REVISTA ELECTRÓNICA DE DIREITO

RED

# A transformação digital na banca e a crescente relevância da resiliência operacional

## The digital transformation in banking and the growing relevance of operational resilience

**Maria Emília Teixeira**

Professora Auxiliar do Departamento de Direito da Universidade Portucalense, Investigadora Responsável do Projeto de Investigação "Regulação e Literacia Financeira" do Instituto Jurídico Portucalense, Coordenadora da Pós-Graduação em Direito Bancário e dos Valores Mobiliários da Universidade Portucalense

Rua Dr. António Bernardino de Almeida, 541, 4200-072 Porto, Portugal

emiliat@upt.pt

https://orcid.org/0000-0001-9127-2148

**Lara Reis**

Advogada, Diretora Central no Haitong Bank, S.A.

Rua Alexandre Herculano, 38, 1269-180 Lisboa, Portugal

lara.reis@haitongib.com

https://orcid.org/0000-0002-0178-9803

Junho de 2022

**RESUMO:** A automatização e digitalização dos processos relacionados com a prestação de serviços financeiros impõem novas formas de operar a estas entidades e impõe-lhes a capacidade para adaptarem os seus procedimentos e processos operacionais à contínua evolução tecnológica.

De entre todos os riscos associados à atividade financeira, o risco operacional assumiu particular destaque e relevância nas agendas de todos os reguladores.

Neste artigo pretendemos abordar os aspetos relevantes do ciclo da gestão de Riscos de Tecnologia da Informação e Comunicação (TIC) e analisaremos as novas perspetivas que o Regulamento DORA trouxe para responder à necessidade de densificação e harmonização de regras aplicáveis ao setor financeiro relacionadas com segurança e gestão de risco das TIC.

**PALAVRAS-CHAVE:** Transformação digital; risco operacional; resiliência operacional; Regulamento DORA; Riscos de Tecnologia da Informação e Comunicação (TIC).

**ABSTRACT:** The automation and digitalisation of procedures related to the provision of financial services impose new ways of operating on these entities and imposes on them the capacity to adapt their operational procedures and processes to the continuous technological evolution.

From among all the risks associated with financial activity, operational risk has been particularly highlighted on the work agenda of all regulators.

In our essay we seek to address the relevant aspects of the Information and Communication Technology (ICT) risk management cycle and analyse the new perspectives that the DORA Regulation brought to respond to the densification and harmonisation of rules for the financial sector related with security and ICT risk management.

**KEY WORDS:** Digital transformation; operational risk; operational resilience; DORA Regulation; Information and Communication Technology (ICT) Risks.

## SUMÁRIO:

## 1. Introdução

As entidades do setor financeiro desempenham uma atividade que, a par de interesses privados, visa a prossecução do interesse público. A automatização e digitalização dos processos relacionados com a prestação de serviços financeiros impõem novas formas de operar a estas entidades e impõe-lhes a necessidade de adaptarem os seus procedimentos e processos operacionais à contínua evolução tecnológica, o que é fundamental para manterem os níveis de credibilidade e confiança junto dos destinatários dos serviços que prestam[1].

Os desafios da necessidade de adaptação constante aplicam-se também aos reguladores e supervisores do setor. De entre todos os riscos associados à atividade financeira, o risco operacional assumiu particular destaque e relevância nas agendas de todos os reguladores e, a nível interno, tanto o Banco de Portugal como a Comissão de Mercado dos Valores Mobiliários já iniciaram diligências que visam o aumento da resiliência operacional das entidades prestadoras de serviços financeiros.

Neste artigo pretendemos abordar os aspetos relevantes do ciclo da gestão de Riscos de Tecnologia da Informação e Comunicação (TIC).

A este respeito, analisaremos as novas perspetivas que o Regulamento DORA trouxe para responder à necessidade de densificação e harmonização de regras aplicáveis ao setor financeiro relacionadas com segurança e gestão de risco das TIC.

Um outro risco que analisaremos e que tem vindo a crescer significativamente é o risco de subcontratação, que envolve a utilização de serviços de computação em nuvem, e que incorpora perigos para a estabilidade do sistema financeiro.

## 2. A Digitalização na banca: duas faces da mesma moeda

O uso de tecnologia no modo de prestação de serviços bancários é uma realidade crescente e sem retorno. Até aos dias de hoje e apesar dos riscos envolvidos, o uso de tecnologia no modo de prestação de serviços bancários não minou a confiança dos clientes bancários, a qual é determinante e essencial para o bom funcionamento do sistema financeiro.

[1] Também a este propósito, veja-se ANDRESSA JARLETTI GONÇALVES DE OLIVEIRA, ET AL., "FinTech: Desafios da Tecnologia Financeira", *in Revista de Direito Econômico e Socioambiental*, Vol. 9, N.º 2, Curitiba, PUCPR, 2018, p. 418, que refere "A recente revolução tecnológica no setor financeiro é impulsionada por vários fatores, tais como a progressiva digitalização dos serviços financeiros, a pressão por redução de custos e a mudança de perfil dos utilizadores dos serviços, sobretudo pelo ingresso das Gerações Y (Milennials) e Z (Digital Natives) no mercado. O tema tem despertado a preocupação de reguladores nacionais e internacionais, especialmente na União Europeia, gerando discussões crescentes sobre os benefícios, riscos, desafios, bem como sobre regulação e supervisão necessárias".

O surgimento e crescimento exponencial das *FinTech*[2] trouxe uma mudança radical na forma de prestação de serviços financeiros. Esta nova realidade gerou inúmeras vantagens, não só para os prestadores de serviços, mas também para os consumidores.

Por um lado, com a prestação de serviços pela via digital, o setor bancário necessita de alocar menos recursos humanos, e com isso reduz os seus custos e o risco operacional. Por outro, alterou-se o perfil do cliente bancário e consumidor de serviços financeiros, na medida em que o mesmo privilegia os meios digitais na procura e satisfação das suas necessidades[3].

Esta alteração de hábitos dos consumidores, obrigou o setor bancário a adaptar-se, mas a inovação, principalmente neste setor, deve ser acompanhada de uma forte regulação e supervisão, uma vez que os desafios se multiplicam e a isso se associa a ocorrência de novos riscos.

O uso de tecnologias inovadoras cria riscos adicionais nas atividades das instituições financeiras, considerando a complexidade dos produtos e serviços financeiros, sendo que aumenta a assimetria de informações entre fornecedores e consumidores o que requer o fortalecimento do controle e a introdução de novos métodos para sua avaliação e gestão[4].

Antever os novos riscos e regulá-los de forma preventiva com segurança e de forma completa torna-se uma tarefa árdua e implicará sempre uma colaboração estreita entre quem inova e quem regula. A regulação deve ainda ser neutra, de forma a igualar e não descriminar os diversos intervenientes, os quais podem estar submetidos ao controlo de diferentes entidades, pelo que, na regulação, há que existir cooperação também entre autoridades.

