejamos perante uma instituição de crédito classificada como significativa, de acordo com o art. 6.º, n.º 4 do Regulamento do Mecanismo Único de Supervisão, esta deve comunicar os incidentes de caráter severo relacionados com as TIC à autoridade nacional competente responsável pelo setor bancário, que transmite imediatamente esse relatório ao BCE (Art. 19.º, n.º 1, 3.º parágrafo).

as eventuais medidas de supervisão a adotar[57]. Este processo de comunicação assenta numa abordagem faseada, estruturada em três níveis.

Em primeiro lugar, deve ser apresentada uma notificação inicial logo que possível após a deteção do incidente[58]. Esta notificação inicial deve ser apresentada o mais rapidamente possível após a classificação do incidente como severo, não podendo ultrapassar o limite máximo de quatro horas a contar desse momento. Além disso, para assegurar que a classificação dos incidentes relacionados com as TIC é feita com a maior brevidade possível, o legislador estabelece também um prazo máximo de vinte e quatro horas para a comunicação, contado a partir do conhecimento inicial do incidente. Desta forma, garante-se que a avaliação da gravidade dos incidentes ocorre de forma célere e que as autoridades competentes recebem a notificação num prazo reduzido após a ocorrência do evento[59/60].

Após a notificação inicial, as autoridades competentes devem receber informações mais pormenorizadas sobre o incidente relacionado com as TIC no relatório intercalar[61/62]. Este relatório deve ser submetido no prazo máximo de setenta e duas horas após a notificação inicial[63]. Caso o estado do incidente sofra alterações significativas ou o seu tratamento evolua com base em novas informações relevantes, deve ser prestado um novo relatório intercalar atualizado[64].

Por fim, após a conclusão da análise das causas subjacentes ao incidente, deve ser elaborado um relatório final[65], que inclua todas as informações pertinentes sobre o incidente. Este deve ser submetido às autoridades competentes no prazo de um mês a contar do relatório intercalar ou do relatório intercalar atualizado[66]. Este deve ser submetido independentemente de já terem sido aplicadas medidas de mitigação e deverá

[57] Considerando 3 do Regulamento Delegado (UE) 2025/301 de 23 de outubro de 2024.
[58] Art. 19.º, n.º 4, al. a).
[59] Artigo 5.º, n.º 1, al. a) do Regulamento Delegado (UE) 2025/301 de 23 de outubro de 2024.
[60] Se um incidente inicialmente não for classificado como severo, mas vier a sê-lo numa fase posterior, a entidade financeira deve submeter a notificação inicial no prazo máximo de quatro horas a contar da classificação (Artigo 5.º, n.º 2 do Regulamento Delegado (UE) 2025/301 de 23 de outubro de 2024).
[61] Art. 19.º, n.º 4, al. b) do Regulamento DORA.
[62] Considerando 3 do Regulamento Delegado (UE) 2025/301 de 23 de outubro de 2024.
[63] Art. 5.º, n.º 1, al. b) do Regulamento Delegado (UE) 2025/301 de 23 de outubro de 2024.
[64] Art. 19.º, n.º 4, al. b) do Regulamento DORA.
[65] Art. 19.º, n.º 4, al. c).
[66] Art. 5.º, n.º 1, al. c) do Regulamento Delegado (UE) 2025/301 de 23 de outubro de 2024.

conter os valores reais do impacto, substituindo estimativas anteriormente comunicadas[67/68].

A informação prestada através da notificação inicial e dos relatórios deve ser completa, incluindo todas as informações necessárias que permitam à autoridade competente determinar o grau de importância do incidente de carácter severo relacionado com as TIC e avaliar os possíveis impactos transfronteiriços[69/70].

Além da comunicação às autoridades competentes, as entidades financeiras estão obrigadas a informar os clientes sobre os incidentes de carácter severo caso estes tenham impacto nos seus interesses financeiros. Esta comunicação deve ocorrer logo que o incidente seja detetado e incluir informação acerca das medidas que foram tomadas para atenuar os efeitos adversos do incidente[71].

O Regulamento DORA prevê igualmente um regime específico para a comunicação de ciberameaças significativas, ou seja, de ameaças potenciais que, pela sua gravidade, justificam atenção especial por parte das entidades financeiras. A qualificação formal de ciberameaças significativas depende da verificação cumulativa de três requisitos, previstos no artigo 10.º do Regulamento Delegado (UE) 2024/1772:

a) Em primeiro lugar, exige-se que, caso se concretize, a ciberameaça possa afetar funções críticas ou importantes da própria entidade financeira, ou então causar impacto noutras entidades financeiras, terceiros prestadores, clientes ou contrapartes financeiras.

b) Em segundo lugar, a ameaça deve apresentar uma elevada probabilidade de materialização. Para aferir essa probabilidade, a entidade financeira deve ponderar, entre outros elementos, a existência de vulnerabilidades conhecidas nos seus

[67] Em tempo útil, relativamente a cada um dos relatórios recebidos, a autoridade nacional competente deve transmitir essas informações às partes interessadas pertinentes, tendo por critério base as suas competências. O Regulamento DORA identifica expressamente no seu artigo 19.º/6 algumas entidades como potenciais destinatárias. No caso das instituições de crédito significativas (na aceção do Mecanismo Único de Supervisão), a autoridade nacional competente deve enviar imediatamente ao BCE os relatórios sobre incidentes severos relacionados com as TIC, bem como as notificações de ciberameaças significativas. Cfr. art. 19.º, n.º 6 do Regulamento DORA e art. 19.º, n.º 1, parágrafo 3.º

[68] CLAUSMEIER, Dirk, "Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)", p. 86.

