COMISSÃO
EUROPEIA

Bruxelas, 24.9.2020
COM(2020) 595 final

2020/0266 (COD)

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

(Texto relevante para efeitos do EEE)

{SEC(2020) 307 final} - {SWD(2020) 198 final} - {SWD(2020) 199 final}

EXPOSIÇÃO DE MOTIVOS

- 1. Razões e objetivos da proposta

A presente proposta integra o pacote Financiamento Digital, um pacote de medidas destinadas a fomentar e apoiar ainda mais o potencial do financiamento digital em termos de inovação e concorrência, atenuando simultaneamente os riscos inerentes. É coerente com as prioridades da Comissão no sentido de preparar a Europa para a era digital e criar uma economia pronta para o futuro, que sirva as pessoas. O pacote de financiamento digital inclui uma nova estratégia em matéria de financiamento digital para o setor financeiro da UE[1], que visa garantir que a UE acolhe a revolução digital, impulsionando-a com empresas europeias inovadoras na vanguarda e disponibilizando os benefícios do financiamento digital aos consumidores e às empresas. Para além da presente proposta, o pacote inclui também uma proposta de regulamento relativo aos mercados de criptoativos[2], uma proposta de regulamento sobre um regime-piloto de infraestruturas de mercado baseadas na tecnologia de registo distribuído[3] e uma proposta de diretiva para esclarecer ou alterar determinadas regras conexas no que se refere aos serviços financeiros a nível da UE[4]. A digitalização e a resiliência operacional no setor financeiro são duas faces da mesma moeda. As tecnologias digitais, também designadas por tecnologias da informação e da comunicação (TIC), tanto geram oportunidades como riscos, que têm de ser bem compreendidos e geridos, em especial em momentos de maior tensão.

Por conseguinte, os decisores políticos e as autoridades de supervisão têm vindo a centrar cada vez mais a sua atenção nos riscos decorrentes da dependência das TIC. Têm, nomeadamente, tentado reforçar a resiliência das empresas por meio do estabelecimento de normas e da coordenação dos esforços de regulamentação ou supervisão. Os referidos esforços têm sido envidados tanto a nível internacional como a nível europeu, abrangendo todos os setores ou centrando-se num conjunto de setores específicos, nomeadamente nos serviços financeiros.

Contudo, os riscos no domínio das TIC continuam a representar um desafio para a estabilidade, o desempenho e a resiliência operacional do sistema financeiro da UE. A reforma que se seguiu à crise financeira de 2008 reforçou, sobretudo, a resiliência financeira[5] do setor financeiro da UE, abordando apenas indiretamente os riscos em matéria de TIC em alguns domínios, enquanto parte das medidas destinadas a resolver, de modo mais alargado, os riscos operacionais.

Se, por um lado, as alterações à legislação da UE em matéria de serviços financeiros no período pós-crise instituíram um conjunto único de regras que regem uma grande parte dos riscos financeiros associados aos serviços financeiros, por outro não abordaram totalmente a

---

1 Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões sobre uma Estratégia em matéria de Financiamento Digital para a EU, 23 de setembro de 2020, COM(2020) 591.

2 Proposta de regulamento do Parlamento Europeu e do Conselho relativo aos mercados de criptoativos e que altera a Diretiva (UE) 2019/1937, COM(2020) 593.

3 Proposta de regulamento do Parlamento Europeu e do Conselho relativo a um regime-piloto para as infraestruturas de mercado baseadas na tecnologia de registo distribuído, COM(2020) 594.

4 Proposta de diretiva do Parlamento Europeu e do Conselho que altera as Diretivas 2006/43/CE, 2009/65/CE, 2009/138/UE, 2011/61/UE, UE/2013/36, 2014/65/UE, (UE) 2015/2366 e UE/2016/2341, COM(2020) 596.

5 As diversas medidas adotadas visavam fundamentalmente reforçar os recursos financeiros e a liquidez das entidades financeiras, bem como reduzir os riscos de mercado e de crédito.

resiliência operacional digital. As medidas adotadas em relação a esta última ficaram marcadas por um conjunto de características que limitavam a sua eficácia. Por exemplo, foram muitas vezes elaboradas diretivas de harmonização mínima ou regulamentação baseada em princípios, deixando bastante espaço para divergência nas abordagens adotadas no mercado único. Além disso, os riscos no domínio das TIC são objeto de uma certa ênfase, de forma limitada ou incompleta, apenas no contexto da cobertura do risco operacional. Por fim, estas medidas variam no quadro da diferente legislação setorial em matéria de serviços financeiros. Por conseguinte, a intervenção a nível da União não supriu até aqui plenamente as necessidades das entidades financeiras para a gestão dos riscos operacionais de modo a resistir, dar resposta e recuperar dos impactos de incidentes no domínio das TIC. Tampouco deu às autoridades de supervisão financeira os instrumentos mais adequados para cumprirem os respetivos mandatos de prevenção da instabilidade financeira decorrente da materialização dos riscos no domínio das TIC.

A ausência de regras pormenorizadas e abrangentes em matéria de resiliência operacional digital a nível da UE conduziu à proliferação de iniciativas nacionais de regulamentação (p. ex.: sobre testes da resiliência operacional digital) e de abordagens de supervisão (p. ex.: abordando as dependências de terceiros no domínio das TIC). A ação a nível dos Estados-Membros tem, porém, um efeito limitado, dada a natureza transfronteiriça dos riscos no domínio das TIC. Além disso, as iniciativas nacionais não coordenadas resultaram em sobreposições, em incoerências, na duplicação de requisitos e em custos administrativos e de conformidade elevados – em especial para as entidades financeiras transfronteiriças –, bem como na não deteção de riscos no domínio das TIC e, por conseguinte, na sua não resolução. Esta situação fragmenta o mercado único, prejudica a estabilidade e a integridade do setor financeiro da UE e põe em perigo a proteção dos consumidores e investidores.

Cumpre portanto instituir um quadro pormenorizado e abrangente para a resiliência operacional digital das entidades financeiras da UE, quadro este que aprofundará a dimensão referente à gestão do risco no quadro do conjunto único de regras. Mais particularmente, reforçará e racionalizará a gestão do risco no domínio das TIC das entidades financeiras, estabelecerá a realização de testes exaustivos dos sistemas de TIC, sensibilizará as autoridades de supervisão para os riscos cibernéticos e os incidentes relacionados com as TIC que as entidades financeiras enfrentam e dará às autoridades de supervisão financeira poderes para fiscalizar os riscos decorrentes da dependência das entidades financeiras em relação a terceiros prestadores de serviços de TIC. A proposta criará um regime de comunicação de incidentes que ajudará a reduzir os encargos administrativos das entidades financeiras e reforçará a eficácia da supervisão.

- Coerência com as disposições existentes da mesma política setorial

A presente proposta integra um esforço mais amplo em curso a nível europeu e internacional para reforçar a cibersegurança nos serviços financeiros e dar resposta aos riscos operacionais de uma forma mais geral[6].

Vem igualmente ao encontro do parecer técnico conjunto de 2019[7] das Autoridades Europeias de Supervisão (AES), que instaram à adoção de uma abordagem mais coerente na resposta aos riscos no domínio das TIC e recomendaram à Comissão que reforçasse, de modo

[6] Comité de Basileia de Supervisão Bancária, *Cyber-resilience: Range of practices*, dezembro de 2018 e *Principles for sound management of operational risk (PSMOR)*, outubro de 2014.

[7] Parecer conjunto das Autoridades Europeias de Supervisão dirigido à Comissão Europeia sobre a necessidade de melhorias legislativas no que respeita aos requisitos de gestão do risco no domínio das TIC no setor financeiro da UE, JC 2019 26 (2019).

proporcionado, a resiliência operacional digital do setor dos serviços financeiros por meio de uma iniciativa setorial específica da UE. As AES emitiram o seu parecer em resposta ao plano de ação para a tecnologia financeira de 2018 da Comissão[8] .

- Coerência com outras políticas da União

Conforme mencionado pela presidente Ursula von der Leyen nas suas orientações políticas[9] – e referido na Comunicação intitulada «Construir o futuro digital da Europa»[10] –, é essencial que a Europa tire partido de todos os benefícios da era digital e reforce a sua capacidade industrial e de inovação, dentro de limites seguros e éticos. A estratégia europeia para os dados[11] define quatro pilares – a proteção de dados, os direitos fundamentais, a segurança e a cibersegurança –, que constituem uma condição prévia para uma sociedade capacitada pela utilização dos dados. Mais recentemente, o Parlamento Europeu tem envidado esforços no sentido de elaborar um relatório sobre finanças digitais, no qual, nomeadamente, se insta à adoção de uma abordagem comum à ciber-resiliência do setor financeiro[12]. Um quadro legislativo que reforce a resiliência operacional digital das entidades financeiras da UE será coerente com estes objetivos políticos. A proposta apoiaria, igualmente, as políticas que visam a recuperação após o coronavírus, uma vez que asseguraria que o aumento da dependência do financiamento digital é acompanhado de uma resiliência operacional adequada.

A iniciativa manteria os benefícios associados ao quadro horizontal para a cibersegurança (p. ex.: a Diretiva Segurança das Redes e da Informação, Diretiva SRI), mantendo no seu âmbito de aplicação o setor financeiro. O setor financeiro continuaria a estar estreitamente associado ao organismo de cooperação em matéria de SRI e as autoridades de supervisão conseguiriam partilhar informações dentro do ecossistema SRI existente. A iniciativa seria coerente com a Diretiva Infraestruturas Críticas Europeias (ICE), que se encontra atualmente em processo de revisão para reforçar a proteção e resiliência de infraestruturas críticas contra ameaças não cibernéticas. Por fim, a presente proposta é plenamente consentânea com a Estratégia da UE para a União da Segurança[13], que insta a uma iniciativa sobre a resiliência operacional digital dos setores financeiros, dada a sua elevada dependência dos serviços de TIC e a sua elevada vulnerabilidade aos ciberataques.

2. BASE JURÍDICA, SUBSIDIARIEDADE E PROPORCIONALIDADE

- Base jurídica

A proposta de regulamento baseia-se no artigo 114.º do TFUE.

---

8 Comissão Europeia, *Plano de Ação para a Tecnologia Financeira*, COM(2018) 0109 final.

9 Presidente Ursula von der Leyen, Orientações Políticas para a Próxima Comissão Europeia 2019-2024, https://ec.europa.eu/commission/sites/beta-political/files/political-guidelines-next-commission_pt.pdf.

10 Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões – *Construir o futuro digital da Europa*, COM(2020) 67 final.

11 Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, *Uma estratégia europeia para os dados*, COM(2020) 66 final.

12 «Relatório que contém recomendações à Comissão sobre finanças digitais: riscos emergentes em criptoativos – desafios ao nível da regulamentação e da supervisão no domínio dos serviços, instituições e mercados financeiros» (2020/2034(INL), https://oeil.secure.europarl.europa.eu/oeil/popups/ficheprocedure.do?reference=2020/2034(INL)&l=en.

13 Comunicação da Comissão ao Parlamento Europeu, ao Conselho Europeu, ao Conselho, ao Comité Económico e Social Europeu e ao Comité das Regiões, sobre a Estratégia da UE para a União da Segurança, COM(2020) 605 final.

A proposta remove obstáculos e melhora o estabelecimento e funcionamento do mercado interno de serviços financeiros, harmonizando as regras aplicáveis à gestão de riscos no domínio das TIC, à comunicação de informações, à realização de testes e ao risco de terceiros no domínio das TIC. As disparidades existentes neste domínio, tanto no domínio legislativo como da supervisão, assim como a nível nacional e da UE, constituem obstáculos ao mercado único dos serviços financeiros, uma vez que as entidades financeiras com atividade transfronteiriça se deparam com requisitos regulamentares ou expectativas de supervisão diferentes, ou mesmo sobrepostas, que podem impedir o exercício das liberdades de estabelecimento e prestação de serviços. As diferentes regras também falseiam a concorrência entre os mesmos tipos de entidades financeiras em Estados-Membros diferentes. Além disso, nos domínios em que não há harmonização ou há uma harmonização parcial ou limitada, o desenvolvimento de abordagens e regras nacionais divergentes, estejam elas em vigor ou em processo de aprovação e aplicação a nível nacional, podem constituir fatores de dissuasão das liberdades do mercado único de serviços financeiros. É esse o caso, em especial, dos quadros para a realização de testes operacionais digitais e para a fiscalização de terceiros prestadores de serviços críticos no domínio das TIC.

Uma vez que a proposta afeta diversas diretivas do Parlamento Europeu e do Conselho adotadas com base no artigo 53.º, n.º 1, do TFUE, é apresentada, simultaneamente, uma proposta de diretiva que reflita as alterações necessárias dessas diretivas.

- Subsidiariedade

O elevado grau de interligação dos serviços financeiros, a significativa atividade transfronteiriça das entidades financeiras e a considerável dependência do setor financeiro, no seu todo, de terceiros prestadores de serviços de TIC são fatores que exigem a viabilização de uma robusta resiliência operacional digital, para preservar a solidez dos mercados financeiros da UE no interesse comum. As disparidades resultantes de regimes assimétricos ou parciais, de sobreposições ou da multiplicidade de requisitos aplicáveis às mesmas entidades financeiras com atividade transfronteiriça ou titulares de várias autorizações[14] no mercado único só podem ser resolvidas a nível da União.

A presente proposta vem harmonizar a componente operacional digital de um setor profundamente integrado e interligado, que já beneficia de um conjunto único de regras e de uma supervisão comum na maioria dos restantes domínios. No que respeita a questões como a comunicação de incidentes relacionados com as TIC, só por meio de regras da União harmonizadas se poderia reduzir o nível de encargos administrativos e custos financeiros associados à comunicação do mesmo incidente relacionado com as TIC a diversas autoridades nacionais e da União. A ação da UE é igualmente necessária para facilitar o reconhecimento mútuo dos resultados dos testes avançados da resiliência operacional digital das entidades com atividade transfronteiriça, os quais, na ausência de regras da União, estão ou poderão estar sujeitas a diferentes quadros em diferentes Estados-Membros. Apenas uma ação a nível da União poderá dar resposta às diferenças entre as abordagens de realização de testes aplicadas pelos Estados-Membros. A ação à escala da UE também é necessária para colmatar a falta de poderes de supervisão adequados para monitorizar os riscos decorrentes dos terceiros prestadores de serviços de TIC, nomeadamente os riscos de concentração e de contágio no setor financeiro da UE.

[14] A mesma entidade financeira pode ter uma licença bancária, de empresa de investimento e de instituição de pagamento, cada uma das quais emitida por uma autoridade de supervisão diferente de um ou mais Estados-Membros.

- Proporcionalidade

As regras propostas não excedem o necessário para atingir os objetivos da proposta, abrangendo apenas aspetos aos quais os Estados-Membros não conseguirão dar resposta por si mesmos e limitando-se a situações em que os encargos administrativos e os custos sejam proporcionados aos objetivos específicos e gerais a alcançar.

A proporcionalidade é tida em conta em termos do âmbito de aplicação e de intensidade, por meio da utilização de critérios de avaliação qualitativos e quantitativos através dos quais se pretende assegurar que, não obstante o facto de abrangerem todas as entidades financeiras, as novas regras sejam simultaneamente adaptadas aos riscos e às necessidades decorrentes das respetivas características específicas em termos de dimensão e perfil de atividades. A proporcionalidade é igualmente integrada nas regras em matéria de gestão do risco no domínio das TIC, de realização de testes da resiliência digital, da comunicação de incidentes graves relacionados com as TIC e da fiscalização de terceiros prestadores de serviços de TIC críticos.

- Escolha do instrumento

As medidas necessárias para governar a gestão do risco no domínio das TIC, a comunicação de incidentes relacionados com as TIC, a realização dos testes e a fiscalização de terceiros prestadores de serviços críticos no domínio das TIC têm de estar contidas num regulamento, para assegurar que os requisitos sejam efetiva e diretamente aplicáveis de modo uniforme, sem prejuízo da proporcionalidade e das regras específicas previstas no presente regulamento. A coerência na abordagem aos riscos operacionais digitais contribui para reforçar a confiança no sistema financeiro e preservar a sua estabilidade. Dado que o recurso a um regulamento ajuda a reduzir a complexidade regulamentar, fomenta a convergência da supervisão e aumenta a segurança jurídica, o presente regulamento contribui igualmente para limitar os custos de conformidade das entidades financeiras, em especial para as que desenvolvem atividades transfronteiriças, o que, por sua vez, ajudará a eliminar as distorções da concorrência.

O presente regulamento elimina igualmente as disparidades legislativas e as assimetrias das abordagens nacionais de regulamentação ou supervisão do risco no domínio das TIC, removendo portanto os obstáculos no mercado único dos serviços financeiros, em especial no que respeita à facilidade do exercício das liberdades de estabelecimento e prestação de serviços pelas entidades financeiras com uma presença transfronteiriça.

Por fim, o conjunto único de regras tem sido sobretudo desenvolvido por meio de regulamentos, pelo que a sua atualização no que respeita à componente relativa à resiliência operacional digital deve seguir a mesma escolha de instrumento jurídico.

3. RESULTADOS DAS AVALIAÇÕES *EX POST*, DAS CONSULTAS DAS PARTES INTERESSADAS E DAS AVALIAÇÕES DE IMPACTO

- Avaliações *ex post*/balanços de qualidade da legislação existente

Até ao momento, não existe qualquer legislação em matéria de serviços financeiros centrada na resiliência operacional e que dê uma resposta abrangente aos riscos decorrentes da digitalização, nem mesmo a que estabelece regras para dar resposta, de uma forma mais geral, à dimensão do risco operacional, com uma subcomponente relativa ao risco no domínio das TIC. A intervenção da União tem ajudado, até ao momento, a suprir as necessidades e a dar resposta aos problemas presentes no rescaldo da crise financeira de 2008: as instituições de

crédito não se encontravam suficientemente capitalizadas, os mercados não estavam suficientemente integrados e a harmonização, até então, era mantida a um nível mínimo. À altura, o risco no domínio das TIC não era considerado uma prioridade, pelo que os quadros jurídicos de diversos subsetores financeiros evoluíram de modo descoordenado. Ainda assim, a ação da União alcançou os seus objetivos de assegurar a estabilidade financeira e estabelecer um conjunto único de regras harmonizadas em matéria prudencial e de conduta do mercado aplicáveis às entidades financeiras em toda a UE. Uma vez que os fatores que, no passado, motivaram a intervenção legislativa da União não permitiam que as regras específicas e abrangentes abordassem a utilização generalizada de tecnologias digitais e os riscos dela decorrentes no domínio financeiro, a realização de uma avaliação explícita afigura-se desafiante. Cada pilar do presente regulamento reflete um exercício implícito de avaliação e as alterações legislativas que dele advêm.