O processo de transformação digital na banca tem sido progressivo e é indispensável para o setor[5]. Inicialmente, a banca empenhou-se em desenvolver canais de comunicação e interação

---

[2] Sobre a origem do termo, veja-se SIMON FERNANDEZ VAZQUEZ, ET AL., "Blockchain in FinTech: A Mapping Study", *in Sustainability*, Vol. 11, N.º 22, Switzerland, MDPI AG, 2019, p. 6366. que refere "Financial technology, also known as 'FinTech', denotes the use of computer programs or other technology to assist the financial industry. The term was used for the first time at the beginning of the 1990s and what started as a word related solely to the financial industry, it soon expanded into other very diverse sectors. Since early 2014, the sector has started attracting the attention of regulators, industry members, customers, and academics. Blockchain in FinTech appeared for the first time as the distributed ledgers of Bitcoin, but has recently attracted consideration from practitioners and researchers. Today, financial institutions and other market participants, mainly due to the development of the blockchain technology, are approving the nature of FinTech and the necessity for research in the academic world given the implications of this technology. Financial innovation is not something new, as it has an extensive history. The development of FinTech throughout history can be divided into three main eras".

[3] A este propósito veja-se SANG M. LEE E DONHEE LEE, ""Untact": a new customer service strategy in the digital age", *in Service Business*, Vol. 14, N.º 1, Germany, Springer Science and Business Media LLC., 2019, p. 3: "Customers have different preferences for service during the encounter depending on the type of help needed, personal knowledge about the product or service under purchase consideration, and even their psychological characteristics (e.g., extrovert/introvert). Many technology savvy customers search various information sources on the Web and often know much more about the various aspects of the interested product or service than friendly salespersons at the store. Busy professionals or homemakers prefer to spend as little time for shopping as possible without the interference of store employees. As the number of one-person households increases, these customers greatly value simplicity, efficiency, cost-effectiveness, and time management".

[4] Neste sentido, veja-se SVITLANA MISHCHENKO ET AL., "Innovation risk management in financial institutions", *in Investment Management and Financial Innovations*, Volume 18, Issue 1, Ukraine, LLC CPC Business Perspectives, 2021, p. 190.

[5] Também neste sentido, veja-se DEUTSCHE BANK RESEARCH, *Fintech – The digital (r)evolution in the financial sector Algorithm-based banking with the human touch*, p. 33, Frankfurt am Main, 2014, in https://www.finextra.com/finextra-downloads/featuredocs/prod0000000000345837.pdf (27.01.2022) onde se refere "There are a lot of reasons why a digitisation strategy for banks is indispensable in the 21st century. No doubt, what matters is, among other things, the optimisation of process and cost structures as well as the adaptation to rising data volumes. Furthermore, the change in customer demands is an equally decisive factor as the new competition conditions in the market for standardised financial services"

com o cliente e novos produtos. De seguida, aprimorou e adaptou a sua infraestrutura tecnológica. Atualmente, a banca tem como desígnio traçar a sua estratégia de posicionamento digital face ao surgimento de novos *players* na prestação de serviços concorrentes às atividades que o setor bancário empreende, designadamente no que concerne à intermediação financeira. Novos *stakeholders* a operar no setor, como as *FinTechs* e *BigTechs*, são atualmente os principais concorrentes da banca tradicional, que impõem a esta novos padrões de prestação de serviços, demandando respostas vinte e quatro horas por dia, sete dias por semana, trezentos e sessenta e cinco dias por ano.

O uso de tecnologias disruptivas viabiliza um maior conhecimento dos interesses dos clientes bancários e permite que o setor se ajuste às necessidades, conduzindo a uma prestação de serviços direcionada e otimizada[6], como é o caso do uso de dados associados à tecnologia *Big Data*[7] e *Analytics* ou da inteligência artificial.

Por sua vez, o fenómeno das *distributed ledger tecnhologies*[8], como a *blockchain*[9], aplicadas no processo de prestação de serviços bancários, faculta, a priori, uma maior segurança das transações, não obstante todas as recentes questões jurídicas que o uso de tal tecnologia suscita na legalidade e responsabilidade pelas operações executadas[10].

[6] A este propósito veja-se HOSSEIN HASSANI, ET AL., "Banking with blockchain-ed big data", *in Journal of Management Analytics*, Vol. 5, N.º. 4, Londres, Taylor & Francis Group, 2018, pp. 260, que menciona "blockchain can enable banks to share customer information across their company securely and thereby simplify the administrative process by reducing unnecessary duplication of information and requests. Blockchain helps cut down on duplication as it can allow the independent verification of one client by one bank to be accessed by other banques(…)".

[7] Sobre este assunto, refere ANDRESSA JARLETTI GONÇALVES DE OLIVEIRA, ET AL., "FinTech: Desafios da Tecnologia Financeira", *in Revista de Direito Econômico e Socioambiental*, Vol. 9, N.º 2, Curitiba, PUCPR, 2018, pp. 419 e 420, que "(…) quanto aos serviços financeiros, a utilização de recursos de big data é uma forte tendência, seja para avaliação de risco ou formação de scoring dos clientes. Apesar das vantagens de tal aplicação, reduzindo custos e tempo na análise de dados, há também uma série de desafios, tais como a confiabilidade dos dados coletados pela internet, a ausência de neutralidade dos algoritmos programados para realização da análise, bem como a proteção de dados pessoais, especialmente ante a proximidade de entrada em vigência do novo Regulamento Geral sobre a Proteção de Dados na União Europeia".

[88] Veja-se FÁTIMA LEAL, ET AL., "Decentralisation of FinTech Business Models", *in Lecture Notes in Networks and Systems*, Singapura, Springer Nature Singapore, 2022, p. 350, que a referem "Decentralisation has been seen as the future in several domains. It relies on Distributed Ledger Technology (DLTs) which aim to interact directly with the final client eliminating intermediary entities such as agents, brokers, or bankers. DLTs enable the application of decentralised business models where authorised network members have access to the distributed ledger without relying on a single or centralised authority. Specifically, the distributed ledger uses a peer to-peer environment which is continuously updated and synchronised".

[9] Veja-se sobre este propósito DELBER PINTO GOMES, "Contratos ex machina: breves notas sobre a introdução da tecnologia Blockchain e Smart Contracts", *in Revista Electrónica de Direito*, Vol. 17, N.º 3, Porto, 2018, p. 45, que menciona que "A Blockchain é uma tecnologia polivalente destinada a tornar as transações fiáveis e seguras, sendo que um dos grandes segmentos das transações que se pretendem fiáveis e seguras são precisamente os contratos. Blockchain, enquanto base de dados distribuída (descentralizada), garante a imutabilidade das cadeias de informação que a compõem, através de sistemas de verificação algorítmica e criptográfica. Trata-se de uma tecnologia com um elevado grau de segurança, que a tornam atualmente no método informático mais fidedigno para o registo de informações, evidenciado pela sua crescente utilização em grande escala em diversos setores de atividade e, em particular, no sector financeiro".