[69] Art. 19.º, n.º 1, parágrafo 5.º.

[70] As informações gerais a fornecer encontram-se densificadas nos artigos 1 a 4 do Regulamento Delegado (EU) 2025/301 da Comissão de 23 de outubro de 2024.

[71] Art. 19.º, n.º 3 do Regulamento DORA.

sistemas, as capacidades e intenções dos autores das ameaças (desde que conhecidas); bem como a persistência da ameaça e eventual histórico de incidentes semelhantes que tenham afetado a entidade financeira ou os seus terceiros prestadores, clientes ou contrapartes financeiras;

c) Por fim, a ciberameaça será considerada significativa se, na hipótese da sua concretização, for suscetível de preencher pelo menos um dos limiares de materialidade previstos para os incidentes severos: o critério da criticidade dos serviços afetados (critério previsto no artigo 18.º/1/e), do Regulamento DORA e concretizado no artigo 6.º do Regulamento Delegado); os limiares relativos ao número de clientes, contrapartes financeiras e transações afetadas (artigo 9.º/1 do Regulamento Delegado); e o limiar relativo aos impacto transfronteiriço (artigo 4.º do Regulamento Delegado). Atendendo à natureza da ciberameaça e às informações disponíveis, poderão ainda ser considerados os demais limiares previstos no artigo 9.º (como o impacto reputacional, a duração da indisponibilidade, as perdas de dados ou o impacto económico), sempre que a entidade concluir que este poderão vir a ser atingidos.

Quanto às ciberameaças significativas, por corresponderem a riscos meramente potenciais, não existe um dever legal de comunicação às autoridades. Todavia, o regulamento admite a possibilidade de reporte voluntário[72], sempre que a entidade considere que a ciberameaça em causa possa ser relevante para o sistema financeiro, para os utilizadores ou para os clientes do serviço[73/74].

A consagração de um mecanismo voluntário, mas regulado, visa garantir a uniformização dos procedimentos de notificação, assegurando coerência quanto à forma, conteúdo e destinatários das comunicações. Ainda que facultativo, o facto de este mecanismo estar expressamente previsto e regulado demonstra a vontade do legislador em conferir um papel ativo às entidades financeiras na proteção do sistema e na promoção da transparência. Paralelamente, ao estabelecer um procedimento claro para o tratamento destas comunicações, garante-se que estas comunicações voluntárias recebem um

[72] Artigo 19.º, n.º 2, 1.º parágrafo do Regulamento DORA.
[73] Considerando 24 do Regulamento DORA.
[74] Esta consagração legal de um reporte a título voluntário também é aquela que é coerente com o previsto na Diretiva NIS 2, vd. Considerando 105 e art. 23.º da Diretiva NIS 2.

tratamento uniforme e adequado à sua importância, prevenindo abordagens dispersas ou arbitrárias.

Uma vez que as ciberameaças significativas devem ser notificadas numa base voluntária, o conteúdo dessas notificações não deverá impor encargos às entidades financeiras e deverá ser mais limitado do que as informações solicitadas para incidentes de caráter severo relacionados com as TIC[75]. São apenas impostas algumas regras quanto ao seu conteúdo no artigo 6.º do Regulamento Delegado (UE) 2025/301 de 23 de outubro de 2024.

Já no que respeita à comunicação de ciberameaças significativas aos clientes, contrariamente ao regime de reporte voluntário previsto para a comunicação às autoridades competentes, neste caso existe uma obrigação de comunicação aos clientes sempre que estes possam vir a ser potencialmente afetados. Nessas situações, as entidades devem informá-los das ameaças em causa e das medidas adequadas que poderão considerar tomar para a sua proteção[76].

4. DEVER DE REALIZAR TESTES DE RESILIÊNCIA OPERACIONAL DIGITAL

A realização dos testes de resiliência operacional digital é crucial para garantir a continuidade dos serviços essenciais num ambiente cada vez mais dependente de tecnologias digitais. O DORA, ao impor a obrigatoriedade destes testes às entidades financeiras, visa mitigar riscos cibernéticos, falhas nos sistemas tecnológicos e possíveis interrupções que possam afetar a integridade das instituições financeiras dos seus clientes.

O DORA impõe dois tipos principais de testes que serão detalhados a seguir: os testes regulares de avaliação de resiliência e os testes avançados, com foco nas entidades de maior risco. A aplicação destes testes assegura que as empresas possam identificar vulnerabilidades e aprimorar as suas defesas antes que eventos adversos aconteçam, mantendo a estabilidade do mercado financeiro e a proteção de dados sensíveis.