- Consulta das partes interessadas

A Comissão consultou as partes interessadas durante o processo de elaboração da proposta, nomeadamente:

i) A Comissão levou a cabo uma consulta pública aberta específica (de 19 de dezembro de 2019 a 19 de março de 2020)[15];

ii) A Comissão consultou o público por meio de uma avaliação de impacto inicial (de 19 de dezembro de 2019 a 16 de janeiro de 2020)[16];

iii) Em duas ocasiões (18 de maio de 2020 e 16 de julho de 2020), os serviços da Comissão consultaram peritos dos Estados-Membros pertencentes ao grupo de peritos do setor bancário, dos pagamentos e dos seguros[17];

iv) No âmbito do conjunto de eventos de sensibilização para o financiamento digital realizados em 2020, os serviços da Comissão organizaram um seminário em linha especificamente alusivo ao tema da resiliência operacional digital (19 de maio de 2020).

Pretendia-se com a consulta pública informar a Comissão quanto ao desenvolvimento de um eventual quadro intersetorial da UE para a resiliência operacional digital no domínio dos serviços financeiros. Nas respostas obtidas, ficou patente um amplo apoio à introdução de um quadro específico com medidas centradas nos quatro domínios objeto da consulta, tendo sido salientada a necessidade de assegurar a proporcionalidade, bem como de abordar e explicar a interação com as regras horizontais da Diretiva SRI. A Comissão recebeu duas respostas à avaliação de impacto inicial, nas quais os inquiridos abordaram aspetos específicos relacionados com o respetivo domínio de atividade.

Na reunião do grupo de peritos do setor bancário, dos pagamentos e dos seguros de 18 de maio de 2020, os Estados-Membros manifestaram um amplo apoio ao reforço da resiliência operacional digital do setor financeiro por meio das ações previstas para os quatro elementos delineados pela Comissão. Os Estados-Membros salientaram ainda a necessidade de uma

[15] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-/public-consultation.

[16] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12090-Digital-Operational-Resilience-of-Financial-Services-DORFS-Act-

[17] https://ec.europa.eu/info/business-economy-euro/banking-and-finance/regulatory-process-financial-services/expert-groups-comitology-and-other-committees/expert-group-banking-payments-and-insurance_en.

articulação clara das novas regras com as relativas ao risco operacional (no âmbito da legislação em matéria de serviços financeiros da UE) e com as regras horizontais em matéria de cibersegurança (Diretiva SRI). Durante a segunda reunião, alguns Estados-Membros salientaram a necessidade de assegurar a proporcionalidade e ter em conta a situação específica das pequenas empresas ou das filiais de grupos maiores, bem como a necessidade de atribuir um mandato robusto às ANC que participam na supervisão.

A proposta integra e baseia-se, igualmente, em observações feitas nas reuniões realizadas com partes interessadas e as instituições e autoridades da UE. As partes interessadas, incluindo terceiros prestadores de serviços de TIC, têm acolhido favoravelmente a proposta, de modo geral. Da análise das observações recebidas é patente o apelo à preservação da proporcionalidade e à adoção na conceção das regras de uma abordagem com base em princípios e no risco. Quanto ao lado institucional, os principais contributos foram aqueles do Comité Europeu do Risco Sistémico (CERS), das AES, da Agência da União Europeia para a Cibersegurança (ENISA) e do Banco Central Europeu (BCE), assim como das autoridades competentes dos Estados-Membros.

- Recolha e utilização de conhecimentos especializados

Ao preparar a presente proposta, a Comissão baseou-se em dados qualitativos e quantitativos obtidos junto de fontes reconhecidas, o que inclui os dois pareceres técnicos conjuntos das AES. A estes juntaram-se contributos confidenciais e relatórios públicos de autoridades de supervisão, organismos internacionais de normalização e institutos de investigação proeminentes, bem como contributos quantitativos e qualitativos de partes interessadas identificadas pertencentes ao setor financeiro mundial.

- Avaliação de impacto

A presente proposta é acompanhada por uma avaliação de impacto[18], que foi apresentada ao Comité de Controlo da Regulamentação (CCR) em 29 de abril de 2020 e aprovada em 29 de maio de 2020. O CCR recomendou que fossem feitas melhorias em algumas áreas, com vista a: i) prestar mais informações sobre a questão de saber como irá ser assegurada a proporcionalidade; ii) pôr em maior evidência a medida em que a opção preferencial difere do parecer técnico conjunto das AES e por que motivo essa opção é a melhor; e iii) pôr em maior evidência as interações entre a proposta e a legislação existente da UE, nomeadamente as regras que, atualmente, se encontram em processo de revisão. A avaliação de impacto foi adaptada para dar resposta a estes elementos, abordando igualmente as observações mais pormenorizadas do CCR.

A Comissão ponderou um conjunto de opções políticas para criar um quadro para a resiliência operacional digital, a saber:

- Manutenção do *statu quo*: as regras relativas à resiliência operacional continuariam a ser estabelecidas pelo atual conjunto divergente de disposições referentes aos serviços financeiros da UE, bem como parcialmente pela Diretiva SRI e pelos regimes nacionais existentes ou futuros;

[18] Documento de trabalho dos serviços da Comissão – Relatório da Avaliação de Impacto que acompanha o documento Regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional 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, SWD (2020) 198 de 24.9.2020.

- Opção 1: reforço das reservas de capital: seriam introduzidas reservas de capital adicionais com vista a aumentar a capacidade das entidades financeiras para absorverem perdas que pudessem surgir devido à falta de resiliência operacional digital;
- Opção 2: apresentação de um ato relativo à resiliência operacional digital dos serviços financeiros: permitiria a criação de um quadro abrangente a nível da UE, com regras coerentes destinadas a suprir as necessidades em matéria de resiliência operacional digital de todas as entidades financeiras reguladas, e estabeleceria um quadro de fiscalização dos terceiros prestadores de serviços de TIC críticos;
- Opção 3: um ato relativo à resiliência operacional digital dos serviços financeiros juntamente com uma supervisão centralizada dos terceiros prestadores de serviços de TIC críticos: além do ato relativo à resiliência operacional digital (opção 2), instituir-se-ia uma nova autoridade para supervisionar a prestação de serviços de TIC por terceiros.

Foi selecionada a segunda opção, dado que permite alcançar a maioria dos objetivos pretendidos de modo eficaz, eficiente e coerente com outras políticas da União. A maioria das partes interessadas também prefere esta opção.

A opção selecionada daria origem a custos de natureza recorrente e não recorrente[19]. Os custos não recorrentes devem-se, sobretudo, aos investimentos em sistemas informáticos e, por conseguinte, são difíceis de quantificar dado o diferente estado dos complexos cenários no domínio informático das empresas e, em particular, dos seus sistemas informáticos pré-existentes. Ainda assim, estes custos serão, provavelmente, limitados para as grandes empresas, tendo em conta os significativos investimentos no domínio das TIC que já fizeram. Espera-se, igualmente, que os custos sejam limitados para as pequenas empresas, uma vez que seriam aplicáveis medidas proporcionadas, dado o risco mais baixo das mesmas.

A opção selecionada teria efeitos positivos para as PME em atividade no setor dos serviços financeiros, em termos de impactos económicos, sociais e ambientais. A proposta proporcionará às PME clareza quanto às regras aplicáveis, o que reduzirá os custos de conformidade.

Os principais impactos sociais da opção política selecionada seriam junto dos consumidores e investidores. O aumento dos níveis de resiliência operacional digital do sistema financeiro da UE reduziria a frequência e os custos médios dos incidentes. A sociedade, no seu todo, beneficiaria com o aumento da confiança no setor dos serviços financeiros.

Por fim, em termos de impactos ambientais, a opção política selecionada incentivaria um aumento da utilização da última geração de infraestruturas e serviços de TIC, que se prevê sejam mais sustentáveis em termos ambientais.

- Adequação da regulamentação e simplificação

A eliminação da sobreposição dos requisitos de comunicação de incidentes relacionados com as TIC reduziria os encargos administrativos e os custos conexos. Além disso, a harmonização dos testes da resiliência operacional digital, com reconhecimento mútuo no mercado único,

[19] *Ibid.*, pp. 89-94.

reduzirá os custos, em especial para as empresas transfronteiriças, que de outro modo poderiam ter de realizar diversos testes nos diferentes Estados-Membros[20].

- Direitos fundamentais

A UE está empenhada em assegurar níveis elevados de proteção dos direitos fundamentais. Todas as disposições em matéria de partilha de informações a título voluntário entre as entidades financeiras que o presente regulamento promove seriam postas em prática em ambientes de confiança, no pleno respeito das regras em matéria de proteção dos dados da União, designadamente do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[21] e em especial no tratamento de dados pessoais, se for caso disso, para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento.

4. INCIDÊNCIA ORÇAMENTAL

No que respeita à incidência orçamental, dado que o presente regulamento prevê um reforço das funções das AES por meio da atribuição de poderes para fiscalizar adequadamente os terceiros prestadores de serviços de TIC críticos, a proposta implicaria uma maior utilização de recursos, em especial para cumprir as missões de fiscalização (como atividades de inspeção e auditoria no terreno e em linha), e o recurso a pessoal com conhecimentos especializados específicos no domínio da segurança das TIC.

A escala e distribuição destes custos dependerá da amplitude dos novos poderes de fiscalização e das atribuições (precisas) a conferir às AES. No que respeita aos novos recursos humanos, a EBA, a ESMA e a EIOPA necessitarão de 18 novos funcionários a tempo completo (FTC) – seis FTC para cada autoridade – quando as diversas disposições da proposta forem aplicáveis (cujo custo se estima que ascenda a 15,71 milhões de EUR no período 2022-2027). As AES terão ainda de suportar custos adicionais informáticos, despesas de deslocação em serviço para as inspeções no terreno e custos de tradução (que se estima que ascendam a 12 milhões de EUR no período 2022-2027), bem como outras despesas administrativas (que se estima que ascendam a 2,48 milhões de EUR no período 2022-2027). Por conseguinte, o impacto do custo total previsto é de, aproximadamente, 30,19 milhões de EUR no período 2022-2027.

Importa ainda salientar que, embora os valores necessários (p. ex.: dos novos funcionários e de outras despesas relacionadas com as novas atribuições) relativos à fiscalização direta dependam, com o passar do tempo, da evolução do número e da dimensão dos terceiros prestadores de serviços de TIC críticos a fiscalizar, as respetivas despesas serão plenamente financiadas por meio das taxas cobradas aos intervenientes no mercado. Por conseguinte, não se prevê qualquer impacto a nível de dotações orçamentais da UE (salvo no que respeita aos funcionários adicionais), uma vez que os custos serão plenamente financiados por taxas.

O impacto orçamental e financeiro da presente proposta é explicado em pormenor na ficha financeira legislativa em anexo à presente proposta.

---

20 *Ibidem*.

21 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

5. OUTROS ELEMENTOS

- Planos de execução e acompanhamento, mecanismos de avaliação e prestação de informações

A proposta inclui um plano geral de acompanhamento e avaliação do impacto relativo aos objetivos específicos, que exige que a Comissão proceda a uma revisão pelo menos três anos após a entrada em vigor e preste informações ao Parlamento Europeu e ao Conselho sobre as suas principais conclusões.

A revisão deve ser realizada em conformidade com as Orientações «Legislar Melhor» da Comissão.

- Explicação pormenorizada das disposições específicas da proposta

A proposta estrutura-se em torno de diversos domínios de intervenção política que constituem pilares inter-relacionados fundamentais consensualmente incluídos nas boas práticas e nas orientações europeias e internacionais que visam reforçar a resiliência operacional e a ciber-resiliência do setor financeiro.

Âmbito de aplicação do regulamento e aplicação do princípio da proporcionalidade das medidas necessárias (artigo 2.º)

A fim de assegurar a coerência dos requisitos de gestão do risco no domínio das TIC aplicáveis ao setor financeiro, o regulamento abrange um conjunto de entidades financeiras reguladas a nível da União, nomeadamente instituições de crédito, instituições de pagamento, instituições de moeda eletrónica, empresas de investimento, prestadores de serviços de criptoativos, centrais de valores mobiliários, contrapartes centrais, plataformas de negociação, repositórios de transações, gestores de fundos de investimento alternativos e sociedades gestoras, prestadores de serviços de comunicação de dados, empresas de seguros e de resseguros, mediadores de seguros, mediadores de resseguros e mediadores de seguros a título acessório, instituições de realização de planos de pensões profissionais, agências de notação de risco, revisores oficiais de contas e sociedades de auditoria, administradores de índices de referência críticos e prestadores de serviços de financiamento colaborativo.

Uma tal cobertura facilitará a aplicação homogénea e coerente de todas as componentes da gestão do risco nos domínios relacionados com as TIC, salvaguardando simultaneamente a equidade das condições de concorrência entre as entidades financeiras quanto às suas obrigações regulamentares em matéria de risco no domínio das TIC. Ao mesmo tempo, o regulamento reconhece a existência de diferenças significativas entre as entidades financeiras, tanto em termos de dimensão e perfil de atividades como da sua exposição ao risco digital. Uma vez que as entidades financeiras de maiores dimensões possuem mais recursos, só as entidades financeiras que não se enquadram na definição de microempresas serão obrigadas a, por exemplo, estabelecer disposições de governação complexas e cargos de gestão específicos, realizar avaliações em profundidade depois de fazerem alterações consideráveis na rede e nas infraestruturas do sistema informático, realizar regularmente análises de risco dos sistemas de TIC pré-existentes, expandir a realização de testes aos planos de continuidade das atividades e de resposta e recuperação para abranger cenários de comutação entre a sua principal infraestrutura de TIC e instalações redundantes. Além disso, a realização de testes de penetração por ameaças só será exigida às entidades financeiras que sejam consideradas significativas para efeitos da realização de testes avançados de resiliência digital.

Não obstante esta amplitude, a cobertura não é exaustiva. Mais concretamente, o presente regulamento não abrange os operadores de sistema na aceção do artigo 2.º, alínea p), da Diretiva 98/26/CE[22] relativa ao caráter definitivo da liquidação nos sistemas de pagamentos e de liquidação de valores mobiliários (SFD), nem qualquer outro interveniente no sistema, exceto se o próprio interveniente for uma entidade financeira (ou seja, uma instituição de crédito, uma empresa de investimento, uma CCP) regulada a nível da União, sendo por conseguinte abrangida pelo presente regulamento por direito próprio. Além disso, também o registo da União para as licenças de emissão, cujo funcionamento é regido pela Diretiva 2003/87/CE[23] sob a égide da Comissão Europeia, está fora do âmbito de aplicação do regulamento.

As referidas exclusões da SFD têm em conta a necessidade de um exame mais aprofundado das questões jurídicas e estratégicas respeitantes aos intervenientes e operadores de sistemas da SFD, tendo devidamente em consideração o impacto dos quadros que são atualmente candidatos a sistemas de pagamentos[24] operados por bancos centrais. Uma vez que as referidas questões podem implicar aspetos que são, todavia, distintos das matérias abrangidas pelo presente regulamento, a Comissão continuará a avaliar a necessidade e o impacto de um eventual alargamento do âmbito de aplicação do presente regulamento às entidades e infraestruturas de TIC atualmente fora da sua esfera.

Requisitos relacionados com a governação (artigo 4.º)

O presente regulamento foi concebido para harmonizar melhor as estratégias de atividade das entidades financeiras e a gestão do risco no domínio das TIC. Para o efeito, o órgão de administração terá de manter uma função crucial e ativa na orientação do quadro de gestão do risco no domínio das TIC e deve observar uma rigorosa ciber-higiene. A plena responsabilidade do órgão de administração na gestão do risco no domínio das TIC da entidade financeira constituirá um princípio abrangente que se traduzirá, igualmente, num conjunto de requisitos específicos, tais como a atribuição de competências e responsabilidades claras para todas as funções relacionadas com as TIC, um empenho contínuo no controlo da monitorização da gestão do risco no domínio das TIC, assim como toda a panóplia de processos de aprovação e controlo e uma adequada realização de investimentos e formação no domínio das TIC.

Requisitos de gestão do risco no domínio das TIC (artigos 5.º a 14.º)

A resiliência operacional digital funda-se num conjunto de princípios fundamentais e requisitos do quadro de gestão do risco no domínio das TIC, em consonância com o parecer técnico conjunto das AES. Os requisitos, que se inspiram em normas, orientações e recomendações pertinentes a nível internacional, nacional e setorial, centram-se em torno de funções específicas de gestão do risco no domínio das TIC (identificação, proteção e prevenção, deteção, resposta e recuperação, aprendizagem e evolução, e comunicação). Para acompanhar o ritmo de um cenário de ciberameaça em rápida evolução, as entidades

[22] Diretiva 98/26/CE do Parlamento Europeu e do Conselho, de 19 de maio de 1998, relativa ao caráter definitivo da liquidação nos sistemas de pagamentos e de liquidação de valores mobiliários (JO L 166 de 11.6.1998, p. 45).

[23] Diretiva 2003/87/CE do Parlamento Europeu e do Conselho, de 13 de outubro de 2003, relativa à criação de um sistema de comércio de licenças de emissão de gases com efeito de estufa na União e que altera a Diretiva 96/61/CE do Conselho (JO L 275 de 25.10.2003, p. 32).