[10] Neste sentido, veja-se NIKITA RAJESHKUMAR BAGRECHA, ET AL., "Decentralised Blockchain Technology: Application in Banking Setor", *in 2020 International Conference for Emerging Technology (INCET)*, India, IEEE, 2020, p. 1, que refere "The blockchain technology is a peer-to-peer distributed structure which could be used to overcome the issue in the traditional banking system. It is a collection of blocks that hold the encrypted transactional details sharing the same timestamp. The nodes of the network (miners) are responsible for linking the blocks to one another in chronological order, where each block contains the hash of the block created before in the chain. These hash values are the digital signature of each block and are dependent on two variables, first being the transactional details, and second is the hash value of the previous block".

Mas a atual prioridade do setor bancário situa-se ao nível da gestão reputacional das instituições, bem como na gestão do risco operacional, sendo fundamental deter meios capazes de prevenir e resistir à ocorrência dos mesmos.

De seguida abordaremos a importância da existência de mecanismos de resiliência operacional.

## 3. Os princípios da resiliência operacional

### 3.1. Enquadramento

A resiliência, entendida como a "*capacidade de reagir e superar contrariedade ou situação de crise*" e a "*faculdade de quem consegue lidar de forma positiva com fatores ou condições adversas*"[11], assume especial relevo para as entidades do setor financeiro[12]. Pela importância económico-social de que se revestem, é de interesse público que os bancos estejam dotados da capacidade necessária para criar, assegurar e reavaliar a integridade dos seus processos operacionais, de gestão e comerciais. Além disso devem ser capazes - direta ou indiretamente - de manter esses processos operacionais em curso, e com a mesma qualidade, durante a eventual ocorrência de um incidente[13].

No rescaldo da crise financeira de 2008 — a qual veio expor fragilidades ao nível da gestão, fiscalização e governo interno dos bancos — o legislador e os reguladores europeus preocuparam-se sobretudo em reforçar a resiliência financeira do setor financeiro. Para isso, avançaram com a introdução de medidas destinadas ao reforço dos recursos financeiros e de liquidez dos bancos e à adequada gestão dos riscos de crédito e de mercado.

Mais recentemente, tem-se verificado um maior enfoque dos reguladores na resiliência operacional dos bancos. Efetivamente, as circunstâncias em que os bancos operam e os desafios que enfrentam hoje, trouxeram à luz do dia novas preocupações: (i) a crescente dependência de tecnologia; (ii) a inevitável automatização e digitalização dos processos — quer ao nível da sua relação com os clientes, quer a nível operacional —; (iii) a oferta de mais canais (e uma mais intensa utilização desses canais, como se verificou em virtude da obrigatoriedade de trabalho remoto durante a pandemia de COVID-19) que funcionam como pontos de entrada para ataques externos; e (iv) a relação de interdependência entre os bancos e um pequeno número de grandes empresas que prestam serviços de tecnologias de

[11] PORTO EDITORA, "resiliência" no *Dicionário Infopédia da Língua Portuguesa* [em linha]. Porto: Porto Editora. [consultado a 2022-01-07 18:23:50]. Disponível em https://www.infopedia.pt/dicionarios/lingua-portuguesa/resiliência.

[12] Doravante referir-nos-emos sobretudo a "bancos" por uma questão de simplificação da linguagem, mas entenda-se que tais referências são igualmente aplicáveis a todas as outras instituições supervisionadas pelo Banco de Portugal.

[13] As referências a "incidente" neste texto poderão ser uma avaria, sobrecarga, falha, perturbação, degradação, utilização abusiva, perda ou outro tipo de evento doloso ou não doloso, que comprometa a segurança das redes ou dos sistemas de informação, o funcionamento e a execução de processos, a prestação de serviços ou a integridade e disponibilidade de dados, programas ou outras componentes de serviços e infraestruturas.

informação e comunicação ("TIC") ao setor financeiro. Por outro lado, a atividade dos bancos desenvolve-se em ciclos que pressupõem mudança e transformação regulares (por exemplo, das atividades que desenvolvem e dos serviços que prestam, dos mercados e países nos quais operam, dos seus processos internos, dos sistemas que utilizam, da composição da equipa de gestão) e esses ciclos devem ser geridos de forma sustentada, holística e com base numa análise de riscos, para integrarem medidas de mitigação do risco operacional inerente.

Ora, os bancos estão, por estas razões, cada vez mais vulneráveis ao risco operacional, o que trouxe a resiliência operacional para o topo da agenda dos reguladores do setor financeiro. No contexto nacional, o Banco de Portugal[14] divulgou que uma das prioridades de supervisão para 2022 será a resiliência cibernética e a CMVM identificou no seu "Risk Outlook para 2022" o risco associado à digitalização como um dos principais riscos que as empresas de investimento terão de gerir este ano.

O maior enfoque na importância da resiliência operacional do setor financeiro também tem tido reflexos ao nível legislativo. A CRD[15] e o CRR[16], embora não previssem disposições específicas relativas à gestão de riscos TIC nem à segurança de sistemas e dados, introduziram requisitos genéricos ao nível de governo interno e de gestão de risco operacional, que anteciparam obrigações que apareceram em regulamentação posterior, visando especificamente a gestão dos riscos TIC. Por exemplo, a Diretiva dos Serviços de Pagamento (DSP2)[17], veio introduzir algumas regras para a gestão de riscos operacionais e de segurança no âmbito da prestação de serviços de pagamento. No entanto, deixou de fora a regulamentação de todos os outros serviços prestados pelos bancos.

Em paralelo, a Diretiva NIS[18], não específica do setor financeiro, aplica-se às instituições que qualifiquem como operadores de serviços essenciais, o que pode incluir os bancos. A sua transposição para Portugal através do Regime Jurídico da Segurança do Ciberespaço teve o mérito de esclarecer eventuais dúvidas sobre o seu âmbito de aplicação: ao definir uma lista de operadores de serviços essenciais, entre os quais se incluem todas as instituições de crédito, ficou claro que abrange todas estas entidades independentemente da sua dimensão. O Regime Jurídico da Segurança do Ciberespaço estabeleceu os princípios gerais aplicáveis à segurança do ciberespaço, que depois foram concretizados com maior detalhe no Decreto-Lei n.º 65/2021, de 30 de julho, que estabeleceu obrigações de reporte ao CNCS[19], critérios e regras para a notificação de incidentes e a obrigatoriedade de proceder a análises de risco em relação

[14] BANCO DE PORTUGAL, Relatório de Estabilidade Financeira, Lisboa, 2021, in https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/ref_12_2021_pt.pdf (17.01.2022)
[15] Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013.
[16] Regulamento (UE) 575/2013 do Parlamento Europeu e do Conselho 26 de junho de 2013 relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento.
[17] Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho de 25 de novembro de 2015 relativa aos serviços de pagamento no mercado interno. Esta Diretiva foi transposta para o ordenamento nacional pelo Decreto-Lei n.º 91/2018 ("Regime Jurídico dos Serviços de Pagamento").
[18] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União. Esta Diretiva foi transposta para o ordenamento nacional pela Lei n.º 46/2018, de 13 de agosto.
[19] Centro Nacional de Cibersegurança.

a todos os ativos que garantam a continuidade do funcionamento das redes e dos sistemas de informação.