[75] Considerando 6 do Regulamento Delegado (UE) 2025/301 de 23 de outubro de 2024.
[76] Artigo 19.º, n.º 3, 2.º parágrafo do Regulamento DORA.

4.1. TESTES REGULARES DE AVALIAÇÃO DE RESILIÊNCIA

As entidades financeiras que não sejam microempresas deverão estabelecer, manter e rever um programa sólido e abrangente de testes de resiliência operacional digital para efeitos do quadro de gestão do risco associado às TIC referido nos capítulos anteriores[77].

A realização dos testes deve adotar uma abordagem baseada no risco, considerando fatores como a evolução dos riscos tecnológicos, a criticidade dos ativos de informação e dos serviços prestados, bem como outros elementos relevantes[78]. O programa de testes deve ser amplo, incorporando diferentes tipos de avaliações e metodologias, tais como rastreamento de vulnerabilidades, análise de segurança de redes, revisões de código-fonte (quando possível), testes de compatibilidade, testes de desempenho, testes de penetração e outros métodos previstos no artigo 25.º, n.º 1 do DORA.

Os testes realizados, poderão ser levados a cabo por entidades internas ou externas, sendo essencial que sejam independentes. Quando os testes forem efetuados por testadores internos, a entidade financeira deverá afetar recursos suficientes de modo a evitar conflitos de interesses ao longo das fases de conceção e execução dos testes[79].

Além disso, as entidades têm a obrigação de assegurar que todos os sistemas e aplicações que suportem funções importantes ou críticas sejam testados adequadamente pelo menos uma vez por ano[80]. Após a realização dos testes, devem ser adotadas políticas e procedimentos internos para priorizar, classificar e corrigir todas as vulnerabilidades identificadas, bem como métodos de validação para confirmar que as deficiências foram efetivamente tratadas.

É importante que os testes de resiliência operacional ultrapassem a mera avaliação de respostas a incidentes isolados, concentrando-se na identificação de vulnerabilidades sistémicas e na análise da capacidade de adaptação a cenários complexos[81]. A prioridade deve recair sobre a antecipação de falhas interligadas e a preparação para eventos com

---

[77] Regulamento DORA, artigo 24.º, n.º 1. Por outro lado, as microempresas, também estão sujeitas a obrigações de realizarem testes, embora possam ajustar sua abordagem conforme a sua dimensão e capacidade, equilibrando o risco, a urgência dos testes e a criticidade dos ativos de informação, nos termos do artigo 25.º, n.º 3.

[78] O DORA impõe no seu artigo 25.º, n.º 2., em especial, às centrais de valores mobiliários e contrapartes centrais, devido ao seu maior risco sistémico, a obrigação de realizarem avaliações de vulnerabilidades antes de lançarem ou relançarem serviços novos ou existentes de aplicações e componentes da infraestrutura, e de serviços TIC de apoio às funções críticas ou importantes da entidade financeira.

[79] Regulamento DORA, artigo 24.º, n.º 4.

[80] Regulamento DORA, artigo 24.º, n.º 6.

[81] BELCIU, Alina-Camelia/PREDA, Marius, 2024, "Cyber Resilience Under the EU Framework: Insights from an Applied Case Study on Critical Sectors", pp. 19-20.

efeitos em cascata, assegurando a continuidade dos serviços mesmo em condições de elevada incerteza[82].

4.2. TESTES DE PENETRAÇÃO BASEADO EM AMEAÇAS (TLPT)

Os TLPT[83] consistem num *"quadro que simula as táticas, as técnicas e os procedimentos de autores de ameaças reais que se considera representarem uma efetiva ciberameaça e que realiza testes controlados, adaptados e com base em informações («equipa vermelha») dos sistemas de produção críticos «ao vivo» da entidade financeira"*[84].

Estes testes visam simular ataques reais em ambientes de produção "ao vivo", abrangendo funções críticas ou importantes e todos os sistemas de TIC que lhes dão suporte, incluindo aqueles externalizados a prestadores terceiros,[85] e deverão ser realizados, pelo menos, de 3 em 3 anos[86].

São testes, portanto, mais avançados e especializados, exigidos apenas às entidades financeiras com uma maturidade suficiente em termos de TIC para os realizarem de forma razoável, nomeadamente, as entidades financeiras de grande dimensão e que apresentam maior risco sistémico, como bolsas de valores, centrais de valores mobiliários e contrapartes centrais, e que operam em subsetores com serviços financeiros fundamentais como os pagamentos ou a banca[87].

Para a realização deste tipo de testes, a entidade financeira deverá, idealmente, contratar testadores externos, nos termos do artigo 27.º, todavia, quando não o façam e optem por testadores internos[88], deverão recorrer obrigatoriamente a testadores externos de três em três testes[89].