[24] Em especial o Regulamento do Banco Central Europeu (UE) n.º 795/2014, de 3 de julho de 2014, relativo aos requisitos de superintendência de sistemas de pagamentos sistemicamente importantes.

financeiras têm de manter instrumentos e sistemas de TIC resilientes para minimizar o impacto do risco nesse domínio, identificar continuamente todas as fontes de risco no domínio das TIC, adotar medidas de proteção e prevenção, detetar prontamente atividades anómalas e pôr em prática políticas específicas e abrangentes de continuidade das atividades e planos de recuperação e de catástrofe, como parte integrante da política de continuidade das atividades. As últimas são componentes necessárias à pronta recuperação na sequência de incidentes relacionados com as TIC, em especial de ciberataques, limitando os danos e dando prioridade a uma segura continuação das atividades. O regulamento não impõe, por si próprio, uma normalização específica, mas assenta sim em normas técnicas ou boas práticas do setor reconhecidas a nível europeu e internacional, na medida em que estejam em conformidade com as instruções de supervisão sobre a utilização e integração de tais normas internacionais. O presente regulamento também não abrange a integridade, segurança e resiliência das infraestruturas físicas e das instalações que permitem a utilização da tecnologia, bem como das pessoas e processos pertinentes relacionados com as TIC, que integram a pegada digital das operações da entidade financeira.

Comunicação de incidentes relacionados com as TIC (artigos 15.º a 20.º)

A harmonização e racionalização da comunicação de incidentes relacionados com as TIC é alcançada, em primeiro lugar, por meio de um requisito geral que obriga as entidades financeiras a estabelecerem e a porem em prática um processo de monitorização e registo dos incidentes relacionados com as TIC e, posteriormente, de uma obrigação de os classificar com base em critérios enunciados no regulamento e posteriormente desenvolvidos pelas AES para especificar limiares de materialidade. Em segundo lugar, só é obrigatória a comunicação às autoridades competentes dos incidentes relacionados com as TIC que sejam considerados graves. A comunicação deve ser efetuada por meio de um modelo comum e deve seguir um procedimento harmonizado criado pelas AES. As entidades financeiras devem apresentar relatórios iniciais, intercalares e finais e informar os seus utilizadores e clientes se o incidente tiver ou for suscetível de ter um impacto nos seus interesses financeiros. As autoridades competentes devem transmitir os pormenores pertinentes dos incidentes a outras instituições ou autoridades: às AES, ao BCE e aos pontos de contacto únicos designados por força da Diretiva (UE) 2016/1148.

Para encetar um diálogo entre as entidades financeiras e as autoridades competentes, que ajudaria a minimizar o impacto e a identificar medidas corretivas adequadas, a comunicação de incidentes graves relacionados com as TIC deve ser completada pela formulação de observações e orientações a nível da supervisão.

Por fim, deve-se continuar a explorar a possibilidade de centralizar a nível da União a comunicação de incidentes relacionados com as TIC num relatório conjunto das AES, do BCE e da ENISA sobre a avaliação da viabilidade do estabelecimento de uma plataforma única da UE (a seguir designada «plataforma») para a comunicação de incidentes graves relacionados com as TIC pelas entidades financeiras.

Testes da resiliência operacional digital (artigos 21.º a 24.º)

É necessário realizar periodicamente testes às capacidades e funções incluídas no quadro de gestão do risco no domínio das TIC quanto à sua prontidão e à identificação de pontos fracos, insuficiências ou lacunas, bem como quanto à pronta aplicação de medidas corretivas. O presente regulamento permite uma aplicação proporcionada dos requisitos em matéria de testes da resiliência operacional digital em função da dimensão e do perfil de atividades e de risco das entidades financeiras: embora todas as entidades devam realizar testes dos sistemas e instrumentos de TIC, só as entidades que sejam identificadas pelas autoridades competentes (com base em critérios constantes do presente regulamento e posteriormente desenvolvidos

pelas AES) como sendo significativas e tendo alcançado um determinado nível de maturidade cibernética devem ser obrigadas a realizar testes avançados, assentes em testes de penetração com base em ameaças. O presente regulamento estabelece ainda requisitos aplicáveis aos responsáveis pela realização dos testes e o reconhecimento dos resultados dos testes de penetração com base em ameaças na União pelas entidades financeiras com atividade em diversos Estados-Membros.

Risco de terceiros no domínio das TIC (artigos 25.º a 39.º)

O regulamento foi concebido para assegurar uma boa monitorização do risco de terceiros no domínio das TIC. Este objetivo será alcançado, em primeiro lugar, por meio do respeito das regras baseadas em princípios aplicáveis à monitorização do risco para as entidades financeiras decorrente de terceiros prestadores de serviços de TIC. Em segundo lugar, o regulamento harmoniza elementos fundamentais do serviço e da relação com os terceiros prestadores de serviços de TIC. Estes elementos abrangem aspetos mínimos considerados cruciais para permitir a total monitorização do risco de terceiros no domínio das TIC efetuada pela entidade financeira nas fases de celebração, de execução e de rescisão dos contratos, bem como na fase pós-contratual da sua relação.

Mais particularmente, os contratos que regem a referida relação terão de conter uma descrição completa dos serviços, a indicação dos locais em que se procederá ao tratamento dos dados, descrições completas dos acordos de nível de serviço acompanhadas de metas de desempenho quantitativas e qualitativas, disposições pertinentes sobre a acessibilidade, a disponibilidade, a integridade, a segurança e a proteção de dados pessoais e garantias de acesso, recuperação e reposição em caso de falhas dos terceiros prestadores de serviços de TIC, períodos de pré-aviso e obrigações de prestação de informações pelos terceiros prestadores de serviços de TIC, direitos de acesso, inspeção e auditoria da entidade financeira ou de terceiros designados para o efeito, direitos claros de rescisão e estratégias de saída específicas. Além disso, uma vez que alguns desses elementos contratuais são suscetíveis de normalização, o regulamento promove a utilização a título voluntário de cláusulas contratuais normalizadas para a utilização de serviços de computação em nuvem a elaborar pela Comissão.

Por fim, o regulamento procura promover a convergência das abordagens de supervisão em matéria de risco de terceiros no domínio das TIC no setor financeiro, sujeitando os terceiros prestadores de serviços de TIC críticos a um quadro de fiscalização da União. Por meio de um novo quadro legislativo harmonizado, a AES designada como autoridade de fiscalização principal de cada terceiro prestador de serviços de TIC crítico fica habilitada a assegurar que os prestadores de serviços informáticos que desempenham uma função crítica no funcionamento do setor financeiro sejam devidamente monitorizados a uma escala pan-europeia. O quadro de fiscalização pretendido no âmbito do presente regulamento assenta na arquitetura institucional existente no domínio dos serviços financeiros, mediante a qual o Comité Conjunto das AES assegura a coordenação intersetorial em todas as matérias relativas ao risco no domínio das TIC, em conformidade com as suas atribuições em matéria de cibersegurança, com o apoio do subcomité pertinente (Fórum de Fiscalização), efetuando os trabalhos preparatórios de decisões individuais e das recomendações coletivas dirigidas a terceiros prestadores de serviços críticos.

Partilha de informações (artigo 40.º)

A fim de sensibilizar para o risco no domínio das TIC, minimizar a sua propagação e apoiar as capacidades defensivas e as técnicas de deteção de ameaças das entidades financeiras, o regulamento permite que estas estabeleçam disposições para partilhar entre si dados e informações sobre ciberameaças.

2020/0266 (COD)

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

(Texto relevante para efeitos do EEE)

O PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia, nomeadamente o artigo 114.º,

Tendo em conta a proposta da Comissão Europeia,

Após transmissão do projeto de ato legislativo aos parlamentos nacionais,

Tendo em conta o parecer do Banco Central Europeu[25],

Tendo em conta o parecer do Comité Económico e Social Europeu[26],

Deliberando de acordo com o processo legislativo ordinário,

Considerando o seguinte:

(1) Na era digital, as tecnologias da informação e comunicação (TIC) servem de esteio a sistemas complexos utilizados em atividades societais quotidianas. Mantêm em funcionamento setores fundamentais das nossas economias, nomeadamente o setor financeiro, e melhoram o funcionamento do mercado único. A intensificação da digitalização e interligação também amplificam os riscos no domínio das TIC, tornando a sociedade no seu conjunto – e, em particular, o sistema financeiro – mais vulneráveis a ciberameaças ou perturbações no domínio das TIC. Não obstante o facto de a ubiquidade da utilização de sistemas de TIC e o elevado nível de digitalização e conectividade serem, atualmente, características centrais de todas as atividades das entidades financeiras da União, a resiliência digital não está ainda incorporada de modo suficiente nos seus quadros operacionais.

(2) A utilização das TIC tem adquirido nas últimas décadas um papel fulcral no setor financeiro, assumindo atualmente uma relevância crítica no funcionamento das típicas funções quotidianas de todas as entidades financeiras. A digitalização abrange, por exemplo, os pagamentos, onde se observa uma transição crescente dos métodos com base em numerário e em papel para soluções digitais, bem como a compensação e liquidação de valores mobiliários, a negociação eletrónica e algorítmica, as operações de concessão de empréstimos e de financiamento, o financiamento entre particulares, a notação de risco, a subscrição de seguros, a gestão dos sinistros e as operações de processamento administrativo. Não só o setor financeiro se tornou em grande medida

[25] [*Inserir referência*] JO C , p. .

[26] [*Inserir referência*] JO C , p. .

digital, como também a digitalização aprofundou a interligação e as dependências no interior do próprio setor financeiro e em relação a infraestruturas de terceiros e terceiros prestadores de serviços.

(3) O Comité Europeu do Risco Sistémico (CERS) reafirmou, num relatório de 2020 sobre o ciber-risco sistémico[27], que o elevado nível de interligação existente entre as entidades financeiras, os mercados financeiros e as infraestruturas do mercado financeiro, e, em especial, as interdependências dos seus sistemas de TIC, pode constituir uma vulnerabilidade sistémica, uma vez que os ciberincidentes localizados se poderiam rapidamente espalhar a partir de qualquer uma das aproximadamente 22 mil entidades financeiras da União[28] a todo o sistema financeiro, livre dos embaraços das fronteiras geográficas. As violações graves dos sistemas de TIC no setor financeiro não afetam unicamente as entidades financeiras, de forma isolada. Também abrem caminho à propagação de vulnerabilidades localizadas nos canais de transmissão financeiros e podem desencadear consequências negativas para a estabilidade do sistema financeiro da União, gerando crises de liquidez e uma perda de confiança geral nos mercados financeiros.

(4) Mais recentemente, os riscos no domínio das TIC têm atraído a atenção dos decisores políticos, das autoridades de regulamentação e dos organismos de normalização nacionais, europeus e internacionais, na tentativa de reforçar a resiliência, estabelecer normas e coordenar os esforços de regulamentação e supervisão. A nível internacional, o Comité de Basileia de Supervisão Bancária, o Comité de Pagamentos e Infraestruturas do Mercado, o Conselho de Estabilidade Financeira, o Instituto da Estabilidade Financeira, assim como o G7 e o G20, têm tentado proporcionar às autoridades competentes e aos operadores de mercado em diversas jurisdições instrumentos para reforçar a resiliência dos seus sistemas financeiros.

(5) Não obstante as políticas e iniciativas legislativas específicas a nível nacional e europeu, os riscos no domínio das TIC constituem ainda um desafio para a resiliência operacional, o desempenho e a estabilidade do sistema financeiro da União. A reforma que se seguiu à crise financeira de 2008 reforçou sobretudo a resiliência financeira do setor financeiro da União e visava salvaguardar a competitividade e estabilidade da União do ponto de vista económico, prudencial e da conduta do mercado. Embora a segurança e a resiliência digital no domínio das TIC façam parte do risco operacional, têm sido objeto de uma menor atenção na agenda regulamentar no período pós-crise, tendo-se desenvolvido apenas em alguns domínios das políticas e do panorama regulamentar da União no domínio dos serviços financeiros ou apenas em alguns Estados-Membros.

---

[27] Relatório do CERS intitulado «*Systemic Cyber Risk*», de fevereiro de 2020, https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf.

[28] De acordo com a avaliação de impacto que acompanha o exame das Autoridades Europeias de Supervisão (SWD(2017) 308), existem aproximadamente 5 665 instituições de crédito, 5 934 empresas de investimento, 2 666 empresas de seguros, 1 573 IRPPP, 2 500 sociedades gestoras de investimento, 350 infraestruturas do mercado (tais como CCP, bolsas de valores, internalizadores sistemáticos, repositórios de transações e MTF), 45 ANR e 2 500 instituições de moeda eletrónica e instituições de pagamento autorizadas. No total, existem aproximadamente 21 233 entidades, excluindo entidades de financiamento colaborativo, revisores oficiais de contas e sociedades de revisores oficiais de contas, prestadores de serviços de criptoativos e administradores de índices de referência.

(6) No seu Plano de Ação para a Tecnologia Financeira de 2018, a Comissão[29] destacou a extrema importância de tornar o setor financeiro da União mais resiliente também do ponto de vista operacional, para assegurar a sua segurança tecnológica e bom funcionamento e a sua rápida recuperação das violações e incidentes dos sistemas de TIC, permitindo, em última análise, a eficaz e fácil prestação dos serviços financeiros em toda a União, inclusivamente em situações de pressão, preservando simultaneamente a confiança dos consumidores e do mercado.

(7) Em abril de 2019, a Autoridade Bancária Europeia (EBA), a Autoridade Europeia dos Valores Mobiliários e dos Mercados (ESMA) e a Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (EIOPA) (conjuntamente denominadas «Autoridades Europeias de Supervisão» ou «AES») emitiram conjuntamente dois pareceres técnicos que instavam a uma abordagem coerente dos riscos no domínio das TIC no setor financeiro e recomendavam um reforço proporcionado da resiliência operacional digital do setor dos serviços financeiros por meio de uma iniciativa setorial da União.

(8) O setor financeiro da União é regulamentado por um conjunto único de regras e governado pelo sistema europeu de supervisão financeira. Todavia, as disposições que abordam a resiliência operacional digital e a segurança no domínio das TIC ainda não foram plena e coerentemente harmonizadas, embora a resiliência operacional digital seja vital para assegurar a estabilidade financeira e a integridade do mercado na era digital e não menos importante do que, por exemplo, as normas prudenciais ou de conduta do mercado. Cumpre, pois, desenvolver o conjunto único de regras e o sistema de supervisão, com vista a abranger também esta componente, alargando os mandatos das autoridades de supervisão financeira incumbidas da monitorização e da proteção da estabilidade financeira e da integridade do mercado.

(9) As disparidades legislativas e as assimetrias das abordagens nacionais de regulamentação ou supervisão do risco no domínio das TIC dão origem a obstáculos no mercado único dos serviços financeiros, impedindo o fácil exercício da liberdade de estabelecimento e prestação de serviços pelas entidades financeiras com uma presença transfronteiriça. A concorrência entre os mesmos tipos de entidades financeiras com atividade em diversos Estados-Membros também poderá ser falseada. Mais particularmente, nos domínios em que a harmonização da União tem sido muito limitada – como o da realização de testes da resiliência operacional digital – ou inexistente – como o da monitorização do risco de terceiros no domínio das TIC –, as disparidades decorrentes dos desenvolvimentos pretendidos a nível nacional podem gerar mais obstáculos ao funcionamento do mercado único, em detrimento dos intervenientes no mercado e da estabilidade financeira.

(10) São patentes as lacunas e sobreposições em domínios importantes, como a comunicação de incidentes relacionados com as TIC e a realização de testes da resiliência operacional digital, decorrentes do modo parcial pelo qual se tem, até ao momento, abordado as disposições relacionadas com o risco no domínio das TIC a nível da União. Esta situação é especialmente prejudicial para os utilizadores intensivos das TIC, como o setor financeiro, uma vez que os riscos tecnológicos não

[29] Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Banco Central Europeu, ao Comité Económico e Social Europeu e ao Comité das Regiões, *Plano de Ação para a Tecnologia Financeira: rumo a um setor financeiro europeu mais competitivo e inovador*, COM/2018/0109 final, https://ec.europa.eu/info/publications/180308-action-plan-fintech_en.

conhecem fronteiras e o setor financeiro oferece os seus serviços a nível transfronteiriço, tanto dentro como fora da União.

As entidades financeiras com atividade a nível transfronteiriço ou titulares de diversas autorizações (p. ex.:, uma entidade financeira pode ser titular de uma licença bancária, como empresa de investimento e como instituição de pagamento, todas elas emitidas por autoridades competentes diferentes num ou mais Estados-Membros) enfrentam desafios operacionais para fazer face aos riscos no domínio das TIC e atenuar os impactos negativos dos incidentes no domínio das TIC por si sós e de modo coerente e eficaz em termos de custos.

(11) Uma vez que o conjunto único de regras não foi acompanhado de um quadro abrangente para o risco operacional nem para as TIC, é necessária uma maior harmonização dos requisitos essenciais de resiliência operacional digital para todas as entidades financeiras. As capacidades e a resiliência geral que as entidades financeiras desenvolveriam, com base nos referidos requisitos essenciais, com vista a resistir às indisponibilidades operacionais, ajudariam a preservar a estabilidade e a integridade dos mercados financeiros da União, contribuindo assim para assegurar um elevado nível de proteção dos investidores e consumidores na União. Uma vez que o presente regulamento visa contribuir para o bom funcionamento do mercado único, deve ter por base as disposições do artigo 114.º do TFUE, interpretado nos termos da jurisprudência constante do Tribunal de Justiça da União Europeia.

(12) O presente regulamento visa, em primeiro lugar, consolidar e atualizar os requisitos em matéria de risco no domínio das TIC abordados, até ao momento, em diversos regulamentos e diretivas. Embora os referidos atos jurídicos da União abranjam as principais categorias de risco financeiro (ou seja, risco de crédito, risco de mercado, risco de crédito de contraparte e risco de liquidez, risco da conduta do mercado), no momento da adoção não conseguiam dar uma resposta abrangente a todas as componentes da resiliência operacional. Os requisitos em matéria de risco operacional, à medida que foram sendo aprofundados nos referidos atos jurídicos da União, deram muitas vezes preferência à tradicional abordagem quantitativa do risco (nomeadamente, o estabelecimento de um requisito de fundos próprios para cobrir os riscos no domínio das TIC), em vez de consagrarem requisitos qualitativos específicos com vista a proteger, detetar, conter, recuperar e reparar as capacidades afetadas por incidentes relacionados com as TIC ou de estabelecerem capacidades de comunicação de informações e de realização de testes aos meios digitais. As referidas diretivas e regulamentos pretendiam, sobretudo, abranger as regras essenciais em matéria de supervisão prudencial, integridade do mercado ou conduta.