A proposta de Regulamento DORA[20] vem agora responder à necessidade de densificação e harmonização de regras aplicáveis ao setor financeiro relacionadas com segurança e gestão de risco das TIC, até agora dispersas por legislação europeia e nacional. Os seus pilares assentam numa adequada gestão de riscos TIC, na gestão de riscos de terceiros, na realização de testes da resiliência operacional e na harmonização da terminologia, critérios, prazos e modelos de reporte de incidentes. Mas a grande novidade deste regulamento é a sua aplicação não só às entidades financeiras, mas também às empresas terceiras prestadoras de serviços TIC, trazendo assim estas empresas pela primeira vez para o perímetro de supervisão dos reguladores financeiros[21].

Embora o Regulamento DORA venha atribuir um maior destaque à necessidade de garantir a resiliência operacional e introduza requisitos específicos para este fim; já existia a expetativa por parte dos reguladores do setor financeiro de que os bancos fizessem uma adequada gestão de riscos TIC e sendo expectável os bancos têm apresentado um bom nível de maturidade na implementação destas matérias.

Nos capítulos que se seguem procuraremos tocar aspetos relevantes para todas as fases do ciclo da gestão de riscos TIC – a identificação, classificação e documentação; a proteção e prevenção; a deteção; a resposta e recuperação; a evolução, aprendizagem e comunicação – quer à luz daquilo que são já hoje as boas práticas seguidas pela indústria, assim como das novas perspetivas que o Regulamento DORA nos traz.

## 3.2. Governo Interno

O governo interno diz respeito à forma como os bancos estão organizados e conduzem os seus processos internos de gestão, decisão e execução, nomeadamente os passos que devem ser dados em cada processo interno, quem deve ser envolvido, e quando, para identificar, aprovar, executar e monitorizar esses passos e quem tem responsabilidade pelos processos. Esta organização interna é enquadrada pelos resultados da autoanálise regular de riscos que os bancos devem fazer, no âmbito da qual identificam os riscos a que estão expostos, classificam-nos de acordo com a sua probabilidade de ocorrência e impacto e determinam os processos e controlos internos para endereçar esses riscos.

[20] Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro e que altera os regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 e (UE) n.º 909/2014, COM (2020) 595 final. Esta proposta encontra-se, à data da elaboração deste texto, a seguir o processo legislativo ordinário, prevendo-se uma versão final até ao início de 2023.
[21] A EBA, a ESMA ou a EIOPA serão nomeadas como autoridade fiscalizadora principal para cada entidade terceira prestadora de serviços no domínio das TIC considerada crítica. As autoridades de supervisão nacional acompanharão determinações e recomendações feitas às entidades terceiras através das entidades financeiras que supervisionam.

O caminho para alcançar resiliência operacional numa organização começa na definição da sua visão, valores e prioridades, como seus pilares fundamentais, e que devem refletir a realidade e a cultura do banco. Isto porque a resiliência operacional não tem que significar necessariamente o mesmo para todos os bancos, ao invés, dependerá das suas prioridades, que poderão estar mais voltadas para a satisfação do cliente, para a otimização da *performance* e desempenho financeiro ou até mesmo para a eficiência dos processos, para identificar alguns exemplos. Além disso, a resiliência operacional não deve orientar-se apenas para o fim último do estrito cumprimento de obrigações regulatórias (cumprir com a letra da lei), pois a resiliência operacional deve ser sustentável e de longo prazo e atender ao espírito da lei e à prossecução do propósito corporativo.

Posto isto, é ao órgão de gestão dos bancos que caberá em primeiro lugar a definição destes pilares que estão na base da construção de uma cultura de resiliência operacional, recaindo também sobre este órgão a responsabilidade de garantir a sua salvaguarda. Para este efeito, é o órgão de gestão que deve aprovar as políticas internas que estabelecem a estratégia, os princípios, os valores e os objetivos para a resiliência operacional e que deve tomar as medidas necessárias para implementar essas políticas. Estas medidas vão desde a criação de procedimentos internos; à determinação do nível de apetência ao risco; à aprovação de planos de contingência e continuidade de negócio; à aprovação de planos de auditoria; à delegação de poderes em comités especializados ou noutra unidade da estrutura da organização; e à alocação de recursos financeiros e humanos, em quantidade e qualidade suficientes para esse fim. Adicionalmente, também lhe compete um acompanhamento próximo das medidas tomadas, promovendo o "*tone from the top*" e assegurando que lhe são feitos reportes regulares sobre estas matérias.

A existência de um membro no seio do órgão de gestão que tenha conhecimentos académicos e experiência profissional em matérias técnicas e aspetos regulatórios relacionados com TIC, deve ser um fator a considerar no momento da composição da equipa de administradores, por ser determinante para um envolvimento ativo da liderança nestas matérias.

A comunicação interna complementa outros aspetos de governo interno que foram referidos anteriormente, e, sendo eficaz, transparente, clara e frequente, cumpre um papel fundamental na divulgação, compreensão e adesão de todo o *staff* às normas internas e à cultura da instituição. Promover uma cultura de transparência, não só favorece uma autorregulação como também favorece um clima de confiança que encoraja todas as pessoas da organização a reportar e escalar situações que mereçam atenção e desencadeamento de alerta. A este respeito, acrescentamos que investir em formação interna, sobretudo encorajando uma aprendizagem com os erros passados, evita que incidentes sejam ocultados e que se perpetuem.

Finalmente, destacamos alguns aspetos relacionados com a distribuição de tarefas e organização interna de equipas, que, sendo boas práticas de governo interno, se revestem de especial relevância para a gestão de situações de crise. Desde logo, devem estar claramente

identificadas e alocadas todas tarefas, devem ser definidas responsabilidades de monitorização e linhas de reporte, tendo em conta a experiência e a senioridade individuais e eventuais situações de conflito de interesses que possam, desde logo, ser mitigadas. Estabelecer regras de rotatividade de *staff* - entre equipas, de tarefas ou entre geografias - permite adicionalmente uma partilha de experiências e evita uma redução do nível de alerta para o risco provocado por uma execução repetida de determinadas tarefas num mesmo contexto.