No caso em que houver terceiros prestadores de serviços de TIC envolvidos e for razoável esperar que a sua participação num teste TLPT tenha um impacto adverso na

---

[82] PESCAROLI, Gianluca/NEED-HAM BENNET, 2021, "Operational Resilience and Stress Testing: Hit or Myth?", pp. 39-41.
[83] Do inglês "*threat-led penetration testing*".
[84] Regulamento DORA, artigo 3.º, (17).
[85] Nos termos do artigo 30.º, n.º 3, al. d) do Regulamento DORA, o terceiro prestador de serviços de TIC é obrigado a participar e cooperar plenamente nos testes TLPT realizados pela entidade financeira.
[86] A autoridade competente, designada pelos Estados-membros nos termos do artigo 26.º, nºs 9 e 10, poderá, entretanto, obrigar a entidade financeira a reduzir ou aumentar essa frequência tendo em conta o perfil de risco e as circunstâncias operacionais, nos termos do n.º 1 do mesmo artigo.
[87] Regulamento DORA, considerando 56.
[88] Esta possibilidade de recorrer a testadores internos só existe para as instituições de créditos que não sejam avaliadas como significativas nos termos do artigo 6.º, n.º 4 do Regulamento n.º 1024/2013, do contrário, só poderão recorrer a testadores externos.
[89] Regulamento DORA, artigo 26.º, n.º 8.

qualidade ou na segurança dos serviços que prestam a clientes não abrangidos pelo DORA, ou comprometa a confidencialidade dos dados desses clientes, o regulamento prevê uma solução específica. A entidade financeira e o terceiro prestador de serviços de TIC podem acordar, por escrito, que o próprio terceiro prestador celebre contratos diretamente com um testador externo. O objetivo é realizar um TLPT agrupado, ou seja, um teste único que abranja várias entidades financeiras clientes do mesmo prestador. Apesar de o contrato ser feito diretamente pelo terceiro prestador, a direção e coordenação do teste permanecem a cargo de uma entidade financeira designada[90].

5. DEVER DE GERIR RISCOS DE TERCEIROS NO DOMÍNIO DAS TIC

Os artigos 28.º a 30.º do Regulamento DORA consagram um conjunto deveres relacionados com a gestão do risco associado às TIC decorrente da utilização de serviços prestados por terceiros. A especial atenção conferida pelo legislador europeu a esta matéria justifica-se pela crescente dependência das entidades financeiras de serviços prestados por terceiros. Esta dependência pode deixar as entidades financeiras sujeitas a vulnerabilidades que não controlam[91].

Estas normas regulam aspetos essenciais da negociação contratual, execução, rescisão e relação pós-contratual dos serviços dos serviços prestados por terceiros[92]. A disciplina estabelecida pelo Regulamento DORA reveste particular relevância sempre que estejam em causa funções críticas ou importantes. Estas são funções, que devido à sua natureza, podem, em caso de perturbação, comprometer significativamente a solidez financeira, a continuidade dos serviços ou o cumprimento das obrigações legais da entidade financeira[93].

A externalização deste tipo de funções levanta dois problemas principais: por um lado, leva a uma perda por parte das entidades financeiras do controlo direto das suas funções essenciais; por outro, leva a um aumento do risco sistémico, na medida em que certos prestadores de TIC fornecem serviços críticos a várias entidades financeiras em simultâneo, o que significa que a falha de um único prestador pode afetar múltiplas

[90] Regulamento DORA, artigo 26.º, n.º 4.
[91] TRAUTMANN, Kilian/BOMS, Daniel, 2024, "DORA from the perspective of ICT third-party risk management", p. 183.
[92] CARRILLO, Elena F. Pérez, "Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform", p. 19.
[93] Art. 3.º, (22) do Regulamento DORA.

instituições e gerar repercussões generalizadas no setor financeiro[94]. Essa preocupação é particularmente relevante no contexto atual de elevada concentração do mercado de serviços em nuvem, dominado por poucos fornecedores globais, o que acentua os riscos de dependência e os potenciais efeitos sistémicos da falha de um único prestador[95].

A identificação das funções críticas ou importantes é determinante, pois é a partir dessa qualificação que se ativam as obrigações mais exigentes previstas no regulamento. Entre estas contam-se, a avaliação prévia dos prestadores, de exigência de cláusulas contratuais obrigatórias e de monitorização contínua da relação contratual.

O risco decorrente da contratação de serviços a prestadores de serviços de TIC deve ser gerido pelas entidades financeiras como componente integrante do risco associado às TIC, tal como referido no artigo 6.º, n.º 1 do Regulamento DORA[96]. Além disso, quando subcontratam serviços de TIC as entidades financeiras continuam responsáveis pelo cumprimento das normas de resiliência operacional digital, não podendo essa responsabilidade ser delegada no terceiro[97/98]. A gestão do risco deve ainda respeitar o princípio da proporcionalidade[99].

As entidades financeiras devem adotar uma estratégia para a gestão do risco associado às TIC decorrente da utilização de prestadores terceiros[100], a qual deve assentar num conjunto de princípios fundamentais e ser objeto de revisão periódica[101/102]. Esta estratégia inclui a definição de uma política específica para a utilização de serviços de TIC que apoiem funções críticas ou importantes[103/104].