Com este exercício, que consolida e atualiza as regras em matéria de risco no domínio das TIC, todas as disposições que abordam o risco digital no setor financeiro serão pela primeira vez reunidas de modo coerente num único ato legislativo. Importa, portanto, que a presente iniciativa colmate as lacunas ou resolva as incoerências em alguns dos referidos atos jurídicos, nomeadamente em relação à terminologia utilizada, e faça explicitamente referência ao risco no domínio das TIC por meio de regras específicas para as capacidades de gestão desse risco, a comunicação de informações e a realização de testes, bem como para a monitorização do risco de terceiros.

(13) As entidades financeiras devem adotar a mesma abordagem e as mesmas regras baseadas em princípios ao abordarem o risco no domínio das TIC. A coerência contribuirá para reforçar a confiança no sistema financeiro e preservar a sua

estabilidade, em especial quando se verifica uma excessiva utilização dos sistemas, plataformas e infraestruturas de TIC, o que implica um aumento do risco digital.

A observância de uma ciber-higiene básica deverá também evitar a imposição de pesados custos para a economia, minimizando o impacto e os custos das perturbações no domínio das TIC.

(14) O recurso a um regulamento ajuda a reduzir a complexidade regulamentar, fomenta a convergência da supervisão, aumenta a segurança jurídica e contribuirá simultaneamente para limitar os custos de conformidade, em especial para entidades financeiras com atividade transfronteiriça, e para reduzir as distorções da concorrência. Por conseguinte, a escolha de um regulamento para o estabelecimento de um quadro comum para a resiliência operacional digital das entidades financeiras afigura-se a forma mais adequada de garantir uma aplicação homogénea e coerente de todas as componentes da gestão do risco no domínio das TIC pelos setores financeiros da União.

(15) Além da legislação em matéria de serviços financeiros, a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho[30] constitui o quadro geral para a cibersegurança vigente a nível da União. Entre os sete setores cruciais, a diretiva é também aplicável a três tipos de entidades financeiras, a saber, as instituições de crédito, as plataformas de negociação e as contrapartes centrais. No entanto, uma vez que a Diretiva (UE) 2016/1148 estabelece um regime de identificação a nível nacional dos operadores de serviços essenciais, só determinadas instituições de crédito, plataformas de negociação e contrapartes centrais identificadas pelos Estados-Membros são abrangidas pelo seu âmbito de aplicação, pelo que estão obrigadas a cumprir os requisitos de comunicação de incidentes e de segurança no domínio das TIC estabelecidos na diretiva.

(16) Dado que o presente regulamento aumenta o nível de harmonização das componentes de resiliência digital, introduzindo requisitos de gestão do risco no domínio das TIC e de comunicação de incidentes relacionados com as TIC que são mais rigorosos do que os estabelecidos na legislação vigente em matéria de serviços financeiros da União, constitui também um reforço da harmonização em comparação com os requisitos estabelecidos na Diretiva (UE) 2016/1148. Por conseguinte, o presente regulamento constitui *lex specialis* em relação à Diretiva (UE) 2016/1148.

É fundamental manter uma interligação robusta do setor financeiro e o quadro horizontal de cibersegurança da União deverá assegurar a coerência com as estratégias de cibersegurança já adotadas pelos Estados-Membros e permitir que as autoridades de supervisão tomem conhecimento dos ciberincidentes que afetem outros setores abrangidos pela Diretiva (UE) 2016/1148.

(17) A fim de possibilitar um processo de aprendizagem e retirar efetivamente ensinamentos de outros setores que enfrentam ciberameaças, as entidades financeiras a que se refere a Diretiva (UE) 2016/1148 devem continuar a integrar o «ecossistema» da referida diretiva (p. ex.: o grupo de cooperação SRI e as CSIRT).

As AES e as autoridades nacionais competentes deverão participar nos debates políticos estratégicos e nos trabalhos técnicos do grupo de cooperação SRI, respetivamente, trocar informações e reforçar a cooperação com os pontos de contacto

[30] 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 (JO L 194 de 19.7.2016, p. 1).

únicos designados por força da Diretiva (UE) 2016/1148. As autoridades competentes para efeitos do presente regulamento devem igualmente consultar e cooperar com as CSIRT nacionais nos termos do artigo 9.º da Diretiva (UE) 2016/1148.

(18) Importa, ainda, garantir a coerência com a Diretiva Infraestruturas Críticas Europeias (ICE), que se encontra atualmente em processo de revisão para reforçar a proteção e resiliência de infraestruturas críticas contra ameaças não cibernéticas, com possíveis ramificações para o setor financeiro[31].

(19) Os prestadores de serviços de computação em nuvem são uma das categorias de prestadores de serviços digitais abrangidas pela Diretiva (UE) 2016/1148. Por conseguinte, estão sujeitos a uma supervisão *ex post* realizada pelas autoridades nacionais designadas nos termos da referida diretiva, que se limita aos requisitos em matéria de segurança e de comunicação de incidentes no domínio das TIC estabelecidos no referido ato. Uma vez que o quadro de fiscalização estabelecido pelo presente regulamento se aplica a todos os terceiros prestadores de serviços de TIC críticos, incluindo os prestadores de serviços de computação em nuvem, quando prestam serviços de TIC a entidades financeiras, deve ser considerado complementar da supervisão realizada por força da Diretiva (UE) 2016/1148. Além disso, o quadro de fiscalização estabelecido no presente regulamento deve abranger os prestadores de serviços de computação em nuvem na ausência de um quadro horizontal intersetorial da União que estabeleça uma autoridade de supervisão para o domínio do digital.

(20) Para que mantenham pleno controlo dos riscos no domínio das TIC, é necessário que as entidades financeiras criem capacidades abrangentes que possibilitem uma gestão robusta e eficaz do risco no domínio das TIC, bem como regimes e políticas específicas para a comunicação de incidentes relacionados com as TIC, para a realização de testes aos sistemas, controlos e processos de TIC e para gerir o risco de terceiros no domínio das TIC. É necessário elevar o nível da resiliência operacional digital no sistema financeiro, permitindo simultaneamente uma aplicação proporcionada dos requisitos às entidades financeiras que sejam microempresas na aceção da Recomendação 2003/361/CE da Comissão[32].

(21) Os limiares e as taxonomias que regem a comunicação de incidentes relacionados com as TIC variam significativamente nas diferentes jurisdições nacionais. Embora seja possível chegar a consensos, por meio dos esforços pertinentes envidados pela Agência da União Europeia para a Cibersegurança (ENISA)[33] e pelo grupo de cooperação SRI, no que respeita às entidades financeiras abrangidas pela Diretiva (UE) 2016/1148, ainda existem e podem surgir abordagens divergentes em matéria de limiares e taxonomias para as restantes entidades financeiras. Tal implica que as entidades financeiras são obrigadas a cumprir diversos requisitos, em especial se tiverem atividades em diversas jurisdições da União e integrarem um grupo financeiro. Além disso, estas divergências podem prejudicar a criação de outros regimes

---

31 Diretiva 2008/114/CE do Conselho, de 8 de dezembro de 2008, relativa à identificação e designação das infraestruturas críticas europeias e à avaliação da necessidade de melhorar a sua proteção (JO L 345 de 23.12.2008, p. 75).

32 Recomendação da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas (JO L 124 de 20.5.2003, p. 36).

33 ENISA, *Reference Incident Classification Taxonomy*, https://www.enisa.europa.eu/publications/reference-incident-classification-taxonomy.

uniformes ou centralizados da União que acelerem o processo de comunicação e apoiem uma partilha rápida e facilitada de informações entre as autoridades competentes, que será crucial para dar resposta aos riscos no domínio das TIC em caso de ataques em grande escala com consequências potencialmente sistémicas.

(22) Para permitir que as autoridades competentes cumpram as suas funções de supervisão, obtendo uma visão completa da natureza, da frequência, da significância e do impacto dos incidentes relacionados com as TIC, e reforçar a partilha de informações entre as autoridades públicas pertinentes, nomeadamente as autoridades responsáveis pela aplicação da lei e as autoridades de resolução, é necessário estabelecer regras para completar o regime de comunicação dos incidentes relacionados com as TIC com requisitos que atualmente estão omissos na legislação subsetorial financeira e eliminar quaisquer sobreposições e duplicações existentes para reduzir os custos. É portanto essencial harmonizar o regime de comunicação de incidentes relacionados com as TIC, exigindo a todas as entidades financeiras que os comuniquem apenas às respetivas autoridades competentes. Além disso, as AES devem ser habilitadas a especificar os elementos de comunicação de incidentes relacionados com as TIC, tais como a taxonomia, os prazos, os conjuntos de dados, os modelos e os limiares aplicáveis.

(23) Os requisitos de realização de testes da resiliência operacional digital têm indo a ser desenvolvidos em alguns subsetores financeiros no âmbito de diversos quadros nacionais não coordenados, que tratam as mesmas questões de formas diferentes. Esta situação multiplica os custos para as entidades financeiras transfronteiriças e dificulta o reconhecimento mútuo dos resultados. Por conseguinte, a realização de testes de forma não coordenada pode segmentar o mercado único.

(24) Além disso, nos casos em que não é obrigatório realizar testes, existem vulnerabilidades que continuam a não ser detetadas, o que resulta em maiores riscos para a entidade financeira e, em última análise, para a estabilidade e integridade do setor financeiro. Sem a intervenção da União, a realização de testes de resiliência operacional digital continuaria a ser fragmentada e não existiria um reconhecimento mútuo dos resultados dos testes entre as diversas jurisdições. Além disso, e uma vez que será pouco provável que outros subsetores financeiros adotem regimes deste tipo a uma escala significativa, não terão acesso aos seus potenciais benefícios, como a identificação de vulnerabilidades e riscos, a avaliação das capacidades de defesa e de garantia de continuidade das atividades e o aumento da confiança dos clientes, fornecedores e parceiros comerciais. Para resolver estas sobreposições, divergências e lacunas, é necessário estabelecer regras que visem a realização de testes coordenados pelas entidades financeiras e autoridades competentes, facilitando por conseguinte o reconhecimento mútuo de testes avançados para as entidades financeiras significativas.

(25) A dependência das entidades financeiras de serviços de TIC é em parte motivada pela sua necessidade de adaptação a uma economia digital emergente e competitiva a nível mundial, para reforçar a sua eficiência comercial e atender à procura dos consumidores. A natureza e dimensão desta dependência tem evoluído continuamente nos últimos anos e impulsionou uma redução dos custos de intermediação financeira, permitindo a expansão empresarial e as economias de escala na oferta de atividades financeiras e oferecendo simultaneamente uma gama alargada de instrumentos de TIC para gerir processos internos complexos.

(26) Os complexos acordos contratuais comprovam essa ampla utilização dos serviços de TIC, motivo pelo qual as entidades financeiras se confrontam muitas vezes com

dificuldades em negociar cláusulas contratuais adaptadas às normas prudenciais ou a outros requisitos regulamentares a que estão sujeitas, ou em fazerem valer certos direitos específicos, como os direitos de acesso ou de auditoria, quando estes últimos estão consagrados nos acordos. Acresce que muitos contratos deste tipo não preveem salvaguardas suficientes para a plena monitorização dos processos de externalização, privando assim a entidade financeira dos instrumentos necessários para avaliar esses riscos associados. Além disso, dado que os terceiros prestadores de serviços de TIC prestam muitas vezes serviços normalizados a diferentes tipos de clientes, tais contratos nem sempre dão uma resposta cabal às necessidades individuais ou específicas dos intervenientes do setor financeiro.

(27) Não obstante algumas regras gerais em matéria de externalização, constantes de alguns atos legislativos da União no domínio dos serviços financeiros, a monitorização da dimensão contratual não está plenamente ancorada na legislação da União. Na ausência de normas claras e adaptadas da União aplicáveis aos acordos contratuais celebrados com terceiros prestadores de serviços de TIC, a fonte externa do risco no domínio das TIC não é abordada de forma exaustiva. Por conseguinte, é necessário estabelecer determinados princípios fundamentais para orientar a gestão realizada pelas entidades financeiras do risco de terceiros no domínio das TIC, bem como um conjunto de direitos contratuais relativos a diversos elementos da execução e rescisão de contratos, com vista a consagrar determinadas salvaguardas mínimas que permitam às entidades financeiras proceder a uma efetiva monitorização de todos os riscos que possam surgir a nível de terceiros no domínio das TIC.

(28) Existe uma falta de homogeneidade e convergência em matéria de risco de terceiros no domínio das TIC e dependência de terceiros no domínio das TIC. Não obstante alguns esforços para abordar o domínio específico da externalização, tais como as recomendações de 2017 relativas à subcontratação externa a prestadores de serviços de computação em nuvem[34], a questão do risco sistémico que pode ser desencadeado pela exposição do setor financeiro a um conjunto limitado de terceiros prestadores de serviços de TIC críticos só é abordada de forma muito limitada na legislação da União. Esta insuficiência a nível da União é agravada pela ausência de instrumentos e mandatos específicos que permitam às autoridades de supervisão nacionais obterem um bom conhecimento das dependências de terceiros no domínio das TIC e monitorizarem de forma adequada os riscos decorrentes da concentração dessas dependências.

(29) Tendo em conta os potenciais riscos sistémicos que o aumento das práticas de externalização e a concentração ao nível das TIC implicam, e estando ciente da insuficiência dos regimes nacionais que permitem às autoridades financeiras quantificar, qualificar e remediar as consequências dos riscos no domínio das TIC que decorrem dos terceiros prestadores de serviços de TIC críticos, há que estabelecer um quadro de fiscalização adequado que permita a contínua monitorização das atividades dos terceiros prestadores de serviços de TIC que assumam um caráter crítico para as entidades financeiras.

(30) Dado que as ameaças no domínio das TIC têm vindo a tornar-se mais complexas e sofisticadas, a adequação das medidas de deteção e prevenção dependerá, em grande

[34] Recomendações relativas à subcontratação externa a prestadores de serviços de computação em nuvem (EBA/REC/2017/03), revogadas pelas Orientações da EBA relativas à subcontratação (EBA/GL/2019/02).

medida, da partilha regular de informações entre as entidades financeiras sobre as ameaças e vulnerabilidades. A partilha de informações contribui para uma maior sensibilização para as ciberameaças, o que, por sua vez, reforça a capacidade das entidades financeiras para impedirem que essas ameaças se materializem, para melhor conter os efeitos dos incidentes relacionados com as TIC e para recuperar dos mesmos de modo mais eficiente. Na ausência de orientações a nível da União, diversos fatores, nomeadamente a insegurança sobre a compatibilidade com as regras em matéria de proteção de dados, anti-*trust* e de responsabilidade, parecem ter inibido a referida partilha de informações.

(31) Além disso, a hesitação sobre o tipo de informações que podem ser partilhadas com outros intervenientes no mercado, ou com autoridades não supervisoras (como a ENISA, para um contributo analítico, ou a Europol, para fins de aplicação da lei) levou a que informações úteis não fossem partilhadas. A dimensão e a qualidade da partilha de informações continuam a ser limitadas e fragmentadas, sendo os intercâmbios pertinentes sobretudo realizados a nível local (por meio de iniciativas nacionais) e não havendo acordos de partilha de informações a nível da União adaptados às necessidades de um setor financeiro integrado.

(32) Importa portanto incentivar as entidades financeiras a, coletivamente, tirarem partido dos seus conhecimentos e experiências práticas individuais a nível estratégico, tático e operacional, com vista a reforçarem as suas capacidades para, de forma adequada, avaliarem, monitorizarem, se defenderem e darem resposta às ciberameaças. Por conseguinte, é necessário possibilitar o surgimento a nível da União de regimes que prevejam acordos de partilha de informações a título voluntário, que, quando realizada em ambientes fiáveis, ajudaria a comunidade financeira a prevenir e dar resposta coletivamente às ameaças, limitando rapidamente a propagação dos riscos no domínio das TIC e impedindo o possível contágio ao longo dos canais financeiros. O recurso aos referidos regimes deve realizar-se no pleno respeito das regras aplicáveis em matéria de direito da concorrência da União[35], bem como de modo que garanta o pleno respeito das regras da União em matéria de proteção dos dados, em especial o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho[36], nomeadamente no contexto do tratamento de dados pessoais necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, nos termos do artigo 6.º, n.º 1, alínea f), do referido regulamento.

(33) Não obstante a ampla cobertura pretendida com o presente regulamento, a aplicação das regras de resiliência operacional digital deve ter em consideração as significativas diferenças entre as entidades financeiras em termos de dimensão, perfil de atividades ou exposição ao risco digital. Como princípio geral, ao afetarem recursos e capacidades à aplicação do quadro de gestão do risco no domínio das TIC, as entidades financeiras devem equilibrar cuidadosamente as suas necessidades relacionadas com as TIC em função da sua dimensão e do seu perfil de atividades, enquanto as autoridades competentes deverão avaliar e rever de forma recorrente a abordagem de tal afetação.

---

35 Comunicação da Comissão – Orientações sobre a aplicação do artigo 101.º do Tratado sobre o Funcionamento da União Europeia aos acordos de cooperação horizontal, 2011/C 11/01.

36 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

(34) Uma vez que as entidades financeiras de maior dimensão dispõem de mais recursos e conseguirão mais rapidamente mobilizar fundos para desenvolver as estruturas de governação e estabelecer diversas estratégias empresariais, o estabelecimento de estruturas de governação mais complexas só deve ser imposto às entidades financeiras que não sejam microempresas na aceção do presente regulamento. As referidas entidades estão melhor equipadas, em especial, para criarem funções específicas de gestão para supervisionar os acordos com terceiros prestadores de serviços de TIC ou gerir as crises, para organizarem a sua gestão do risco no domínio das TIC de acordo com o modelo das três linhas de defesa, ou ainda para adotarem um documento de recursos humanos que explicite integralmente as políticas de direitos de acesso.