Devem ser criadas todas as condições para que o trabalho de equipa, e entre equipas, seja harmonioso e articulado, nomeadamente pela existência de canais de partilha de informação que funcionem de forma fluida e eficiente e façam chegar a informação certa, às pessoas certas, no momento certo. Sobretudo perante um incidente, a comunicação e a rápida articulação para troca de informações, são cruciais para garantir uma tomada de decisões informadas e o controlo do incidente. Torna-se assim essencial nomear uma pessoa com responsabilidade de coordenação e gestão de situações de crise, que assegure a centralização das operações e coordene a reação e a resposta de forma concertada. O Regulamento DORA traz ainda uma novidade a respeito de organização interna ao prever a criação de um cargo que tenha a responsabilidade de monitorizar os serviços TIC que estejam subcontratados a terceiros.

## 3.3. Planeamento

Uma organização melhor preparada conseguirá navegar mais facilmente uma situação de crise provocada pela ocorrência de um incidente, pelo que o planeamento é um dos princípios chave da resiliência operacional.

O primeiro vetor do planeamento é a existência de um conjunto de normas que transponham para a realidade interna as exigências legais e regulamentares, adaptando-as às atividades prosseguidas pela organização, ao seu perfil de risco, à dimensão e complexidade da sua estrutura. Essas normas internas devem ser abrangentes e claras, e regularmente revistas para garantir a sua atualidade face a desenvolvimentos legislativos ou organizacionais. Devem também ser divulgadas a toda a organização, estar arquivadas de forma estruturada e disponíveis a todo o tempo para consulta.

O normativo interno identifica os princípios e valores fundamentais da organização que, sendo os pilares de uma estratégia de segurança, todas as pessoas na estrutura devem conhecer e integrar nas decisões que tomam. O detalhe dos passos a tomar, a responsabilidade por cada tarefa e as linhas de reporte internas e externas, são definidos em procedimentos no âmbito de planos de contingência e continuidade de negócio. O conjunto de normas internas deve consubstanciar uma abordagem integrada e estruturada da instituição e do grupo onde esta se insere.

Deve ser antecipadamente definido em normativo o estabelecimento de métricas para avaliar internamente o impacto de um incidente. As métricas assentam em critérios que vão desde a duração da disrupção; ao volume de dados comprometidos e de danos atuais ou futuros; e ao número de clientes afetados. Este exercício de autoanálise do impacto que um incidente pode ter, permite identificar processos e funções mais críticos, cuja interrupção (ainda que de curta duração) possa comprometer a continuidade da atividade, afetar gravemente a sua reputação, causar um grave prejuízo financeiro e conduzir à perda de clientes. É importante definir níveis de tolerância ao risco e tolerância à disrupção de cada processo ou função considerado crítico. Por outro lado, a determinação da severidade de um incidente permite definir um prazo máximo de resposta e a quem deve escalar-se o incidente.

O planeamento passa também por ter uma visão holística e permanentemente atualizada da estrutura organizacional. Esta visão global implica a identificação, classificação e documentação: de todas as pessoas relevantes; das funções que desempenham; dos processos (identificando o seu nível de criticidade); dos sistemas e dos seus utilizadores, das infraestruturas nas quais assentam as atividades prosseguidas e dos equipamentos físicos. Este exercício permite também identificar a todo o tempo quaisquer falhas ou necessidades adicionais de recursos humanos ou técnicos.

Finalmente, uma análise de cenários potenciais de crise (variando a natureza, severidade, duração e perfil de risco) e a realização regular de testes às pessoas e aos sistemas (estes testes podem ser avaliações e análises de vulnerabilidade, análises de fonte aberta, avaliações da segurança das redes, análises das lacunas, análises da segurança física, questionários e programas informáticos de análise, revisões do código fonte, testes com base em cenários, testes de compatibilidade, testes de desempenho ou testes de extremo a extremo ou testes de penetração), permite a identificação antecipada de eventuais fragilidades na capacidade de prevenção, deteção, resposta ou recuperação das instituições e um melhoramento contínuo dos processos.

O Regulamento DORA sugere que as entidades deverão criar os seus programas de testes regulares da resiliência operacional proporcionalmente às necessidades que decorrem da sua dimensão, áreas de negócio e perfil de risco, podendo, quando necessário, recorrer a terceiros especializados para a realização desses testes.

## 3.4. Gestão de dependências de terceiros

De acordo com informação divulgada pelo Banco de Portugal, o peso da subcontratação (*outsourcing*) nas áreas de informação, digitalização e cibersegurança verificado nos maiores

bancos em Portugal, é superior a 60%[22]. É inevitável que os bancos dependam cada vez mais dos serviços tecnológicos prestados por terceiros, primeiro porque não é sua vocação a prestação de serviços tecnológicos e porque não têm os meios (financeiros e humanos) para acompanhar o ritmo de desenvolvimento de uma indústria que está em profunda transformação. Além disso, o recurso a terceiros especialistas neste tipo de serviços garante maior sucesso na otimização dos seus processos, uma maior eficiência na relação entre custos e benefícios e o acesso a uma oferta de serviços que vai de encontro às novas expetativas dos consumidores, sobretudo das gerações de *millenials* ou *digital natives*.

Os serviços procurados juntos das empresas tecnológicas são uma fatia importante no universo de atividades, vão desde o armazenamento de dados e infraestrutura, à gestão de redes, à análise de dados e disponibilização de software. Este tipo de serviços e ferramentas assumem especial relevância na gestão das relações contratuais com clientes, mas também são frequentemente utilizados na monitorização do cumprimento normativo e regulatório e na execução de operações como crédito ou negociação de valores mobiliários.

Particularmente significativo tem sido o crescimento da subcontratação envolvendo a utilização de serviços de computação em nuvem, que oferecem a possibilidade de distribuir os centros de dados por várias geografias e assim reduzir o risco operacional resultante de concentração geográfica. Além disso, a utilização da nuvem permite reduzir custos com manutenção de infraestrutura e, sendo uma opção de gestão mais ágil, permite uma canalização de recursos para outras áreas. As vantagens que a computação em nuvem oferece tornam esta uma opção muito apetecível, mas este tipo de decisões deve ser acompanhado de uma adequada análise e gestão dos riscos que também traz associados.

Vejamos então em maior detalhe os riscos que a subcontratação acarreta para a estabilidade do sistema financeiro. Desde logo, a partilha ou acesso por parte de um terceiro a informação sensível e/ou em larga escala que seja detida por um banco, aumenta a vulnerabilidade da segurança dessa informação, e o risco de atos fraudulentos e práticas ilícitas, tendo como alvo qualquer um de nós, como clientes bancários.

A subcontratação é com frequência feita para empresas com presença transfronteiriça, o que traz desafios decorrentes de diferenças legislativas entre os países e problemas de determinação de lei e jurisdição aplicáveis a esses serviços. Nomeadamente, a dispersão geográfica de dados entre países que não oferecem garantias semelhantes de proteção, nem beneficiam de igual controlo por parte de entidades de supervisão, pode dificultar a manutenção da segurança e confidencialidade desses dados.