---

[94] PARCHIMOWICZ, Katarzyna, "Do nor get lost in the cloud: how EU financial institutions could avoid problems with cloud services arising under DORA", pp. 471-472.
[95] TRAUTMANN, Kilian, 2023, "EU-DORA regulation as a result of cloud computing adoption by the financial services industry", p.157.
[96] Art. 28.º, n.º 1 do Regulamento DORA.
[97] Art. 28.º, n.º 1, al. a) do Regulamento DORA.
[98] TOLIN, Grace/PUNIA, Gavin/EMMANUEL, Jonathan, "EU Digital Operational Resilience Regulation (DORA)", p. 14.
[99] Art. 28.º, n.º 1, al. b) do Regulamento DORA.
[100] Considerando 1 do Regulamento Delegado (UE) 2024/1773 de 13 de março de 2024.
[101] Art. 28.º, n.º 2 do Regulamento DORA.
[102] Não estão sujeitas a esta obrigação, as entidades abrangidas pelo quadro simplificado de gestão do risco associado às TIC (art. 16.º/1 do Regulamento DORA) e as microempresas.
[103] Art. 1.º do Regulamento Delegado (UE) 2024/1773 de 13 de março de 2024.
[104] Esta política define os princípios, regras e procedimentos que as entidades financeiras deem seguir sempre que externalizem funções críticas ou importantes para terceiros prestadores. A sua elaboração deve respeitar o princípio da proporcionalidade, sendo ajustadas à dimensão perfil de risco global e à complexidade da entidade financeira. Esta política dispõe acerca da seleção dos prestadores, os requisitos mínimos a incluir nos contratos, a monitorização contínua dos serviços prestados e a adoção de planos de saída adequados. A estrutura e conteúdo da política vêm concretizados no Regulamento Delegado (UE) 2024/1773, de 13 de março de 2024.

No âmbito do quadro da gestão de risco, as entidades financeiras devem manter um registo de informações relativas a todos os acordos contratuais celebrados para a utilização dos serviços de TIC prestados por terceiros, devendo distinguir entre os acordos que apoiem funções críticas ou importantes e os restantes[105].

Uma vez por ano, as entidades financeiras estão ainda obrigadas a comunicar, às autoridades competentes: (i) o número de novos acordos contratuais relativos à utilização de serviços de TIC; (ii) as categorias dos terceiros prestadores de serviços de TIC; (iii) o tipo de acordos celebrados; (iv) os serviços de TIC prestados e as funções que estão a ser realizadas[106].

Por fim, devem informar as autoridades competentes sempre que planeiem celebrar um acordo contratual que apoie funções críticas ou importantes, bem como quando uma determinada função venha a ser qualificada como crítica ou importante[107].

5.1.FASE PRÉ-CONTRATUAL

Antes da celebração de um acordo contratual com um terceiro prestador de serviços de TIC, as entidades financeiras devem ponderar três fatores essenciais: em primeiro lugar, a seleção de um prestador de serviços de TIC adequado; em segundo lugar, a avaliação de se estão a transferir funções críticas ou importantes para esse prestador; e, em último lugar, a definição do conteúdo do contrato, assegurando a sua conformidade com as exigências do Regulamento DORA[108].

No que respeita à escolha do terceiro prestador de serviços de TIC, as entidades financeiras devem considerar a possibilidade daquele contrato reforçar o risco de concentração[109]. Este corresponde ao risco de dependência excessiva em relação a um único fornecedor, suscetível de gerar impactos negativos tanto na instituição individual, como no sistema financeiro em geral[110]. Para as instituições financeiras de menor ou média dimensão, a dependência pode causar um desequilíbrio de poder nas negociações contratuais e, posteriormente, na execução do serviço. No caso das entidades de maior dimensão, a dependência excessiva de um fornecedor pode causar problemas de estabilidade e aumentar o risco sistémico de todo o sistema financeiro.

---

[105] Art. 28.º, n.º 3, 1.º e 2.º parágrafos do Regulamento DORA.
[106] Art. 28.º, n.º 3, 3.º parágrafo do Regulamento DORA.
[107] Art. 28.º, n.º 3, 4.º parágrafo do Regulamento DORA.
[108] PARCHIMOWICZ, Katarzyna, "Do nor get lost in the cloud: how EU financial institutions could avoid problems with cloud services arising under DORA", p. 468.
[109] Artigo 28.º, n.º 4, al. º d) e artigo 29.º do Regulamento DORA.
[110] PARCHIMOWICZ, Katarzyna, "Do nor get lost in the cloud: how EU financial institutions could avoid problems with cloud services arising under DORA", p. 469.

Acresce que as entidades financeiras estão ainda obrigadas a efetuar *due diligence* relativamente ao potencial prestador de serviços de TIC, de modo a avaliar se este é adequado ou não[111]. É ainda vedada às entidades financeiras a celebração de acordos contratuais com prestadores que não cumpram normas de segurança de informação adequadas.

Posteriormente, as entidades financeiras devem avaliar se estão a externalizar uma função crítica ou não[112]. Este trata-se de um passo essencial, uma vez que a identificação de funções críticas ou importantes determina a aplicação de deveres reforçados em matéria de gestão do risco, avaliação contratual e monitorização contínua, nos termos exigidos pelo Regulamento DORA.