Seguindo o mesmo princípio, apenas as referidas entidades financeiras deverão ser chamadas e realizar avaliações em profundidade após a introdução de alterações importantes nas redes e nas infraestruturas e processos dos sistemas de informação, análises do risco regulares de sistemas de TIC pré-existentes ou a alargar a realização de testes dos planos de continuidade das atividades e de resposta e recuperação para abranger cenários de comutação entre a sua infraestrutura primária de TIC e instalações redundantes.

(35) Além disso, uma vez que apenas as entidades financeiras consideradas significativas para efeitos da realização de testes avançados de resiliência digital devem ser obrigadas a realizar testes de penetração com base em ameaças, os processos administrativos e os custos financeiros que a realização de tais testes implicam devem recair sobre uma pequena percentagem das entidades financeiras. Por fim, com vista a aliviar os encargos regulamentares, apenas as entidades financeiras que não sejam microempresas deverão ter de comunicar regularmente às autoridades competentes todos os custos e perdas provocados por perturbações no domínio das TIC e os resultados das avaliações pós-incidentes na sequência de perturbações significativas a esse nível.

(36) Para assegurar a plena conformidade e a coerência global entre, por um lado, as estratégias de atividade das entidades financeiras e, por outro, a gestão do risco no domínio das TIC, é necessário exigir ao órgão de administração que mantenha um papel fulcral e ativo na orientação e adaptação do quadro de gestão do risco no domínio das TIC e da estratégia global de resiliência digital. A abordagem a adotar pelo órgão de administração deve centrar-se não só nos meios para assegurar a resiliência dos sistemas de TIC como também abranger as pessoas e os processos por meio de um conjunto de políticas que cultivem, em cada nível da empresa e em todos os funcionários, uma boa sensibilização para os riscos cibernéticos e um empenho no respeito de uma ciber-higiene rigorosa a todos os níveis.

A responsabilidade final do órgão de administração pela gestão dos riscos no domínio das TIC de uma entidade financeira deve constituir um princípio global dessa abordagem abrangente, que se deverá também traduzir no empenhamento contínuo do órgão de administração no controlo da monitorização da gestão do risco no domínio das TIC.

(37) Além disso, a total responsabilidade do órgão de administração andará a par com a garantia de um nível do investimento em TIC e do orçamento global da entidade financeira que lhe permita alcançar o seu cenário de referência em matéria de resiliência operacional.

(38) Inspirando-se nas normas, orientações, recomendações ou abordagens pertinentes estabelecidas a nível internacional, nacional e setorial em matéria de gestão do risco

cibernético[37], o presente regulamento promove um conjunto de funções que facilitam a estruturação geral da gestão do risco no domínio das TIC. As entidades financeiras são livres de utilizar modelos de gestão do risco no domínio das TIC enquadrados ou categorizados de diferentes formas, contanto que as principais capacidades que criarem vão ao encontro das necessidades decorrentes dos objetivos previstos pelas funções (identificação, proteção e prevenção, deteção, resposta e recuperação, aprendizagem e evolução e comunicação) estabelecidas no presente regulamento.

(39) Para acompanhar o ritmo de um cenário de ciberameaças em rápida evolução, as entidades financeiras devem dispor de sistemas de TIC atualizados que sejam fiáveis e tenham capacidade suficiente, não só para proceder ao tratamento dos dados necessário à prestação dos seus serviços, mas também para assegurar uma resiliência tecnológica que lhes permita fazer face, de modo adequado, às necessidades adicionais de tratamento que possam ser geradas por condições de tensão no mercado ou por outras situações adversas. Não obstante o facto de não implicar qualquer normalização de sistemas, instrumentos ou tecnologias de TIC específicos, o presente regulamento depende da correta utilização pelas entidades financeiras de normas técnicas (p. ex.: ISO) ou de boas práticas setoriais reconhecidas a nível europeu e internacional, na medida em que essa utilização seja plenamente compatível com as instruções de supervisão específicas sobre a utilização e integração de normas internacionais.

(40) São necessários planos eficientes de continuidade das atividades e de recuperação que permitam às entidades financeiras resolver rápida e atempadamente os incidentes relacionados com as TIC, em especial os ciberataques, limitando os danos e dando prioridade à retoma da atividade e às medidas de recuperação. No entanto, embora os sistemas de recurso devam entrar em funcionamento sem demora, tal não pode, de modo algum, pôr em risco a integridade e segurança das redes e dos sistemas de informação ou a confidencialidade dos dados.

(41) Embora o presente regulamento autorize as entidades financeiras a determinarem de modo flexível os objetivos em termos de tempo de recuperação e, portanto, a estabelecerem tais objetivos tendo plenamente em conta a natureza e o caráter crítico da função pertinente, bem como quaisquer necessidades operacionais específicas, haverá que exigir igualmente uma análise do potencial impacto global na eficiência do mercado ao determinar os referidos objetivos.

(42) As consequências significativas dos ciberataques são amplificadas quando estes ocorrem no setor financeiro, um domínio que se encontra em muito maior risco de ser visado por intervenientes criminosos que procuram obter ganhos financeiros diretamente na fonte. Para atenuar tais riscos, prevenir a perda de integridade ou a indisponibilidade dos sistemas de TIC e a violação de dados confidenciais ou prevenir danos à infraestrutura física de TIC, é necessário melhorar significativamente a comunicação dos incidentes graves relacionados com as TIC pelas entidades financeiras.

---

[37] CPMI-IOSCO, *Guidance on cyber resilience for financial market infrastructures*, https://www.bis.org/cpmi/publ/d146.pdf G7, *Fundamental Elements of Cybersecurity for the Financial Sector*, https://www.ecb.europa.eu/paym/pol/shared/pdf/G7_Fundamental_Elements_Oct_2016.pdf; Quadro de cibersegurança do Instituto Nacional de Normas e Tecnologia, https://www.nist.gov/cyberframework; CEF, *CIRR toolkit*, https://www.fsb.org/2020/04/effective-practices-for-cyber-incident-response-and-recovery-consultative-document.

A comunicação de incidentes relacionados com as TIC deve ser harmonizada para todas as entidades financeiras, exigindo que estas procedam a essa comunicação unicamente às respetivas autoridades competentes. Não obstante o facto de todas as entidades financeiras serem abrangidas por esta obrigação de comunicação, nem todas devem ser afetadas do mesmo modo, uma vez que os prazos e os limiares de materialidade pertinentes devem ser calibrados para abranger unicamente os incidentes relacionados com as TIC mais graves. A comunicação direta permitiria o acesso dos supervisores financeiros a informações sobre incidentes relacionados com as TIC. Todavia, as autoridades de supervisão devem transmitir estas informações às autoridades públicas não financeiras (autoridades competentes no domínio da SRI, autoridades nacionais de proteção de dados e autoridades responsáveis pela aplicação da lei no caso dos incidentes de natureza criminosa). É necessário canalizar as informações sobre os incidentes relacionados com as TIC: os supervisores financeiros devem transmitir todas as observações ou orientações necessárias à entidade financeira, ao passo que as AES devem partilhar dados anonimizados sobre as ameaças e vulnerabilidades relacionadas com um evento para contribuir para uma melhor defesa coletiva.

(43) Haverá que continuar a ponderar a possível centralização da comunicação de incidentes relacionados com as TIC, por meio de uma plataforma única e central da UE que receba diretamente as comunicações pertinentes e proceda automaticamente à notificação das autoridades competentes ou simplesmente centralize os relatórios que lhe sejam transmitidos pelas autoridades competentes nacionais, desempenhando uma função de coordenação. As AES deverão elaborar, em consulta com o BCE e com a ENISA, até uma determinada data, um relatório conjunto que explore a viabilidade do estabelecimento da referida plataforma central da UE.

(44) A fim de alcançar uma robusta resiliência operacional digital, e em consonância com as normas internacionais (p. ex.: os elementos fundamentais da realização de testes de penetração com base em ameaças, elaborados pelo G7), afigura-se oportuno que as entidades financeiras realizem regularmente testes ao seu pessoal e sistemas de TIC em termos de eficácia das respetivas capacidades de prevenção, deteção, resposta e recuperação, por forma a detetar e resolver possíveis vulnerabilidades. Para dar resposta às diferenças existentes entre os subsetores financeiros e dentro dos próprios subsetores em matéria de prontidão no domínio da cibersegurança das entidades financeiras, a realização dos testes deve compreender uma ampla variedade de instrumentos e medidas, desde a avaliação de requisitos básicos (p. ex.: avaliações e análises de vulnerabilidade, análises de código aberto, avaliações da segurança das redes, análises das lacunas, análises da segurança física, questionários e programas informáticos de análise, revisões do código fonte, se possível, testes com base em cenários, testes de compatibilidade, testes de desempenho ou testes de extremo a extremo) aos testes mais avançados (p. ex.: testes de penetração com base em ameaças para as entidades financeiras com uma maturidade suficiente em termos de TIC para poderem realizar tais testes). Os testes de resiliência operacional digital deverão, por conseguinte, ser mais exigentes para as entidades financeiras significativas (tais como grandes instituições de crédito, bolsas de valores, centrais de valores mobiliários, contrapartes centrais, etc.). Simultaneamente, a realização de testes de resiliência operacional digital também deve assumir uma maior relevância para alguns subsetores com uma função sistémica central (p. ex.: pagamentos, banca, compensação e liquidação) e menor relevância para outros subsetores (p. ex.: gestores de ativos, agências de notação de risco, etc.). As entidades financeiras transfronteiriças que exerçam a sua liberdade de estabelecimento ou prestação de serviços na União devem

cumprir um conjunto único de requisitos de realização de testes avançados (p. ex.: testes de penetração com base em ameaças) no respetivo Estado-Membro de origem, devendo os testes abranger as infraestruturas de TIC em todas as jurisdições em que o grupo transfronteiriço desenvolva a sua atividade na União e permitindo assim aos referidos grupos suportar os custos dos testes numa única jurisdição.

(45) A fim de assegurar uma robusta monitorização do risco de terceiros no domínio das TIC, há que estabelecer um conjunto de regras com base em princípios para orientar a monitorização realizada pelas entidades financeiras dos riscos decorrentes da externalização de funções a terceiros prestadores de serviços de TIC e, de modo mais geral, da dependência de terceiros no domínio das TIC.

(46) As entidades financeiras devem ser sempre plenamente responsáveis pelo cumprimento das obrigações decorrentes do presente regulamento. A monitorização proporcionada do risco ao nível dos terceiros prestadores de serviços de TIC deve ser organizada tendo em devida conta a escala, complexidade e importância das dependências relacionadas com as TIC e a criticalidade ou importância dos serviços, dos processos ou das funções objeto de acordos contratuais, bem como, por fim, com base numa cuidadosa avaliação do possível impacto na continuidade e qualidade dos serviços financeiros a nível individual e a nível do grupo, se for caso disso.

(47) A realização de tal monitorização deve seguir uma abordagem estratégica do risco de terceiros no domínio das TIC formalizada por meio da adoção pelo órgão de administração da entidade financeira de uma estratégia específica, radicada na análise contínua de todas essas dependências de terceiros no domínio das TIC. A fim de reforçar a sensibilização para a supervisão de dependências de terceiros no domínio das TIC, e com vista a prestar um maior apoio ao quadro de fiscalização estabelecido no presente regulamento, as autoridades financeiras devem receber informações essenciais dos registos e devem poder solicitar extratos destes numa base *ad hoc*.

(48) À celebração formal dos acordos contratuais deve estar subjacente e deve preceder uma análise exaustiva na fase pré-contratual, sendo a rescisão dos contratos desencadeada mediante, pelo menos, um conjunto de circunstâncias demonstrativas de insuficiências do terceiro prestador de serviços de TIC.

(49) A fim de fazer face ao impacto sistémico do risco de concentração de terceiros no domínio das TIC, há que promover uma solução equilibrada por meio de uma abordagem flexível e gradual, uma vez que o estabelecimento de limites máximos rígidos ou restrições rigorosas pode prejudicar a atividade e a liberdade contratual. As entidades financeiras devem avaliar exaustivamente os acordos contratuais para identificar a probabilidade do surgimento desse risco, incluindo por meio de análises em profundidade de acordos de reexternalização, nomeadamente nos casos em que sejam celebrados com terceiros prestadores de serviços de TIC estabelecidos em países terceiros. Nesta fase, com vista a encontrar a um equilíbrio justo entre o imperativo que dita a preservação da liberdade contratual e o que dita a salvaguarda da estabilidade financeira, não se afigura adequado prever limites máximos rigorosos e limites de exposição a terceiros no domínio das TIC. A AES incumbida da fiscalização de cada terceiro prestador de serviços de TIC (a «autoridade de fiscalização principal») deve, no exercício das suas atribuições de fiscalização, prestar especial atenção para compreender plenamente a magnitude das interdependências e descobrir situações específicas em que seja provável que um elevado nível de concentração de terceiros prestadores de serviços de TIC na União ponha sob pressão a estabilidade e integridade do sistema financeiro da União, devendo antes propiciar um diálogo com

terceiros prestadores de serviços de TIC críticos, sempre que esse risco seja identificado[38].

(50) A fim de possibilitar a avaliação e monitorização regular da capacidade do terceiro prestador de serviços de TIC de prestar de modo seguro os serviços à entidade financeira sem afetar negativamente a resiliência desta última, há que proceder à harmonização dos elementos contratuais fundamentais durante a execução dos contratos com terceiros prestadores de serviços de TIC. Os referidos elementos abrangem unicamente aspetos contratuais mínimos considerados cruciais para possibilitar a plena monitorização realizada pela entidade financeira do ponto de vista da salvaguarda da sua resiliência, que depende da estabilidade e segurança do serviço de TIC.

(51) Os acordos contratuais devem, em especial, prever a especificação das descrições completas das funções e dos serviços, bem como dos locais em que tais funções são desempenhadas e onde são tratados os dados, assim como uma indicação das descrições completas do nível de serviço acompanhada de metas de desempenho quantitativas e qualitativas no âmbito dos níveis de serviço acordados, para permitir a realização de uma efetiva monitorização pela entidade financeira. Do mesmo modo, as disposições sobre a acessibilidade, a disponibilidade, a integridade, a segurança e a proteção de dados pessoais, assim como as garantias de acesso, recuperação e devolução em caso de insolvência, resolução ou cessação da atividade do terceiro prestador de serviços de TIC devem ser consideradas elementos essenciais da capacidade da entidade financeira de assegurar a monitorização do risco de terceiros.

(52) Para assegurar que as entidades financeiras continuam a ter pleno controlo de todos os acontecimentos suscetíveis de debilitar a respetiva segurança no domínio das TIC, há que estabelecer períodos de pré-aviso e obrigações de comunicação do terceiro prestador de serviços de TIC caso surjam acontecimentos com um potencial impacto importante na capacidade de o terceiro prestador de serviços de TIC desempenhar eficazmente funções críticas ou importantes, incluindo a prestação de assistência por este último em caso de incidente relacionado com as TIC sem custos adicionais ou a um custo previamente determinado.

(53) Os direitos de acesso, inspeção ou auditoria por parte da entidade financeira ou de um terceiro designado para o efeito constituem instrumentos cruciais da monitorização contínua realizada pelas entidades financeiras do desempenho do terceiro prestador de serviços de TIC, juntamente com a plena cooperação deste último durante as inspeções. Do mesmo modo, também a autoridade competente da entidade financeira deve ter o direito, mediante notificação, de inspecionar e auditar o terceiro prestador de serviços de TIC, sob reserva da confidencialidade.

(54) Os acordos contratuais devem prever direitos de rescisão claros e os prazos de pré-aviso conexos, assim como estratégias de saída que possibilitem, em especial, períodos obrigatórios de transição durante os quais o terceiro prestador de serviços de TIC deve continuar a desempenhar as funções pertinentes com vista a reduzir o risco de perturbações a nível da entidade financeira e permitir a esta última substituir

[38] Além disso, caso surja um risco de abuso por parte de um terceiro prestador de serviços de TIC considerado dominante, as entidades financeiras devem ainda ter a possibilidade de apresentar uma queixa formal ou informal junto da Comissão Europeia ou das autoridades nacionais no domínio do direito da concorrência.

efetivamente o terceiro prestador de serviços de TIC ou, em alternativa, recorrer a soluções internas, coerentes com a complexidade do serviço prestado.

(55) Além disso, a utilização a título voluntário de cláusulas contratuais normalizadas desenvolvidas pela Comissão para os serviços de computação em nuvem podem, igualmente, tranquilizar as entidades financeiras e os respetivos terceiros prestadores de serviços de TIC, reforçando o nível de segurança jurídica quanto à utilização de serviços de computação em nuvem pelo setor financeiro, em total consonância com os requisitos e as expetativas estabelecidas pela regulamentação relativa aos serviços financeiros. Os esforços assentam em medidas já previstas no Plano de Ação para a Tecnologia Financeira de 2018, no qual a Comissão anunciou a sua intenção de incentivar a elaboração de cláusulas contratuais-tipo para o recurso à externalização de serviços de computação em nuvem pelas instituições financeiras, tirando partido dos esforços das partes interessadas da computação em nuvem a nível intersetorial já facilitados pela Comissão, com o apoio da participação do setor financeiro.

(56) A fim de promover a convergência e eficiência no que respeita às abordagens de supervisão do risco de terceiros no domínio das TIC para o setor financeiro, reforçar a resiliência operacional digital das entidades financeiras que dependem de terceiros prestadores de serviços de TIC críticos para o desempenho de funções operacionais e, assim, contribuir para preservar a estabilidade do sistema financeiro da União e a integridade do mercado único de serviços financeiros, os terceiros prestadores de serviços de TIC críticos devem estar sujeitos a um quadro de fiscalização da União.

(57) Uma vez que a aplicação de um tratamento especial só se justifica no caso dos terceiros prestadores de serviços críticos, há que estabelecer um regime de designação para efeitos de aplicação do Quadro de Fiscalização da União, para ter em conta a dimensão e natureza da dependência do setor financeiro de tais terceiros prestadores de serviços de TIC, que se traduza num conjunto de critérios quantitativos e qualitativos que fundamentaria a inclusão para efeitos de fiscalização nos parâmetros de criticalidade. É conveniente conceder uma opção de inclusão a título voluntário no Quadro de Fiscalização aos terceiros prestadores de serviços de TIC que não sejam automaticamente designados em virtude da aplicação dos critérios supramencionados, ao passo que os terceiros prestadores de serviços de TIC que já estejam sujeitos a quadros de regimes de fiscalização estabelecidos a nível do Eurosistema com vista a apoiar as atribuições a que se refere o artigo 127.º, n.º 2, do Tratado sobre o Funcionamento da União Europeia devem, consequentemente, estar isentos.