Com a externalização para um terceiro de processos internos, naturalmente há um distanciamento por parte banco em relação a esses processos, pois a sua execução regular deixa de estar diretamente na sua esfera. A confiança de que esses processos estariam nas "boas mãos" de terceiros conduziu no passado a uma perda de controlo por parte dos bancos

[22] Segundo informação divulgada no Relatório de Estabilidade Financeira do Banco de Portugal, publicado em dezembro de 2021, p. 76.

e à dependência excessiva das empresas subcontratadas, por falta de *expertise* interna; tornando os bancos, de certa forma, "reféns" dessas empresas (*lock-in risk*). Por outro lado, as empresas subcontratadas estando conscientes desta dependência, foram chamando a si um poder desequilibrado na relação contratual com os bancos, com consequências ao nível dos direitos dos bancos nesses contratos e de um relaxamento do cumprimento das obrigações por parte das empresas terceiras. Sem falar do risco da concentração da prestação de serviços TIC num pequeno grupo de gigantes tecnológicos, o que, em caso de alguma falha ou ataque a esses prestadores de serviços[23], teria impactos sistémicos nefastos.

Embora sendo consensual que a subcontratação não deve pressupor uma transferência da *responsabilidade* dos processos da esfera do banco para terceiros, na prática a dinâmica da subcontratação era muitas vezes distinta. A MiFID II[24] introduziu pela primeira vez o princípio de que a subcontratação de funções importantes não poderia ser feita "de um modo que prejudique materialmente a qualidade do […] controlo interno ou a capacidade de a entidade supervisora controlar", mas foram as orientações da EBA relativas a subcontratação[25] (as quais integraram recomendações anteriores relativas à subcontratação de prestação de serviços de computação em nuvem[26]) e as orientações da EBA sobre TIC e gestão de riscos de segurança[27] que densificaram os requisitos aplicáveis a esta figura. Entre outros, formalizou-se a necessidade de uma análise prévia com vista a determinar o nível de importância e criticidade do serviço a subcontratar e a necessidade de uma *due diligence* ao subcontratante para aferir a qualidade e suficiência dos seus meios para executar os serviços planeados. Além disso, estabeleceu-se que o contrato de subcontratação deve ter um conteúdo mínimo, garantindo ao banco os direitos necessários para a monitorização dos serviços (como por exemplo, direitos de informação, inspeções ou auditorias) e impondo à entidade subcontratada um conjunto de obrigações. No entanto, estas orientações da EBA têm apenas natureza recomendatória, pelo que o Regulamento DORA pretende resolver um vazio regulatório em relação a algumas matérias relacionadas com subcontratação.

Esta proposta de regulamento prevê que as autoridades de supervisão possam, quando a criticidade dos serviços prestados o justifique, fazer auditorias e inspeções diretamente aos prestadores de serviços TIC, possam emitir recomendações e determinações específicas, aplicar-lhes sanções e impor a cessação de contratos de subcontratação. Este alargamento da autoridade dos supervisores financeiros a terceiros que prestem serviços aos bancos é uma novidade na Europa e já suscitou preocupação por parte dos supervisores em relação à sua

[23] De acordo com o relatório da AGÊNCIA DA UNIÃO EUROPEIA PARA A CIBERSEGURANÇA (ENISA), *ENISA Threat Landscape For Supply Chain Attacks*, de julho 2021, estima-se que em 2021 tenha havido 4 vezes mais ataques a fornecedores do que em 2020 e que a tendência seja para um crescimento exponencial destes ataques.
[24] Diretiva 2014/65/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa aos mercados de instrumentos financeiros.
[25] Orientações da EBA relativas à subcontratação, de 25 de fevereiro de 2019 (EBA/GL/2019/02).
[26] Recomendações relativas à subcontratação externa a prestadores de serviços de computação em nuvem (EBA/REC/2017/03).
[27] Orientações da EBA relativas à gestão dos riscos associados às TIC e à segurança, 28 November 2019 (EBA/GL/2019/04).

implementação, mas esta é uma solução já aplicada, embora com algumas diferenças[28], nos EUA.

Adicionalmente, o regulamento vem estabelecer alguns aspetos que devem ficar acordados contratualmente entre o banco e o terceiro subcontratado, como por exemplo, quais as estratégias de saída, o direito de rescisão contratual ou de substituição e os direitos de acesso, inspeção e auditoria.

Cabe aos bancos uma adequada gestão interna e um acompanhamento contínuo dos vários serviços subcontratados, pelo que devem dispor de uma lista exaustiva destes serviços e identificar eventuais interconexões entre empresas terceiras e outras entidades financeiras.

## 4. Gestão de Incidentes

As repercussões de um incidente que afete serviços TIC podem ser devastadoras a vários níveis e alastrar-se a todo o sistema financeiro. Um incidente desta natureza pode ter origem não maliciosa, se resultar de uma falha ou disrupção, ou maliciosa, se resultar de um ataque com um propósito criminoso. Um incidente pode conduzir a vários danos e prejuízos, para além de custos com processos judiciais, custos com ações para remediar os danos sofridos, perdas de receita futura e aplicação de sanções. Adicionalmente, num incidente de origem maliciosa também há maior probabilidade de um impacto financeiro mais direto e imediato, como a retirada de fundos (próprios ou de clientes do banco) se esse for o propósito do ataque.

A nível operacional, um incidente muito provavelmente implicará falhas em aplicações e redes ou na integração de sistemas, o que levará uma disrupção de certas funções internas por um determinado período de tempo, sendo a sua gravidade maior ou menor consoante a criticidade dessas funções e a duração da interrupção das mesmas.

As dificuldades na prossecução normal das atividades podem impossibilitar o cumprimento de reportes, de outros prazos regulatórios ou de obrigações legais (face a clientes ou fornecedores) o que, por seu lado, poderá desencadear processos contraordenacionais e judiciais.

Finalmente, a circunstância de estar envolvido num incidente relacionado com segurança de informação ou divulgação de dados confidenciais ou sensíveis, tem implicações reputacionais sérias e seguramente demorará muitos anos a recuperar a confiança perdida e a reconstruir uma imagem que invariavelmente sai fortemente degradada.

[28] Para uma análise do enquadramento da supervisão nos EUA, cfr. *FFIEC IT Examination Handbook InfoBase, Administrative Guidelines: Implementation of Interagency Programs for the Supervision of Technology Service Providers*, 2012 in https://ithandbook.ffiec.gov/media/153533/10-10-12_-_administrative_guidelines_sup_of_tsps.pdf (26.01.2022).

Vejamos com mais detalhe as componentes do processo de resposta e recuperação de um incidente.

## 4.1. Reação

A exatidão e a tempestividade são dois princípios fundamentais na gestão de um incidente, particularmente relevantes no momento da reação. Perante a verificação de um incidente, é necessário assegurar que as ações tomadas são rápidas e oportunas, executadas de forma rigorosa, assertiva e eficaz e são assentes em dados fidedignos. Um incidente despoleta a execução da política de continuidade das atividades.