Por fim, as entidades financeiras devem preparar-se para, no momento da negociação do contrato, assegurar o respeito pelas obrigações previstas no Regulamento DORA, as quais serão analisadas no subcapítulo seguinte.

5.2.DISPOSIÇÕES OBRIGATÓRIAS DOS CONTRATOS

Os acordos contratuais celebrados entre a entidade financeira e o terceiro prestador de serviços de TIC estão sujeitos à forma escrita em papel ou num documento com outro formato descarregável, duradouro e acessível[113]. Esta exigência visa assegurar clareza quanto à identificação dos direitos e obrigações das partes e facilita o controlo e monitorização contínua da prestação de serviços e a gestão eficaz do risco associado à externalização.

Para além da exigência de forma, o Regulamento DORA impõe ainda a inclusão de determinados elementos obrigatórios no conteúdo dos contratos celebrados com terceiros prestadores de serviços de TIC[114]. Este conteúdo contratual obrigatório visa assegurar que todas as entidades financeiras, independentemente da sua dimensão ou capacidade negocial, beneficiam de um nível mínimo de proteção nas relações contratuais com terceiros prestadores de serviços de TIC, que podem, em função da sua dimensão ou relevância, dispor de uma vantagem negocial significativa[115].

[111] Art. 28.º, n.º 4, al. d) do Regulamento DORA.
[112] Art. 28.º, nº 4, al. a) do Regulamento DORA.
[113] Art. 30.º, n.º 1 do Regulamento DORA.
[114] Art. 30.º, n.º 2 do Regulamento DORA.
[115] CLAUSMEIER, Dirk, 2023, "Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)", p. 84.

Entre estes elementos obrigatórios, destaca-se: (i) a descrição clara e completa de todas as funções e serviços de TIC a prestar[116]; (ii) a obrigação do prestador de serviços de TIC de prestar assistência à entidade financeira, sem custos adicionais ou por um custo previamente determinado[117]; e (iii) a previsão de um direito de resolução contratual a favor da entidade financeira[118].

Em caso de externalização de funções críticas ou importantes, o conteúdo contratual obrigatório previsto pelo Regulamento DORA torna-se ainda mais extenso[119], devendo contemplar cláusulas que assegurem, entre outros aspetos: (i) o direito da entidade financeira a monitorizar continuamente o desempenho do terceiro prestador de serviços de TIC, incluindo direitos ilimitados de acesso, inspeção e auditoria pela entidade financeira como pelas autoridades competentes[120]; e (ii) a definição de estratégias de saída, que estabeleçam um período de transição adequado, durante o qual o terceiro continuará a desempenhar as respetivas funções ou a prestar serviços de TIC com o objetivo de reduzir o risco de perturbações na entidade financeira, de assegurar a sua resolução e reestruturação efetiva, ou de permitir a migração para outro terceiro prestador de serviços de TIC ou a passagem para soluções internas, consoante a complexidade do serviço prestado[121].

Importa ainda atender a uma situação particular: a possibilidade de o terceiro prestador de serviços de TIC recorrer à subcontratação para executar, total ou parcialmente, as funções ou serviços contratados. Quando não estejam em causa funções críticas ou importantes, a subcontratação é, em regra, livre e não carece de requisitos adicionais específicos, apenas deve ser conforme a estratégia em matéria de risco associado às TIC, devido a terceiros. No entanto, o Regulamento DORA impõe que a admissão de subcontratação de funções críticas ou importantes esteja sujeita a uma autorização contratual, devendo as condições desta subcontratação ser previstas de forma clara e completa[122/123].

O legislador europeu confere especial relevância à subcontratação de funções críticas ou importantes porque esta pode amplificar os riscos já inerentes à externalização,

[116] Art. 30.º, n.º 2, al. a) do Regulamento DORA.
[117] Art. 30.º, n.º 2, al. f) do Regulamento DORA.
[118] Art. 30.º, n.º 2, al. h) do Regulamento DORA.
[119] Art. 30.º, n.º 3 do Regulamento DORA.
[120] Art. 30.º, n.º 3, al. e) do Regulamento DORA.
[121] Art. 30.º, n.º 3, al. f) do Regulamento DORA.
[122] Art. 30.º, n.º 2, al. a) do Regulamento DORA.
[123] TOLIN, Grace/PUNIA, Gavin/EMMANUEL, Jonathan, "EU Digital Operational Resilience Regulation (DORA)", p. 17.

introduzindo um novo nível de dependência que fragiliza o controlo da entidade financeira, aumenta o risco de dependência face a terceiros que concentram a prestação de múltiplos serviços de TIC e dificulta a identificação de quem, na prática, presta os serviços.