(58) O requisito de constituição na União dos terceiros prestadores de serviços de TIC que tenham sido designados como críticos não equivale à localização dos dados, uma vez que o presente regulamento não implica qualquer outro requisito em matéria de armazenamento ou tratamento de dados na União.

(59) O referido quadro não pode prejudicar a competência dos Estados-Membros no que respeita à realização de missões de inspeção de terceiros prestadores de serviços de TIC que não sejam críticos na aceção do presente regulamento, mas que possam ser considerados importantes a nível nacional.

(60) A fim de potencializar a existente arquitetura institucional multifacetada no domínio dos serviços financeiros, o Comité Conjunto das AES deve continuar a assegurar a coordenação intersetorial global quanto a todas as matérias relativas ao risco no domínio das TIC, em consonância com as suas atribuições em matéria de cibersegurança, com o apoio de um novo subcomité (o Fórum de Fiscalização), que leva a cabo os trabalhos preparatórios quer para as decisões individuais dirigidas a

terceiros prestadores de serviços de TIC críticos quer para as recomendações coletivas, nomeadamente sobre a avaliação comparativa dos programas de fiscalização de terceiros prestadores de serviços de TIC críticos e a identificação de boas práticas para dar resposta às questões relativas ao risco de concentração no domínio das TIC.

(61) A fim de assegurar que os terceiros prestadores de serviços de TIC que desempenham uma função crítica no funcionamento do setor financeiro são objeto de uma fiscalização proporcionada à escala da União, uma das AES deve ser designada como Autoridade de Fiscalização Principal em relação a cada terceiro prestador de serviços de TIC crítico.

(62) A Autoridade de Fiscalização Principal deve estar habilitada a realizar investigações e inspeções no local e administrativas a terceiros prestadores de serviços TIC críticos, aceder a todas as instalações e locais pertinentes e obter informações completas e atualizadas que lhe permitam obter um efetivo conhecimento do tipo, da dimensão e do impacto do risco de terceiros no domínio das TIC que as entidades financeiras e, em última análise, o sistema financeiro da União enfrentam.

Confiar às AES a liderança da fiscalização constitui uma condição prévia para compreender e fazer face à dimensão sistémica do risco no domínio das TIC no setor financeiro. A pegada da União em matéria de terceiros prestadores de serviços de TIC críticos e as potenciais questões sobre a concentração do risco no domínio das TIC dela decorrentes exigem a adoção de uma abordagem coletiva a nível da União. A realização de diversas auditorias e o exercício dos direitos de acesso por numerosas autoridades competentes, separadamente, com pouca ou nenhuma coordenação, não conduziria a uma visão global completa do risco de terceiros no domínio das TIC, criando uma redundância, um ónus e uma complexidade desnecessária para os terceiros prestadores de serviços de TIC críticos que teriam de fazer face a numerosos pedidos do género.

(63) Além disso, é importante que as Autoridades de Fiscalização Principais possam apresentar recomendações sobre questões relativas ao risco no domínio das TIC, nomeadamente a oposição a determinados acordos contratuais que, em última análise, afetariam a estabilidade da entidade financeira ou do sistema financeiro. Como parte da respetiva função de supervisão prudencial das entidades financeiras, as autoridades competentes nacionais devem ponderar devidamente o cumprimento de tais recomendações importantes formuladas pelas Autoridades de Fiscalização Principais.

(64) O Quadro de Fiscalização não substitui, de forma alguma ou em parte alguma, a gestão que as entidades financeiras fazem do risco decorrente do recurso a terceiros prestadores de serviços de TIC, nomeadamente, a obrigação de monitorização contínua dos respetivos acordos contratuais celebrados com terceiros prestadores de serviços de TIC críticos, nem afeta a total responsabilidade das entidades financeiras pelo cumprimento de todos os requisitos do presente regulamento e da legislação pertinente em matéria de serviços financeiros. A fim de evitar duplicações e sobreposições, as autoridades competentes devem evitar adotar medidas de modo individual que visem a monitorização dos riscos de terceiros prestadores de serviços de TIC críticos, devendo todas essas medidas ser previamente coordenadas e acordadas no contexto do Quadro de Fiscalização.

(65) A fim de promover a convergência a nível internacional em matéria de boas práticas a aplicar no exame da gestão do risco digital de terceiros prestadores de serviços de TIC, é necessário incentivar as AES a celebrarem acordos de cooperação com as autoridades competentes de supervisão e regulamentação de países terceiros, para

facilitar o desenvolvimento de boas práticas em matéria de risco de terceiros no domínio das TIC.

(66) Para potencializar os conhecimentos técnicos especializados dos peritos das autoridades competentes em matéria de gestão do risco operacional e no domínio das TIC, as Autoridades de Fiscalização Principais devem tirar partido da experiência de supervisão nacional e estabelecer equipas de avaliação para cada terceiro prestador de serviços de TIC crítico, colocando em comum equipas multidisciplinares para apoiar a preparação e a efetiva execução de atividades de fiscalização, nomeadamente inspeções no local a terceiros prestadores de serviços de TIC críticos, bem como o necessário acompanhamento posterior.

(67) As autoridades competentes devem estar investidas de todos os poderes de supervisão, investigação e sancionatórios necessários para garantir a aplicação do presente regulamento. As sanções administrativas deverão, em princípio, ser publicadas. Uma vez que as entidades financeiras e os terceiros prestadores de serviços de TIC podem estar estabelecidos em diferentes Estados-Membros e ser supervisionados por diferentes autoridades setoriais competentes, há que assegurar uma cooperação estreita entre as autoridades competentes relevantes, incluindo o BCE, no que diz respeito às atribuições específicas que lhe são conferidas pelo Regulamento (UE) n.º 1024/2013 do Conselho[39], bem como a consulta das AES, através do intercâmbio de informações e da prestação de assistência no contexto das atividades de supervisão.

(68) A fim de quantificar e qualificar mais aprofundadamente os critérios de designação de terceiros prestadores de serviços de TIC críticos e harmonizar as taxas de fiscalização, o poder de adotar atos nos termos do artigo 290.º do Tratado sobre o Funcionamento da União Europeia deve ser delegado na Comissão no que diz respeito: a uma especificação mais aprofundada do impacto sistémico que uma falha de um terceiro prestador de serviços de TIC pode ter nas entidades financeiras a quem presta serviços, aos números de instituições de importância sistémica global (G-SII) ou outras instituições de importância sistémica (O-SII) que dependem do respetivo terceiro prestador de serviços de TIC, ao número de terceiros prestadores de serviços de TIC ativos num determinado mercado, aos custo de migração para outro terceiro prestador de serviços de TIC, ao número de Estados-Membros em que o terceiro prestador de serviços de TIC pertinente presta serviços e em que as entidades financeiras que recorrem ao terceiro prestador de serviços de TIC desenvolvem a sua atividade, bem como o montante de taxas de fiscalização e as respetivas formas de pagamento.

É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível de peritos, e que essas consultas sejam conduzidas de acordo com os princípios estabelecidos no Acordo Interinstitucional «Legislar Melhor», de 13 de abril de 2016[40]. Em especial, e a fim de assegurar a igualdade de participação na preparação de atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros e os seus próprios peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão incumbidos da elaboração dos atos delegados.

---

39 Regulamento (UE) n.º 1024/2013 do Conselho, de 15 de outubro de 2013, que confere ao BCE atribuições específicas no que diz respeito às políticas relativas à supervisão prudencial das instituições de crédito (JO L 287 de 29.10.2013, p. 63).

40 JO L 123 de 12.5.2016, p. 1.

(69) Uma vez que o presente regulamento, juntamente com a Diretiva (UE) 20xx/xx do Parlamento Europeu e do Conselho[41], implica uma consolidação das disposições em matéria de gestão do risco no domínio das TIC dispersas por diversos regulamentos e diretivas do acervo da União em matéria de serviços financeiros, nomeadamente os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 e (UE) n.º 909/2014, a fim de assegurar a total coerência, há que alterar os referidos regulamentos para clarificar que as disposições pertinentes relacionadas com o risco no domínio das TIC são estabelecidas no presente regulamento.

É conveniente que se assegure a harmonização dos requisitos estabelecidos no presente regulamento por meio de normas técnicas. Enquanto organismos com conhecimentos muito especializados, há que mandatar as AES para elaborarem projetos de normas técnicas de regulamentação que não impliquem escolhas políticas, a apresentar à Comissão. Devem ser desenvolvidas normas técnicas de regulamentação em matéria de gestão do risco no domínio das TIC, comunicação, realização de testes e requisitos essenciais para uma robusta monitorização do risco de terceiros no domínio das TIC.

(70) É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive ao nível dos peritos. A Comissão e as AES devem assegurar que essas normas e requisitos podem ser aplicados por todas as entidades financeiras de forma proporcionada tendo em conta a natureza, escala e complexidade dessas entidades e das respetivas atividades.

(71) Para facilitar a comparabilidade dos relatórios de incidentes graves relacionados com as TIC e assegurar a transparência dos acordos contratuais a utilizar no âmbito dos serviços de TIC prestados por terceiros prestadores de serviços de TIC, importa mandatar as AES para elaborarem projeto de normas técnicas de execução que criem procedimentos, formulários e modelos normalizados para que as entidades possam comunicar incidentes graves relacionados com as TIC, bem como modelos normalizados para o registo de informações. Ao elaborar as referidas normas, as AES devem ter em conta a dimensão e complexidade das entidades financeiras, bem como a natureza e o nível de risco das respetivas atividades. A Comissão deverá ser ainda habilitada a adotar as referidas normas técnicas de execução por meio de atos de execução nos termos do artigo 291.º do TFUE e em conformidade com o artigo 15.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010, (UE) n.º 1095/2010, respetivamente. Dado que já foram especificados requisitos adicionais por meio de atos de delegados e de execução com base em normas técnicas de regulamentação e normas técnicas de execução nos Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 e (UE) n.º 909/2014, respetivamente, afigura-se oportuno mandatar as AES, seja a título individual ou conjuntamente, por meio do Comité Conjunto, para apresentarem normas técnicas de regulamentação e execução à Comissão para adoção de atos delegados e de execução que transponham ou atualizem as regras vigentes de gestão do risco no domínio das TIC.

(72) Para o efeito, será necessário uma posterior alteração dos atos delegados e de execução em vigor em diversos domínios da legislação em matéria de serviços financeiros. É necessário alterar o âmbito de aplicação dos artigos referentes ao risco operacional com base nos quais a habilitação dos referidos atos incumbe da adoção de atos delegados e de execução, com vista a transpor para o presente regulamento todas as

[41] [*Inserir referência completa*]

disposições que abrangem a resiliência operacional digital que atualmente integram os referidos regulamentos.

(73) Atendendo a que o objetivo do presente regulamento, a saber, alcançar um elevado nível de resiliência operacional digital em relação a todas as entidades financeiras, não pode ser suficientemente alcançado pelos Estados-Membros por requerer a harmonização de uma multiplicidade de regras diferentes atualmente vigentes ou em alguns atos da União ou nos sistemas jurídicos dos diferentes Estados-Membros, mas pode, devido à sua dimensão e aos seus efeitos, ser mais bem alcançado a nível da União, a União pode tomar medidas em conformidade com o princípio da subsidiariedade consagrado no artigo 5.º do Tratado da União Europeia. Em conformidade com o princípio da proporcionalidade consagrado no mesmo artigo, o presente regulamento não excede o necessário para atingir aquele objetivo.

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

DISPOSIÇÕES GERAIS

Artigo 1.º

Objeto

1. O presente regulamento estabelece os seguintes requisitos uniformes no que respeita à segurança das redes e sistemas de informação que apoiam os processos operacionais das entidades financeiras necessários para alcançar um elevado nível de resiliência operacional digital:

   (a) Requisitos aplicáveis às entidades financeiras em matéria de:

   – gestão do risco no domínio das Tecnologias da Informação e Comunicação (TIC),

   – comunicação de incidentes graves relacionados com as TIC às autoridades competentes,

   – realização de testes de resiliência operacional digital,

   – partilha de dados e informações sobre as ciberameaças e as vulnerabilidades informáticas,

   – medidas para a boa gestão do risco de terceiros no domínio das TIC pelas entidades financeiras;

   (b) Requisitos referentes aos acordos contratuais celebrados entre terceiros prestadores de serviços de TIC e entidades financeiras;

   (c) Quadro de fiscalização dos terceiros prestadores de serviços de TIC críticos na prestação desses serviços a entidades financeiras;

   (d) Regras de cooperação entre as autoridades competentes e regras de supervisão e aplicação da lei pelas autoridades competentes em todas as matérias abrangidas pelo presente regulamento.

2. Quanto às entidades financeiras identificadas como operadores de serviços essenciais nos termos das regras nacionais que transpõem o artigo 5.º da

Diretiva (UE) 2016/1148, considera-se que o presente regulamento constitui um ato jurídico setorial da União para efeitos do artigo 1.º, n.º 7, da referida diretiva.

Artigo 2.º

Âmbito de aplicação pessoal

1. O presente regulamento é aplicável às seguintes entidades:

(a) Instituições de crédito;

(b) Instituições de pagamento;

(c) Instituições de moeda eletrónica;

(d) Empresas de investimento;

(e) Prestadores de serviços de criptoativos, emitentes de criptoativos, emitentes de criptofichas referenciadas a ativos e emitentes de criptofichas referenciadas a ativos significativas;

(f) Centrais de valores mobiliários;

(g) Contrapartes centrais;

(h) Plataformas de negociação;

(i) Repositórios de transações;

(j) Gestores de fundos de investimento alternativos;

(k) Sociedades gestoras;

(l) Prestadores de serviços de comunicação de dados;

(m) Empresas de seguros e de resseguros;

(n) Mediadores de seguros, mediadores de resseguros e mediadores de seguros a título acessório;

(o) Instituições de realização de planos de pensões profissionais

(p) Agências de notação de risco;

(q) Revisores oficiais de contas e sociedades de revisores oficiais de contas;

(r) Administradores de índices de referência críticos;

(s) Prestadores de serviços de financiamento colaborativo;

(t) Repositórios de titularizações;

(u) Terceiros prestadores de serviços de TIC.

2. Para efeitos do presente regulamento, as entidades a que se referem as alíneas a) a t) são coletivamente referidas como «entidades financeiras».

Artigo 3.º

Definições

Para efeitos do presente regulamento, entende-se por:

(1) «Resiliência operacional digital», a capacidade da entidade financeira para criar, assegurar e reavaliar a sua integridade operacional de um ponto de vista tecnológico, assegurando direta ou indiretamente, com recurso a serviços de terceiros prestadores

de serviços de TIC, toda a gama de capacidades relacionadas com as TIC necessárias para salvaguardar a segurança das redes e dos sistemas de informação que a entidade financeira utiliza e que permitem a contínua prestação de serviços financeiros e a qualidade dos mesmos;

(2) «Rede e sistema de informação», uma rede e sistema de informação na aceção do artigo 4.º, ponto 1, da Diretiva (UE) 2016/1148;

(3) «Segurança das redes e dos sistemas de informação», a segurança das redes e dos sistemas de informação na aceção do artigo 4.º, ponto 2, da Diretiva (UE) 2016/1148;

(4) «Risco no domínio das TIC», qualquer circunstância razoavelmente identificável relacionada com a utilização de redes e sistemas de informação – nomeadamente, uma avaria, sobrecarga, falha, perturbação, degradação, utilização abusiva, perda ou outro tipo de evento doloso ou não doloso – que, caso se materialize, pode comprometer a segurança das redes e dos sistemas de informação, de qualquer instrumento ou processo tecnológico, do funcionamento e da execução de processos ou da prestação de serviços, comprometendo assim a integridade ou disponibilidade dos dados, dos programas informáticos ou de quaisquer outras componentes dos serviços e das infraestruturas de TIC ou provocando uma violação da confidencialidade, um dano à infraestrutura física das TIC ou outros efeitos adversos;

(5) «Ativo de informação», um conjunto de informações, tangível ou intangível, que deve ser protegido;

(6) «Incidente relacionado com as TIC», uma ocorrência identificada imprevista nas redes e sistemas de informação, seja ela resultante de atividade dolosa ou não, que comprometa a segurança das redes e sistemas de informação, das informações tratadas, armazenadas ou transmitidas pelos referidos sistemas ou tenha quaisquer efeitos adversos na disponibilidade, confidencialidade, continuidade ou autenticidade dos serviços financeiros prestados pela entidade financeira;

(7) «Incidente grave relacionado com as TIC», um incidente relacionado com as TIC com um impacto negativo potencialmente elevado nas redes e sistemas de informação que apoiam as funções críticas da entidade financeira;

(8) «Ciberameaça», uma ciberameaça na aceção do artigo 2.º, ponto 8, do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[42];

(9) «Ciberataque», um incidente doloso relacionado com as TIC numa tentativa de destruir, revelar, alterar, incapacitar, furtar, obter acesso não autorizado ou utilizar sem autorização um ativo, perpetrado por qualquer tipo de autor de ameaças;

(10) «Informações sobre ameaças», as informações que foram agregadas, transformadas, analisadas, interpretadas ou suplementadas para dar o contexto necessário à tomada de decisão e que proporcionam um conhecimento pertinente e suficiente para atenuar o impacto de um incidente relacionado com as TIC ou de uma ciberameaça, incluindo os pormenores técnicos de um ciberataque, os respetivos autores, a sua forma de atuar e as suas motivações;

[42] Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho, de 17 de abril de 2019, relativo à ENISA (Agência da União Europeia para a Cibersegurança) e à certificação da cibersegurança das tecnologias da informação e comunicação e que revoga o Regulamento (UE) n.º 526/2013 (Regulamento Cibersegurança) (JO L 151 de 7.6.2019, p. 15).