Na fase de reação a prioridade é ativar os planos específicos que ponham em marcha medidas, processos e tecnologia capaz de conter as consequências adversas do incidente, quer a nível interno, quer o seu alastramento para outras entidades do mesmo grupo ou até para entidades externas. As medidas de mitigação do impacto de incidentes prescrevem o que deve ser feito em determinadas situações, nomeadamente podem determinar se certos serviços devem ser suspensos ou mantidos atendendo à sua criticidade; indicam se certos fornecedores devem ser substituídos ou se os serviços que prestam devem ser internalizados; ou se devem isolar-se redes ou sistemas no caso de estarem comprometidos.

A existência de uma lista atualizada de quem deve ser informado internamente (como por exemplo membros de órgãos sociais, linhas de negócio, equipas de apoio técnico ou de apoio ao cliente, diretor jurídico, responsável de Compliance, responsável pela proteção de dados ou responsável pelas relações com investidores) e externamente (como por exemplo clientes, contrapartes, credores, fornecedores, autoridades nacionais ou público em geral), quando devem ser feitas comunicações e em que circunstâncias, assegura uma gestão eficaz da comunicação no momento de crise. Devem ser também previamente definidos quais os canais de comunicação que serão utilizados e se serão feitas comunicações aos meios de comunicação social. Podem ser preparados modelos de reporte ou mensagens tipo que facilitam a preparação das comunicações.

Durante todo o processo de reação, a comunicação regular com os vários *stakeholders* é fundamental, e pode ter em vista diferentes finalidades como a troca de informações sobre as ações empreendidas e os resultados obtidos, ou a gestão dos fatos que são do conhecimento público no sentido de assegurar que, havendo uma atualização sobre os desenvolvimentos, se evita a extrapolação dos acontecimentos. A granularidade da informação prestada a cada momento, a frequência da comunicação e a linguagem utilizada devem ser adequadas ao público alvo, mas veremos com maior detalhe os requisitos específicos dos reportes que devem ser feitos aos reguladores e outras entidades.

As circunstâncias do incidente podem tornar necessária a ativação dos locais de contingência, que são locais alternativos dotados dos recursos, capacidades e funcionalidades para replicar os sistemas mais críticos dos escritórios principais.

A capacidade de reação a um incidente pode medir-se utilizando critérios objetivos e numéricos, como por exemplo: (i) o volume de incidentes que foram detetados e resolvidos de forma automática (i.e. sem intervenção humana) através dos sistemas de segurança implementados; (ii) o período de tempo decorrido entre a existência da ameaça e a deteção da mesma (dwell time); (iii) o objetivo de tempo de recuperação (RTO)[29] e (iv) objetivo do ponto de recuperação (RPO)[30].

Depois de extraídas e guardadas as evidências necessárias que permitam investigar as causas que estiveram na origem do incidente, devem ser removidos todos os expedientes introduzidos pelo atacante.

## 4.2. Registo e Reporte

Na pendência da ocorrência de um incidente deve procurar assegurar-se, tanto quanto possível, o registo do maior número de informação sobre as ações e decisões tomadas nas várias fases do processo. Idealmente por um observador independente, que não esteja diretamente envolvido na resposta ao incidente e que esteja, portanto, desejavelmente distanciado dos fatos. Para além deste registo funcionar como uma evidência da forma como foi conduzida a resposta ao incidente, para efeitos de reportes e inspeções ou auditorias, serve igualmente como um documento de suporte para a avaliação global do desempenho do processo e para um apuramento de responsabilidades e identificação de eventuais aspetos que careçam de melhorias.

Para o registo e reporte de incidentes existe taxonomia específica que procura harmonizar a classificação dos incidentes e do seu grau de severidade. A harmonização da terminologia visa garantir a consistência das comunicações e a comparabilidade dos reportes. Um incidente é classificado consoante as causas que estiveram na sua origem, podendo estas ser, por exemplo, uma falha de sistema, um erro humano, um ataque malicioso, fenómeno natural ou uma falha no fornecimento de bens ou serviços por terceiro; mas também atendendo à forma de ataque, se o mesmo foi veiculado por um vírus, *malware*, *worm* ou *hyperlink*, e aos canais utilizados para o ataque, como o email ou web browser. Além disso, também se consideram o tipo de incidente, se se trata de um *zero-day attack*, a exploração de uma vulnerabilidade ou um incidente isolado; e a intencionalidade que possa ter motivado o ataque, se maliciosa, uma

[29] RTO é o atraso máximo aceitável entre a interrupção do serviço e a restauração do serviço. Isso determina o que é considerado uma janela de tempo aceitável quando o serviço está indisponível.
[30] RPO é o tempo máximo aceitável desde o último ponto de recuperação de dados. Isso determina o que é considerado uma perda aceitável de dados entre o último ponto de recuperação e a interrupção do serviço.

atividade fraudulenta, tentativa de roubo, motivações políticas, ativismo ou espionagem. Finalmente a identificação do autor do ataque como sendo um amador, um criminoso, um *hacktivist*, ou mesmo um estado, permite enquadrar a intencionalidade do mesmo.

Um incidente poderá ter que ser reportado ao Banco de Portugal[31], ao CNCS[32] e à Comissão Nacional de Proteção de Dados[33], dependendo da sua natureza, classificação e impacto. O Regulamento DORA pretende introduzir regras normalizadas para o reporte de incidentes relacionados com TIC.

## 4.3. Recuperação e evolução

Os procedimentos de recuperação devem ser previamente definidos e aprovados no contexto da fase de planeamento identificada *supra*. Estes procedimentos devem ser regularmente testados para deteção de falhas e identificação de oportunidades de melhoria, bem como para a sua atualização contínua face a desenvolvimentos regulatórios ou de negócio. A existência de procedimentos definidos com detalhe, evita o recurso ao improviso e minimiza o risco de erro humano.

Para facilitar a restauração de dados no processo de recuperação, deve assegurar-se que são implementadas políticas de cópias de segurança que definem a frequência com que essas cópias são feitas e os dados que devem ser abrangidos.

Estes procedimentos devem estabelecer as prioridades na fase de recuperação, atendendo à criticidade dos serviços e/ou processos e à necessidade de restabelecimento desses serviços ou processos, sobretudo quando estejam em causa o incumprimento de obrigações regulatórias, impacto económico relevante ou um número alargado de clientes ou utilizadores afetados.

Os planos de recuperação devem incluir objetivos e metas a atingir, nomeadamente para recuperar, reinstalar e reconfigurar. Por exemplo, quando um incidente afeta a disponibilidade de dados, após a recuperação ou restauro desses dados, é necessário confirmar a sua integridade, acessibilidade e utilidade.