O Regulamento Delegado da Comissão Europeia de 27 de março de 2025 (C(2025)1682 final)[124], que completa o Regulamento DORA no que respeita à subcontratação de serviços de TIC que suportam funções críticas ou importantes, estabelece um conjunto de obrigações adicionais que as entidades financeiras devem observar sempre que o prestador recorra à subcontratação. No essencial, este regulamento delegado apresenta um conjunto de obrigações para a subcontratação de funções críticas ou importantes que reproduz, em larga medida, as obrigações já impostas pelo Regulamento DORA à externalização direta dessas mesmas funções. Entre as medidas previstas, destacam-se a obrigação de avaliar previamente a subcontratação[125], a exigência de um conteúdo contratual mínimo[126] e o direito de resolver o contrato com o prestador em caso de incumprimento[127].

[124] O Regulamento Delegado da Comissão Europeia de 27 de março de 2025 (C(2025)1682 final) foi adotado pela Comissão, mas, à data, ainda não foi publicado no Jornal Oficial da União Europeia. Encontra-se sujeito ao procedimento de controlo previsto no artigo 290.º do TFUE, pelo que o seu conteúdo ainda não é definitivo e poderá ser objeto de alterações antes da sua publicação oficial.
[125] Art. 3.º do Regulamento Delegado da Comissão Europeia de 27 de março de 2025 (C(2025)1682 final).
[126] Art. 4.º do Regulamento Delegado da Comissão Europeia de 27 de março de 2025 (C(2025)1682 final).
[127] Art. 6.º do Regulamento Delegado da Comissão Europeia de 27 de março de 2025 (C(2025)1682 final).

IV) CONCLUSÃO

O Regulamento DORA surgiu como resposta aos desafios crescentes colocados pela digitalização do setor financeiro, em especial os riscos operacionais associados à dependência das tecnologias da informação e comunicação (TIC) e à ausência de um enquadramento normativo europeu que garantisse uma abordagem uniforme, coordenada e eficaz frente a essas vulnerabilidades.

A análise desenvolvida ao longo deste trabalho permite constatar que o legislador europeu procurou enfrentar esses desafios por meio de um regime ambicioso, transversal e exigente, aplicável a um vasto leque de entidades do setor financeiro. O quadro normativo introduzido é, contudo, complexo e exigirá transformações estruturais significativas: reorganização de processos internos, criação de funções específicas, contratação de profissionais especializados e investimento contínuo em soluções tecnológicas.

Não obstante os mecanismos de mitigação previstos — como a aplicação diferenciada de certas obrigações às micro e a algumas pequenas entidades em casos específicos, e a consagração formal do princípio da proporcionalidade — constata-se que, na prática, muitas entidades, inclusive de pequena e média dimensão, estão sujeitas a um conjunto quase idêntico de obrigações em comparação com instituições de grande porte. A falta de orientações detalhadas sobre como operacionalizar a proporcionalidade agrava esse cenário, podendo levar à adoção de uma abordagem meramente formalista de cumprimento. Em vez de fomentar uma cultura de resiliência genuína e adaptada à realidade de cada entidade, há o risco de que o cumprimento das obrigações do DORA se transforme em um exercício burocrático, centrado em demonstrar documentalmente a conformidade com os requisitos — a chamada "*check-box culture*" — em detrimento da efetiva robustez operacional.

A efetividade do regulamento dependerá, ainda, da adoção tempestiva e coordenada das medidas de Nível 2 e Nível 3 pelas Autoridades Europeias de Supervisão. Nos anos de 2024 e 2025, foram aprovados regulamentos delegados e de execução que detalham obrigações relativas à gestão de risco TIC, reporte de incidentes e supervisão de prestadores terceiros. Paralelamente, as autoridades vêm publicando medidas de Nível 3 — como os princípios da ESMA sobre supervisão de terceiros[128] e a consulta pública da

[128] Disponível em https://www.esma.europa.eu/press-news/esma-news/esma-publishes-principles-third-party-risk-supervision.

EBA sobre gestão de riscos com terceiros, ainda em curso até outubro de 2025[129]. Espera-se, até o final do ano, a adoção de uma última série de orientações técnicas. A consolidação dessas normas será crucial para garantir segurança jurídica e operacionalizar, com coerência e proporcionalidade, os deveres impostos pelo DORA.
Importa ainda lembrar que o ambiente tecnológico é dinâmico e em constante mutação. O sucesso do DORA dependerá da sua capacidade de se manter atualizado frente à rápida evolução dos riscos digitais e das inovações tecnológicas, incluindo as arquiteturas descentralizadas e as soluções emergentes no universo da Web3[130].

Em suma, o Regulamento DORA representa um marco na construção da resiliência operacional digital do setor financeiro europeu. No entanto, a sua efetividade não será determinada apenas pelo seu conteúdo normativo, mas pela forma como será interpretado, implementado e vivenciado pelas entidades financeiras e pelas autoridades competentes. Para além da conformidade formal, será necessária uma verdadeira mudança de paradigma cultural, em que a resiliência digital se torne uma prioridade estratégica — e não como um mero exercício de conformidade no papel.

[129] https://www.eba.europa.eu/publications-and-media/press-releases/eba-launches-consultation-its-draft-guidelines-third-party-risk-management-regard-non-ict-related.
[130] BASSAN, Fabio, 2023, “Digital Platforms and Blockchains: The age of Participatory Regulation”, p. 1120.