(11) «Defesa em profundidade», uma estratégia relacionada com as TIC que integra pessoas, processos e tecnologias para criar uma diversidade de obstáculos em diversos níveis e dimensões da entidade;

(12) «Vulnerabilidade», um ponto fraco, uma suscetibilidade ou uma falha de um ativo, sistema, processo ou controlo suscetível de ser explorado por uma ameaça;

(13) «Testes de penetração com base em ameaças», um 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 críticos de produção da entidade;

(14) «Risco de terceiros no domínio das TIC», o risco no domínio das TIC a que uma entidade financeira pode estar sujeita devido à sua utilização de serviços de TIC prestados por terceiros prestadores de serviços de TIC ou por outros subcontratantes desses terceiros;

(15) «Terceiro prestador de serviços de TIC», uma empresa que presta serviços digitais e de dados, nomeadamente prestadores de serviços de computação em nuvem, programas informáticos, serviços de análise de dados, centros de dados, mas com exclusão dos fornecedores de componentes de equipamento informático e as empresas autorizadas ao abrigo do direito da União a prestar serviços de comunicações eletrónicas na aceção do artigo 2.º, ponto 4, da Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho[43];

(16) «Serviços de TIC», os serviços digitais e de dados prestados por meio de sistemas de TIC a um ou mais utilizadores internos ou externos, nomeadamente o fornecimento, introdução e armazenamento de dados, os serviços de tratamento e de comunicação de dados ou o controlo de dados, bem como os serviços de apoio comercial ou de apoio à tomada de decisões com base em dados;

(17) «Função crítica ou importante», uma função cuja interrupção, anomalia ou falha debilitaria consideravelmente o contínuo cumprimento das condições e obrigações decorrentes da autorização da entidade financeira, ou das suas restantes obrigações ao abrigo da legislação aplicável no domínio dos serviços financeiros, ou o seu desempenho financeiro ou a solidez ou continuidade dos seus serviços e das suas atividades;

(18) «Terceiro prestador de serviços de TIC crítico», um terceiro prestador de serviços de TIC designado nos termos do artigo 29.º e sujeito ao Quadro de Fiscalização a que se referem os artigos 30.º a 37.º;

(19) «Terceiro prestador de serviços de TIC estabelecido num país terceiro», um terceiro prestador de serviços de TIC que seja uma pessoa coletiva estabelecida num país terceiro, não tenha atividade/não esteja presente na União e tenha celebrado um acordo contratual com uma entidade financeira para a prestação de serviços de TIC;

(20) «Subcontratante de TIC estabelecido num país terceiro», um subcontratante de TIC que seja uma pessoa coletiva estabelecida num país terceiro, não tenha atividade/não esteja presente na União e tenha celebrado um acordo contratual ou com um terceiro

[43] Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho, de 11 de dezembro de 2018, que estabelece o Código Europeu das Comunicações Eletrónicas (reformulação), (JO L 321 de 17.12.2018, p. 36).

prestador de serviços de TIC ou com ou terceiro prestador de serviços de TIC estabelecido num país terceiro;

(21) «Risco de concentração no domínio das TIC», a exposição a um ou mais terceiros prestadores de serviços de TIC críticos que cria um nível de dependência desses prestadores de tal modo que a indisponibilidade, uma avaria ou outro tipo de insuficiência destes últimos pode pôr em perigo a capacidade de uma entidade financeira, e, em última análise, do sistema financeiro da União no seu todo, para desempenhar funções críticas, ou acarretar outro tipo de efeitos negativos para essa entidade, incluindo perdas consideráveis;

(22) «Órgão de administração», o órgão de administração na aceção do artigo 4.º, n.º 1, ponto 36, da Diretiva 2014/65/UE, do artigo 3.º, n.º 1, ponto 7, da Diretiva 2013/36/UE, do artigo 2.º, n.º 1, alínea s), da Diretiva 2009/65/CE, do Artigo 2.º, n.º 1, ponto 45, do Regulamento (UE) n.º 909/2014, do artigo 3.º, n.º 1, ponto 20, do Regulamento (UE) 2016/1011 do Parlamento Europeu e do Conselho[44] e do artigo 3.º, n.º 1, alínea u), do Regulamento (UE) 20xx/xx do Parlamento Europeu e do Conselho[45] [MICA] ou as pessoas equivalentes que administram efetivamente a entidade ou desempenham funções fundamentais em conformidade com a legislação nacional ou da União pertinente;

(23) «Instituição de crédito», uma instituição de crédito na aceção do artigo 4.º, n.º 1, ponto 1, do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho[46];

(24) «Empresa de investimento», uma empresa de investimento na aceção do artigo 4.º, n.º 1, ponto 1, da Diretiva 2014/65/UE;

(25) «Instituição de pagamento», uma instituição de pagamento na aceção do artigo 1.º, n.º 1, alínea d), da Diretiva (UE) 2015/2366;

(26) «Instituição de moeda eletrónica», uma instituição de moeda eletrónica na aceção do artigo 2.º, ponto 1), da Diretiva 2009/110/CE do Parlamento Europeu e do Conselho[47];

(27) «Contraparte central», uma contraparte central na aceção do artigo 2.º, ponto 1, do Regulamento (UE) n.º 648/2012;

(28) «Repositório de transações», um repositório de transações na aceção do artigo 2.º, ponto 2, do Regulamento (UE) n.º 648/2012;

(29) «Central de valores mobiliário», uma central de valores mobiliários na aceção do artigo 2.º, n.º 1, ponto 1, do Regulamento (UE) n.º 909/2014;

---

44 Regulamento (UE) 2016/1011 do Parlamento Europeu e do Conselho, de 8 de junho de 2016, relativo aos índices utilizados como índices de referência no quadro de instrumentos e contratos financeiros ou para aferir o desempenho de fundos de investimento e que altera as Diretivas 2008/48/CE e 2014/17/UE e o Regulamento (UE) n.º 596/2014 (JO L 171 de 29.6.2016, p. 1).

45 [*Inserir título completo e informação do JO*].

46 Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento e que altera o Regulamento (UE) n.º 648/2012 (JO L 176 de 27.6.2013, p. 1).

47 Diretiva 2009/110/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, relativa ao acesso à atividade das instituições de moeda eletrónica, ao seu exercício e à sua supervisão prudencial, que altera as Diretivas 2005/60/CE e 2006/48/CE e revoga a Diretiva 2000/46/CE (JO L 267 de 10.10.2009, p. 7).

(30) «Plataforma de negociação», uma plataforma de negociação na aceção do artigo 4.º, n.º 1, ponto 24, da Diretiva 2014/65/UE;

(31) «Gestor de fundos de investimento alternativos», um gestor de fundos de investimento alternativos na aceção do artigo 4.º, n.º 1, alínea b), da Diretiva 2011/61/UE;

(32) «Sociedade gestora», uma sociedade gestora na aceção do artigo 2.º, n.º 1, alínea b), da Diretiva 2009/65/CE;

(33) «Prestador de serviços de comunicação de dados», um prestador de serviços de comunicação de dados na aceção do artigo 4.º, n.º 1, ponto 63, da Diretiva 2014/65/UE;

(34) «Empresa de seguros», uma empresa de seguros na aceção do artigo 13.º, ponto 1, da Diretiva 2009/138/CE;

(35) «Empresa de resseguros», uma empresa de resseguros na aceção do artigo 13.º, ponto 4, da Diretiva 2009/138/CE;

(36) «Mediador de seguros», um mediador de seguros na aceção do artigo 2.º, n.º 1, ponto 3, da Diretiva (UE) 2016/97;

(37) «Mediador de seguros a título acessório», um mediador de seguros a título acessório na aceção do artigo 2.º, n.º 1, ponto 4, da Diretiva (UE) 2016/97;

(38) «Mediador de resseguros», um mediador de resseguros na aceção do artigo 2.º, n.º 1, ponto 5, da Diretiva (UE) 2016/97;

(39) «Instituição de realização de planos de pensões profissionais», uma instituição de realização de planos de pensões profissionais na aceção do artigo 6.º, ponto 1, da Diretiva (UE) 2016/2341;

(40) «Agência de notação de risco», uma agência de notação de risco na aceção do artigo 3.º, n.º 1, alínea a), do Regulamento (CE) n.º 1060/2009;

(41) «Revisor oficial de contas», um revisor oficial de contas na aceção do artigo 2.º, ponto 2, da Diretiva 2006/43/CE;

(42) «Sociedade de revisores oficiais de contas», uma sociedade de revisores oficiais de contas na aceção do artigo 2.º, ponto 3, da Diretiva 2006/43/CE;

(43) «Prestador de serviços de criptoativos», um prestador de serviços de criptoativos na aceção do artigo 3.º, n.º 1, alínea n), do Regulamento (UE) 202x/xx [*Serviço das Publicações: inserir referência do MICAR*];

(44) «Emitente de criptoativos», um emitente de criptoativos na aceção do artigo 3.º, n.º 1, alínea h), do [*Serviço das Publicações: inserir referência do MICAR*];

(45) «Emitente de criptofichas referenciadas a ativos», um emitente de criptofichas referenciadas a ativos na aceção do artigo 3.º, n.º 1, alínea i), do [*Serviço das Publicações: inserir referência do MICAR*];

(46) «Emitente de criptofichas referenciadas a ativos significativas», um emitente de criptofichas referenciadas a ativos significativas na aceção do artigo 3.º, n.º 1, alínea j), do [*Serviço das Publicações: inserir referência do MICAR*];

(47) «Administrador de índices de referência críticos», um administrador de índices de referência críticos na aceção do artigo x, alínea x), do Regulamento (UE) xx/202x [*Serviço das Publicações: inserir referência do Regulamento Índices de Referência*];

(48) «Prestador de serviços de financiamento colaborativo», um prestador de serviços de financiamento colaborativo na aceção do artigo x, alínea x), do Regulamento (UE) 202x/xx [*Serviço das Publicações: inserir referência do Regulamento Financiamento Colaborativo*];

(49) «Repositório de titularizações», um repositório de titularizações na aceção do artigo 2.º, ponto 23, do Regulamento (UE) 2017/2402;

(50) «Microempresa», uma entidade financeira na aceção do artigo 2.º, ponto 3, do anexo da Recomendação 2003/361/CE.

CAPÍTULO II

GESTÃO DO RISCO NO DOMÍNIO DAS TIC

SECÇÃO I

Artigo 4.º

Governação e organização

1. As entidades financeiras devem implantar quadros de governação e controlo que garantam uma gestão eficaz e prudente de todos os riscos no domínio das TIC.

2. O órgão de administração da entidade financeira define, aprova, fiscaliza e é responsável pela aplicação de todas as disposições relacionadas com o quadro de gestão do risco no domínio das TIC a que se refere o artigo 5.º, n.º 1.

Para efeitos do primeiro parágrafo, o órgão de administração deve:

(a) Assumir a responsabilidade final pela gestão dos riscos no domínio das TIC da entidade financeira;

(b) Estabelecer competências e responsabilidades claras para todas as funções relacionadas com as TIC;

(c) Determinar o nível adequado de tolerância ao risco no domínio das TIC da entidade financeira, como referido no artigo 5.º, n.º 9, alínea b);

(d) Aprovar, fiscalizar e reavaliar periodicamente a aplicação da política de continuidade das atividades no domínio das TIC e do plano de recuperação em caso de catástrofe no domínio das TIC a que se refere o artigo 10.º, n.^{os} 1 e 3, respetivamente;

(e) Aprovar e reavaliar periodicamente os planos de auditoria das TIC, as auditorias das TIC e as alterações significativas a esse nível;

(f) Atribuir e reavaliar periodicamente um orçamento adequado para suprir as necessidades da entidade financeira em matéria de resiliência operacional digital a respeito de todos os tipos de recursos, incluindo formação sobre as competências e os riscos no domínio das TIC para todos os funcionários pertinentes;

(g) Aprovar e reavaliar periodicamente a política da entidade financeira em matéria de acordos relativos à utilização de serviços de TIC prestados por terceiros;

(h) Ser devidamente informado sobre os acordos celebrados para a utilização de serviços de TIC prestados por terceiros, sobre quaisquer alterações significativas previstas relativas aos terceiros prestadores de serviços de TIC e sobre o potencial impacto de tais alterações em funções críticas ou importantes objeto dos referidos acordos, nomeadamente por meio de um resumo da análise do risco para avaliar os impactos das referidas alterações;

(i) Ser devidamente informado sobre os incidentes relacionados com as TIC e o respetivo impacto e sobre as medidas corretivas, de resposta e de recuperação.

3. As entidades financeiras, salvo as microempresas, devem criar um cargo para monitorizar os acordos celebrados com terceiros prestadores de serviços de TIC relativos à utilização de serviços de TIC ou designar um membro da direção de topo responsável pela fiscalização da exposição ao risco conexo e pela documentação pertinente.

4. Os membros do órgão de administração devem frequentar regularmente ações de formação específica para obter e manter um nível de conhecimentos e competências suficiente para compreender e avaliar os riscos no domínio das TIC e o respetivo impacto no funcionamento da entidade financeira.

SECÇÃO II

Artigo 5.º

Quadro de gestão do risco associado às TIC

1. As entidades financeiras devem dispor de um quadro de gestão do risco associado às TIC sólido, abrangente e bem documentado, que lhes permita dar resposta ao risco associado às TIC de uma forma rápida, eficiente e abrangente, e assegurar um nível elevado de resiliência operacional digital proporcionado às necessidades, à dimensão e à complexidade das suas atividades.

2. O quadro de gestão do risco associado às TIC a que se refere o n.º 1 deve incluir as estratégias, políticas, procedimentos, protocolos e ferramentas de TIC que sejam necessárias para proteger devida e eficazmente todos os componentes e infraestruturas físicas pertinentes, designadamente equipamento informático e servidores, bem como todas as instalações, centros de dados e áreas consideradas sensíveis, por forma a assegurar que todos estes elementos físicos estão devidamente protegidos contra riscos, nomeadamente em termos de danos e de acesso ou utilização não autorizados.

3. As entidades financeiras devem minimizar o impacto do risco associado às TIC implementando as estratégias, políticas, procedimentos, protocolos e ferramentas adequados, tal como determinado no quadro de gestão do risco associado às TIC. Devem igualmente fornecer informações completas e atualizadas sobre os riscos associados às TIC, tal como exigido pelas autoridades competentes.

4. Como parte do quadro de gestão do risco associado às TIC a que se refere o n.º 1, as entidades financeiras que não sejam microempresas devem implementar um sistema de gestão da segurança das informações baseado em normas internacionais reconhecidas e em conformidade com as orientações de supervisão, que deverão rever periodicamente.

5. As entidades financeiras que não sejam microempresas devem assegurar uma segregação adequada entre as funções de gestão, de controlo e de auditoria interna das TIC, de acordo com o modelo de três linhas de defesa ou com um modelo interno de controlo e gestão do risco.

6. O quadro de gestão do risco associado às TIC a que se refere o n.º 1 deve ser documentado e revisto pelo menos uma vez por ano, bem como quando ocorrerem incidentes graves relacionados com as TIC, de acordo com as instruções ou conclusões de supervisão decorrentes dos processos de auditoria ou dos testes de resiliência operacional digital pertinentes. O quadro deve ser continuamente melhorado com base nas lições retiradas da implementação e monitorização.

7. O quadro de gestão do risco associado às TIC a que se refere o n.º 1 deve ser auditado periodicamente por auditores especializados em TIC que possuam conhecimentos gerais, competências e conhecimentos especializados suficientes sobre o risco associado às TIC. A frequência e a ênfase das auditorias às TIC devem ser consentâneas com os pertinentes riscos associados às TIC.

8. Deve ser estabelecido um processo formal de acompanhamento, incluindo regras para a verificação e correção atempada dos resultados críticos das auditorias às TIC, tendo em conta as conclusões da análise da auditoria e atendendo simultaneamente à natureza, à dimensão e à complexidade dos serviços e das atividades das entidades financeiras.

9. O quadro de gestão do risco associado às TIC a que se refere o n.º 1 deve incluir uma estratégia de resiliência digital que defina a sua forma de implementação. Para o efeito, deve incluir os métodos para dar resposta ao risco e alcançar os objetivos específicos associados às TIC, devendo para tal:

   (a) Explicar de que forma o quadro de gestão do risco associado às TIC apoia a estratégia e os objetivos empresariais da entidade financeira;

   (b) Estabelecer o nível de tolerância ao risco relativo associado às TIC, em conformidade com a apetência para o risco da entidade financeira, assim como analisar a tolerância ao impacto de eventuais perturbações nas TIC;

   (c) Definir objetivos claros em relação à segurança das informações;

   (d) Explicar a arquitetura de referência das TIC e eventuais alterações necessárias para alcançar objetivos empresariais específicos;

   (e) Delinear os diferentes mecanismos criados para detetar, proteger e prevenir os impactos dos incidentes relacionados com as TIC;

   (f) Comprovar o número de incidentes graves relacionados com as TIC comunicados e a eficácia das medidas preventivas;

   (g) Definir uma estratégia holística com múltiplos fornecedores no domínio das TIC ao nível da entidade, mostrando as principais dependências de entidades terceiras prestadoras de serviços no domínio das TIC e explicando a lógica subjacente à contratação de vários prestadores de serviços terceiros;

   (h) Realizar testes à resiliência operacional digital;

   (i) Delinear uma estratégia de comunicação caso ocorram incidentes relacionados com as TIC.

10. Mediante aprovação das autoridades competentes, as entidades financeiras podem delegar as tarefas de verificação do cumprimento dos requisitos de gestão do risco associado às TIC a empresas dentro do grupo ou externas.

Artigo 6.º
Sistemas, protocolos e ferramentas no domínio das TIC

1. As entidades financeiras devem utilizar e manter atualizados sistemas, protocolos e ferramentas no domínio das TIC que satisfaçam as seguintes condições:

   (a) Os sistemas e as ferramentas são adequados à natureza, variedade, complexidade e dimensão das operações que apoiam a realização das suas atividades;

   (b) São fiáveis;

   (c) Têm capacidade suficiente para proceder tratar os dados necessários para a atempada realização das atividades e prestação dos serviços, bem como para lidar com grandes volumes de encomendas, mensagens ou transações, na medida do necessário, nomeadamente em caso de introdução de uma tecnologia nova;

   (d) São tecnologicamente resilientes para lidar adequadamente com necessidades adicionais de tratamento de informações decorrentes de condições de grande tensão no mercado ou noutras situações adversas.