Uma análise retrospetiva da gestão de um incidente e a autoavaliação do desempenho numa situação de crise, permitem retirar lições e aprendizagens com as quais os bancos devem procurar melhorar os seus processos internos e a sua capacidade de antecipar e evitar futuros incidentes. O Regulamento DORA prevê que sejam realizados exames pós-incidente que afiram

[31] Nos termos do Regime Jurídico dos Serviços de Pagamento, da Instrução do Banco de Portugal n.º 1/2019 de 15 de janeiro e da Instrução do Banco de Portugal n.º 21/2019 de 25 de novembro.
[32] Nos termos da Lei n.º 46/2018 de 13 de agosto e do Decreto-lei n.º 65/2021 de 30 de julho.
[33] Nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

a prontidão da reação, a qualidade da análise forense e a eficácia das ações tomadas e da comunicação. Os ensinamentos retirados deste exercício, bem como dos testes regulares e da partilha de experiências entre entidades, devem ser incorporados num processo de melhoria continua do quadro de gestão de riscos TIC.

Por outro lado, a partilha de conhecimentos, competências e experiências entre bancos permite um alinhamento da indústria em relação às melhores práticas e uma melhor compreensão das fragilidades comuns e dos riscos que advêm de interdependências entre instituições. Esta partilha deve ser fomentada através de um quadro normativo que promova a troca de informações entre bancos sobre ameaças e vulnerabilidades para que, coletivamente, tirem partido das experiências individuais.

## 5. Conclusão

Uma vez feita esta breve incursão, poderemos concluir que:

De entre os múltiplos riscos associados à atividade financeira, existem dois que têm assumido particular relevância: o risco operacional e o risco de gestão das TIC.

A nível interno, os supervisores já os sinalizaram e iniciaram diligências para os controlar, sendo que o Banco de Portugal já divulgou como uma prioridade de supervisão para 2022 a resiliência cibernética. Por sua vez a CMVM identificou, no seu "Risk Outlook para 2022", o risco associado à digitalização como um dos principais riscos que as empresas de investimento terão de gerir este ano.

A nível europeu, surge-nos a proposta do Regulamento DORA que pretende responder à necessidade de densificação e harmonização de regras aplicáveis ao setor financeiro relacionadas com segurança e gestão de risco das TIC. Um dos seus pilares assenta na realização de testes da resiliência operacional e na harmonização da terminologia, critérios, prazos e modelos de reporte de incidentes.

Uma das grandes novidades deste Regulamento Europeu é sua aplicação não só às entidades financeiras, mas também às empresas terceiras prestadoras de serviços TIC, trazendo assim estas empresas, pela primeira vez, para o perímetro de supervisão dos reguladores financeiros.

Concluímos também que será ao órgão de gestão dos bancos que caberá, em primeiro lugar, a definição dos pilares em que assentará a construção de uma cultura de resiliência operacional, bem como sobre ele recairá a responsabilidade de garantir a sua salvaguarda. Para tal, deverá aprovar as políticas internas que estabelecem a estratégia, os princípios, os valores e os objetivos para a resiliência operacional e ainda tomar as medidas necessárias para implementar essas políticas

A MiFID II introduziu pela primeira vez o princípio de que a subcontratação de funções importantes não pode ser feita "de um modo que prejudique materialmente a qualidade do […] controlo interno ou a capacidade de a entidade supervisora controlar". As orientações da EBA relativas a subcontratação, sobre TIC e gestão de riscos de segurança, apesar da sua natureza recomendatória, densificaram os requisitos aplicáveis, daí que o Regulamento DORA pretenda agora resolver um vazio regulatório em relação a algumas matérias relacionadas com subcontratação, prevendo, designadamente, que as autoridades de supervisão possam, quando a criticidade dos serviços prestados o justifique, fazer auditorias e inspeções diretamente aos prestadores de serviços TIC, possam emitir recomendações e determinações específicas, aplicar-lhes sanções e impor a cessação de contratos de subcontratação.

Resta-nos, contudo, aguardar o decurso do tempo e constatar em que medida serão ou não suficientes estas medidas e se, entretanto, a realidade e evolução dos tempos trará novos riscos e novas necessidades de resposta.

## Bibliografia

BAGRECHA, NIKITA RAJESHKUMAR, ET AL., "Decentralised Blockchain Technology: Application in Banking Setor", *in 2020 International Conference for Emerging Technology (INCET)*, India, IEEE, 2020, pp. 1-5.

BANCO DE PORTUGAL, *Relatório de Estabilidade Financeira*, Lisboa, 2021, in https://www.bportugal.pt/sites/default/files/anexos/pdf-boletim/ref_12_2021_pt.pdf (17.01.2022)

DEUTSCHE BANK RESEARCH, *Fintech – The digital (r)evolution in the financial sector Algorithm-based banking with the human touch, Frankfurt am Main*, 2014, in https://www.finextra.com/finextra-downloads/featuredocs/prod0000000000345837.pdf (27.01.2022)

*FFIEC IT Examination Handbook InfoBase, Administrative Guidelines: Implementation of Interagency Programs for the Supervision of Technology Service Providers*, 2012 in https://ithandbook.ffiec.gov/media/153533/10-10-12_-_administrative_guidelines_sup_of_tsps.pdf (26.01.2022)

GOMES, DELBER PINTO, "Contratos ex machina: breves notas sobre a introdução da tecnologia Blockchain e Smart Contracts", *in Revista Electrónica de Direito*, Vol. 17, N.º 3, Porto, 2018, pp. 40-55

HASSANI, HOSSEIN, ET AL., "Banking with blockchain-ed big data", *in Journal of Management Analytics*, Vol. 5, N.º. 4, Londres, Taylor & Francis Group, 2018, pp. 256-275

LEAL, FÁTIMA / TEIXEIRA, MARIA EMÍLIA / MOREIRA, FERNANDO, "Decentralisation of FinTech Business Models", *in Lecture Notes in Networks and Systems*, Singapura, Springer Nature Singapore, 2022, pp. 343-353.

LEE, SANG M. / LEE, DONHEE, ""Untact": a new customer service strategy in the digital age", *in Service Business"*, Vol. 14, N.º 1, Germany, Springer Science and Business Media LLC., 2019, pp. 1-22.

MISHCHENKO, SVITLANA ET AL., "Innovation risk management in financial institutions", *in Investment Management and Financial Innovations*, Volume 18, Issue 1, Ukraine, LLC CPC Business Perspectives, 2021, pp. 190-202.

OLIVEIRA, ANDRESSA JARLETTI GONÇALVES DE, ET AL., "FinTech: Desafios da Tecnologia Financeira", *in Revista de Direito Econômico e Socioambiental*, Vol. 9, N.º 2, Curitiba, PUCPR, 2018, pp. 417-421

PORTO EDITORA, "resiliência" no *Dicionário Infopédia da Língua Portuguesa* [em linha]. Porto: Porto Editora. (7.01.2022). Disponível em https://www.infopedia.pt/dicionarios/lingua-portuguesa/resiliência.

VAZQUEZ, SIMON FERNANDEZ, ET AL., "Blockchain in FinTech: A Mapping Study", *in Sustainability*, Vol. 11, N.º 22, Switzerland, MDPI AG, 2019, p. 6366.

(texto submetido a 6.05.2022 e aceite para publicação a 8.06.2022)