BIBLIOGRAFIA:

BASSAN, Fabio, 2023, "Digital Platforms and Blockchains: The age of Participatory Regulation", *European Business Law Review,* Vol. 34, No. 7, pp. 1103-1132.

BEGOZZI, Valerio/OLDANI, Matteo/TERRIZZANO, Francesca, 2023, "The growing importance of digital risk & governance", *Risk Management Magazine,* Vol. 18, No. 2, pp. 27-36.

BELCIU, Alina-Camelia/PREDA, Marius, 2024, "Cyber Resilience Under the EU Framework: Insights from an Applied Case Study on Critical Sectors", *International Journal of Information Security and Cybercrime*, Vol. 13, No. 2, pp. 18-32.

BIERECKI, Dominik, 2024, "Principle of Proportionality in the Application of the Digital Operational Resilience Act (DORA)", *Europejski Przegląd Prawa i Stosunków Międzynarodowych*, n.º 3/2024/71.

BUTTIGIEG, Chistopher P./ZIMMERMANN, Beatriz Brunelli, 2024, "The Digital Operational Resilience Act: Challenges and Some Reflections on the Adequacy of Europe's Architecture for Financial Supervision", in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4831717 (15/03/2025).

CARRILLO, Elena F. Pérez, 2023, "Cybersecurity in European Financial Institutions: New Grounds for Corporate Governance Reform", *European Business Law Review,* Vol. 34, No. 7, pp. 1133-1166.

CLAUSMEIER, Dirk, 2023, "Regulation of the European Parliament and the Council on digital operational resilience for the financial sector (DORA)", *International Cybersecurity Law Review,* Vol. 4, pp. 79-90.

CORTEZ, Elif Kiesow/DEKKER, Martijn, 2022, "A Corporate Governance Approach to Cybersecurity Risk Disclosure", *European Journal of Risk Regulation*, Vol. 13, No. 3, pp. 443-463.

DUGGAN, Derek, 2024, "The impact of the Digital Operational Resilience Act on financial market infrastructures in Europe", *Journal of Securities Operations & Custody,* Vol. 16, No. 4, pp. 344-350.

ESENER, Esen, 2024, "Adaptive Governance for Blockchain Networks", *Stanford Journal of Blockchain Law & Policy*, Vol. 7, No. 1, pp. 76-109.

KARAM, Elias/PLANCHET, Frédéric, 2012, Operational risks in financial sectors, *"Advances in Decision Sciences*", Vol. 2012.

KLAUS, J. Hopt, 2021, "Corporate Governance of Banks and Financial Institutions: Economic Theory, Supervisory Practice, Evidence and Policy", *European Business Organization Law Review*, in https://doi.org/10.1007/s40804-020-00201-z.

PARCHIMOWICZ, Katarzyna, 2024, "Do nor get lost in the cloud: how EU financial institutions could avoid problems with cloud services arising under DORA", *Law, Innovation and Technology*, vol. 16, No. 2, pp. 463-487.

PESCAROLI, Gianluca/NEED-HAM BENNET, 2021, "Operational Resilience and Stress Testing: Hit or Myth?", *Journal of Financial Transformation, vol, 53,* Maio, pp. 32-43.

RAMALHO, Inês Palma, 2021, "O princípio da proporcionalidade no sector financeiro", *InforBanca, Revista do Instituto de Formação Bancária*, Ed. 122, pp. 8-18.

REIS, Laura/TEIXEIRA, Maria Emília, 2022, "A transformação digital na banca e a crescente relevância da resiliência operacional", *Revista Electrónica de Direito (RED)*, Vol. 28, No. 2, in https://cij.up.pt/pt/red/edicoes-anteriores/2022-nordm-2/a-transformacao-digital-na-banca-e-a-crescente-relevancia-da-resiliencia-operacional/ (13/03/2025).

RODRIGUES, André Alfar, 2023, "*Manual de Inovação Financeira – Uma introdução ao universo das Criptomoedas e da Blockchain*", AAFDL Editora.

TALEB, Nassim Nicholas, 2014, *"Antifragile: Things That Gain from Disorder",* Random House Trade Paperbacks, New York.

THUAMA, Rois NI/COSTIGAN, Sean S., 2023, "DORA - Understanding the New Regulatory Framework on Digital Operational Resilience", *in https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4549564 (2/04/2025).*

TOLIN, Grace/PUNIA, Gavin/EMMANUEL, Jonathan, 2025, "EU Digital Operational Resilience Regulation (DORA)", *Global Privacy Law,* Vol. 6, No. 1, pp. 12-21.

TRAUTMANN, Kilian, 2023, "EU-DORA regulation as a result of cloud computing adoption by the financial services industry", *Journal of International Banking Law and Regulation,* Vol. 38, No. 5, pp. 155-161.

TRAUTMANN, Kilian/BOMS, Daniel, 2024, “DORA from the perspective of ICT third-party risk management”, *Journal of International Banking Law and Regulation,* Vol. 39, No. 5, pp. 182-186.