2. Quando utilizam normas técnicas reconhecidas internacionalmente e as melhores práticas do setor em termos de segurança das informações e controlos internos das TIC, as entidades financeiras devem utilizar essas normas e práticas em consonância com qualquer recomendação de supervisão pertinente no que toca à sua integração.

Artigo 7.º
Identificação

1. Como parte do quadro de gestão do risco associado às TIC referido no artigo 5.º, n.º 1, as entidades financeiras devem identificar, classificar e documentar adequadamente todas as funções empresariais relacionadas com as TIC, os ativos de informação que apoiam essas funções e as configurações e interconexões do sistema TIC com outros sistemas TIC internos e externos. As entidades financeiras devem rever na medida do necessário e pelo menos uma vez por ano a adequação da classificação dos ativos de informação e de qualquer documentação pertinente.

2. As entidades financeiras devem identificar numa base contínua todas as fontes de risco associado às TIC, em especial a exposição ao risco associada a outras entidades financeiras e decorrente de outras entidades financeiras, bem como avaliar as ciberameaças e as vulnerabilidades das TIC pertinentes para as suas funções empresariais relacionadas com as TIC e os seus ativos de informação. As entidades financeiras devem rever periodicamente e pelo menos anualmente os cenários de risco que as podem afetar.

3. As entidades financeiras que não sejam microempresas devem efetuar uma avaliação do risco aquando de qualquer grande alteração na infraestrutura das redes e dos sistemas de informação, nos processos ou nos procedimentos que afetem as suas funções, nos processos de apoio ou nos ativos de informação.

4. As entidades financeiras devem identificar todas as contas dos sistemas TIC, nomeadamente as conservadas à distância, os recursos e os equipamentos informáticos e de rede, e devem fazer um levantamento dos equipamentos físicos considerados críticos. Devem igualmente descrever a configuração dos ativos TIC e das ligações e interdependências entre os diferentes ativos TIC.

5. As entidades financeiras devem identificar e documentar todos os processos que dependem de entidades terceiras prestadoras de serviços no domínio das TIC e devem identificar as interconexões com as entidades terceiras prestadoras de serviços no domínio das TIC.

6. Para efeitos dos n.os 1, 4 e 5, as entidades financeiras devem elaborar e atualizar periodicamente os inventários relevantes.

7. As entidades financeiras que não sejam microempresas devem realizar periodicamente e pelo menos uma vez por ano uma avaliação de risco específica no domínio das TIC a todos os sistemas TIC pré-existentes, em especial antes e depois de conectarem tecnologias, aplicações ou sistemas antigos e novos.

Artigo 8.º

Proteção e prevenção

1. Com o intuito de proteger adequadamente os sistemas TIC e de organizar medidas de resposta, as entidades financeiras devem monitorizar e controlar continuamente o funcionamento dos sistemas e das ferramentas TIC e minimizar o impacto desses riscos através da implementação das ferramentas, das políticas e dos procedimentos de segurança adequados no domínio das TIC.

2. As entidades financeiras devem conceber, adquirir e executar estratégias, políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC que visem, em especial, assegurar a resiliência, a continuidade e a disponibilidade dos sistemas TIC e manter elevados níveis de segurança, confidencialidade e integridade dos dados, quer estejam guardados, a ser utilizados ou em trânsito.

3. Para alcançar os objetivos referidos no n.º 2, as entidades financeiras devem utilizar tecnologia e processos de vanguarda no domínio das TIC que permitam:

   (a) Garantir a segurança dos meios de transferência de informações;

   (b) Minimizar o risco de corrupção ou perda de dados, acesso não autorizado e falhas técnicas que possam prejudicar a atividade empresarial;

   (c) Prevenir fugas de informação;

   (d) Assegurar que os dados estão protegidos contra riscos relacionados com má administração ou tratamento incorreto, nomeadamente uma conservação inadequada dos registos.

4. Como parte do quadro de gestão do risco associado às TIC referido no artigo 5.º, n.º 1, as entidades financeiras devem:

   (a) Desenvolver e documentar uma política de segurança das informações que defina regras para proteger a confidencialidade, a integridade e a disponibilidade dos seus recursos TIC, dados e ativos em formato informático, bem como os dos seus clientes;

(b) De acordo com uma abordagem baseada no risco, estabelecer uma gestão sólida das redes e infraestruturas utilizando técnicas, métodos e protocolos adequados, nomeadamente a implementação de mecanismos automatizados para isolar os ativos informáticos afetados em caso de ciberataque;

(c) Executar políticas que limitem o acesso físico e virtual aos recursos e aos dados dos sistemas TIC àquilo que é estritamente necessário para funções e atividades legítimas e aprovadas e, para o efeito, estabelecer um conjunto de políticas, procedimentos e controlos centrado nos direitos de acesso e na boa administração dos mesmos;

(d) Executar políticas e protocolos que garantam mecanismos de autenticação robustos, com base nas normas pertinentes e em sistemas de controlos dedicados com vista a prevenir o acesso às chaves criptográficas por meio das quais os dados são encriptados com base nos resultados de processos aprovados de classificação dos dados e de avaliação do risco;

(e) Executar políticas, procedimentos e controlos relativos à gestão das alterações das TIC, nomeadamente mudanças de programas informáticos, equipamentos informáticos, componentes de *firmware*, alterações do próprio sistema ou de segurança, com base numa abordagem de avaliação do risco e como parte integrante do processo global de gestão de alterações da entidade financeira, por forma a assegurar que todas as alterações dos sistemas TIC são registadas, testadas, avaliadas, aprovadas, executadas e verificadas de forma controlada;

(f) Dispor de políticas adequadas e abrangentes para correções e atualizações.

Para efeitos da alínea b), as entidades financeiras devem conceber a infraestrutura de conexão das redes de forma a que essas conexões possam ser instantaneamente cortadas e deve assegurar a sua compartimentação e segmentação, com vista a minimizar e prevenir o contágio, em especial em processos financeiros interligados.

Para efeitos da alínea e), o processo de gestão de alteração das TIC deve ser aprovado pelas chefias adequadas e deve ter protocolos específicos ativos para alterações de emergência.

Artigo 9.º
Deteção

1. As entidades financeiras devem dispor de mecanismos que detetem rapidamente atividades anómalas em conformidade com o artigo 15.º, nomeadamente questões relacionadas com o desempenho das redes e incidentes relacionados com as TIC, identificando todas as potenciais falhas pontuais significativas.

   Todos os mecanismos de deteção referidos no primeiro parágrafo devem ser testados periodicamente em conformidade com o artigo 22.º.

2. Os mecanismos de deteção referidos no n.º 1 devem permitir que o controlo se faça em etapas múltiplas, definir limiares de alerta e critérios que despoletem a deteção de incidentes relacionados com as TIC e os processos de resposta aos mesmos e incluir mecanismos automáticos de alerta para o pessoal competente responsável pela resposta aos incidentes relacionados com as TIC.

3. As entidades financeiras devem canalizar os recursos e as capacidades suficientes, dando a devida consideração à sua dimensão, à sua atividade e aos seus perfis de risco, para monitorizar a atividade dos utilizadores e a ocorrência de anomalias e incidentes relacionados com as TIC, em especial ciberataques.

4. As entidades financeiras referidas no artigo 2.º, n.º 1, alínea l), devem também dispor de sistemas que permitam verificar de forma eficaz as comunicações de transações, identificar as omissões e os erros manifestos e solicitar a retransmissão de quaisquer comunicações erróneas.

Artigo 10.º

Resposta e recuperação

1. Como parte do quadro de gestão do risco associado às TIC referido no artigo 5.º, n.º 1, e com base nos requisitos de identificação definidos no artigo 7.º, a política de continuidade da atividade operacional de uma entidade financeira deve incluir uma política específica de continuidade das atividades no domínio das TIC.

2. As entidades financeiras devem aplicar a política de continuidade das atividades no domínio das TIC referida no n.º 1 através de medidas, planos, procedimentos e mecanismos dedicados, adequados e documentados que visem:

   (a) Registar todos os incidentes relacionados com as TIC;

   (b) Assegurar a continuidade das funções críticas da entidade financeira;

   (c) Dar uma resposta rápida, adequada e eficaz e solucionar todos os incidentes relacionados com as TIC, em especial mas não apenas no contexto de ciberataques, de forma a limitar os danos e a dar prioridade ao relançamento das atividades e às ações de recuperação;

   (d) Ativar sem demora os planos específicos que permitem pôr em prática as medidas, os processos e as tecnologias de contenção adequadas a cada tipo de incidente relacionados com as TIC, prevenindo assim danos mais extensos, bem como uma resposta adequada e os procedimentos de recuperação estabelecidos em conformidade com o artigo 11.º;

   (e) Estimar preliminarmente os impactos, os danos e as perdas;

   (f) Definir ações de comunicação e gestão de crises que assegurem a transmissão de informações atualizadas a todo o pessoal interno competente e a todas as partes interessadas externas pertinentes em conformidade com o artigo 13.º, bem como a sua comunicação às autoridades competentes em conformidade com o artigo 17.º.

3. Como parte do quadro de gestão do risco associado às TIC referido no artigo 5.º, n.º 1, as entidades financeiras devem executar um plano de recuperação em caso de catástrofe associada às TIC que, no caso das entidades financeiras que não sejam microempresas, deve estar sujeito a auditorias independentes.

4. As entidades financeiras devem dispor, manter e testar periodicamente planos de continuidade das atividades no domínio das TIC, designadamente em relação a funções críticas ou importantes externalizadas ou subcontratadas através de acordos com entidades terceiras prestadoras de serviços no domínio das TIC.

5. Como parte da sua gestão abrangente do risco associado às TIC, as entidades financeiras devem:

   (a) Testar a política de continuidade das atividades no domínio das TIC e o plano de recuperação em caso de catástrofe associada às TIC, no mínimo uma vez por ano e após alterações substanciais dos sistemas de TIC;

(b) Testar os planos de comunicação de crises estabelecidos em conformidade com o artigo 13.º.

Para efeitos da alínea a), as entidades financeiras que não sejam microempresas devem incluir nos planos de testagem cenários de ciberataques e de transferência entre a infraestrutura primária de TIC e a capacidade redundante, cópias de segurança e instalações redundantes necessárias ao cumprimento das obrigações definidas no artigo 11.º.

As entidades financeiras devem rever periodicamente a sua política de continuidade das atividades no domínio das TIC e o plano de recuperação em caso de catástrofe associada às TIC tendo em conta os resultados dos testes realizados em conformidade com o primeiro parágrafo e as recomendações decorrentes das auditorias ou das revisões de supervisão.

6. As entidades financeiras que não sejam microempresas devem ter uma função de gestão de crises que, em caso de ativação da sua política de continuidade das atividades no domínio das TIC ou do seu plano de recuperação em caso de catástrofe associada às TIC, estipule claramente os procedimentos para gerir as comunicações internas e externas em caso de crise em conformidade com o artigo 13.º.

7. As entidades financeiras devem manter registos das suas atividades antes e durante a ocorrência de perturbações aquando da ativação da sua política de continuidade das atividades no domínio das TIC ou do seu plano de recuperação em caso de catástrofe associada às TIC. Os registos devem estar prontamente disponíveis.

8. As entidades financeiras referidas no artigo 2.º, n.º 1, alínea f), devem facultar às autoridades competentes cópias dos resultados dos testes de continuidade das atividades no domínio das TIC ou exercícios similares realizados durante o período em análise.

9. As entidades financeiras que não sejam microempresas devem comunicar às autoridades competentes todos os custos e todas as perdas causados por perturbações nas TIC e incidentes relacionados com as TIC.

Artigo 11.º

Políticas de cópias de segurança e métodos de recuperação

1. Com o intuito de assegurar a restauração dos sistemas TIC no menor tempo possível e limitando as perturbações, as entidades financeiras devem desenvolver, como parte do seu quadro de gestão do risco associado às TIC:

   (a) Uma política de cópias de segurança que especifique o âmbito dos dados abrangidos e a frequência mínima com que as cópias de segurança são feitas, com base na natureza crítica das informações ou na sensibilidade dos dados;

   (b) Métodos de recuperação.

2. Os sistemas de cópias de segurança devem entrar em funcionamento sem demora, exceto se tal puser em perigo a segurança das redes e dos sistemas de informação ou a integridade ou confidencialidade dos dados.

3. Quando restauram dados das cópias de segurança utilizando sistemas próprios, as entidades financeiras devem utilizar sistemas TIC com um ambiente operativo diferente do sistema principal, que não estejam diretamente ligados a este último e

que estejam devidamente protegidos contra qualquer acesso não autorizado ou corrupção ao nível das TIC.

Em relação às entidades financeiras referidas no artigo 2.º, n.º 1, alínea g), os planos de recuperação devem permitir a recuperação de todas as transações em curso no momento da perturbação, para permitir que a contraparte central continue a funcionar de forma fiável e conclua as liquidações nas datas previstas.

4. As entidades financeiras devem manter capacidades de TIC redundantes equipadas com recursos, capacidade e funcionalidades suficientes e adequados para garantir as necessidades operacionais.

5. As entidades financeiras referidas no artigo 2.º, n.º 1, alínea f), devem manter ou assegurar que as suas entidades terceiras prestadoras de serviços no domínio das TIC mantenham pelo menos um local de tratamento de dados secundário, dotado de recursos, capacidades, funcionalidades e disposições em matéria de pessoal suficientes e adequados para satisfazer as necessidades operacionais.

   O local de tratamento de dados secundário deve:

   (a) Estar localizado a um distância geográfica do local de tratamento de dados principal que garanta que esse local tem um perfil de risco distinto e que o impeça de ser afetado pela ocorrência que afetou o local principal;

   (b) Ser capaz de assegurar a continuidade dos serviços críticos de forma idêntica ao local principal ou fornecendo o nível de serviços necessário para assegurar que a entidade financeira realiza as suas operações críticas dentro dos objetivos de recuperação;

   (c) Estar imediatamente acessível ao pessoal da entidade financeira por forma a assegurar a continuidade dos serviços críticos caso o local de tratamento de dados primário passe a estar indisponível.

6. Ao determinar o tempo de recuperação e os objetivos concretos de cada função, as entidades financeiras devem ter em conta o potencial impacto global na eficiência do mercado. Os referidos objetivos temporais devem garantir que, em cenários extremos, os níveis de serviço acordados são cumpridos.

7. Aquando da recuperação de um incidente relacionado com as TIC, as entidades financeiras devem realizar múltiplas verificações, nomeadamente conciliações de dados, por forma a garantir que o mais alto nível de integridade desses mesmos dados. Estas verificações também devem ser realizadas aquando da reconstrução de dados de partes interessadas externas, por forma a assegurar a coerência de todos os dados nos diferentes sistemas.

Artigo 12.º
Aprendizagem e evolução

1. As entidades financeiras devem dispor de capacidades e de pessoal adequados à sua dimensão, à sua atividade e aos seus perfis de risco para recolherem informações sobre as vulnerabilidades informáticas e as ciberameaças, os incidentes relacionados com as TIC, em especial ciberataques, e analisarem os impactos prováveis dos mesmos na sua resiliência operacional digital.

2. As entidades financeiras devem realizar exames pós-incidentes relacionados com as TIC quando ocorrerem perturbações significativas das TIC que afetem as suas

atividades principais, analisando as causas das perturbações e identificando as melhorias que deverão introduzir ao nível do funcionamento das TIC ou da política de continuidade das atividades no domínio das TIC referida no artigo 10.º.

Aquando da implementação de alterações, as entidades financeiras que não sejam microempresas devem comunicar essas alterações às autoridades competentes.

Os exames pós-incidentes relacionados com as TIC referidos no primeiro parágrafo devem determinar se os procedimentos estabelecidos foram seguidos e se as medidas adotadas foram eficazes, nomeadamente em relação à:

(a) Prontidão da resposta aos alertas de segurança e da determinação do impacto dos incidentes relacionados com as TIC e da sua gravidade;

(b) Qualidade e celeridade da realização da análise forense;

(c) Eficácia da propagação da reação ao incidente dentro da entidade financeira;

(d) Eficácia da comunicação interna e externa.

3. Os ensinamentos retirados dos testes da resiliência operacional digital realizados em conformidade com os artigos 23.º e 24.º e a partir de incidentes reais relacionados com as TIC, em especial de ciberataques, juntamente com os desafios enfrentados aquando da ativação dos planos de recuperação e continuidade das atividades, juntamente com as informações relevantes trocadas com as contrapartes e avaliadas durante os exames de supervisão, devem ser devidamente incorporados numa base contínua no processo de avaliação do risco associado às TIC. Estes resultados devem traduzir-se em exames adequados dos componentes relevantes do quadro de gestão do risco associado às TIC referido no artigo 5.º, n.º 1.

4. As entidades financeiras devem monitorizar a eficácia da execução da sua estratégia de resiliência digital estipulada no artigo 5.º, n.º 9. Devem também fazer um levantamento da evolução dos riscos associados às TIC ao longo do tempo, analisar a frequência, os tipos, a dimensão e a evolução dos incidentes relacionados com as TIC, em especial os ciberataques e respetivos padrões, com vista a compreender o nível de exposição ao risco associado às TIC e melhorar a maturidade cibernética e o grau de preparação da entidade financeira.

5. Os quadros superiores ligados às TIC devem, no mínimo uma vez por ano, comunicar informações ao órgão de gestão sobre os resultados referidos no n.º 3 e fazer recomendações.

6. As entidades financeiras devem desenvolver programas de sensibilização no domínio da segurança das TIC e formações em matéria de resiliência operacional digital como módulos obrigatórios nos planos de formação do seu pessoal. Estes devem ser aplicáveis a todos os trabalhadores e aos quadros superiores.

As entidades financeiras devem monitorizar continuamente os desenvolvimentos tecnológicos mais importantes, também com vista a compreender os possíveis impactos da implantação dessas novas tecnologias nos requisitos de segurança no domínio das TIC e na resiliência operacional digital. Devem manter-se a par dos mais recentes processos de gestão do risco associado às TIC, combatendo eficazmente os ciberataques nas suas formas atuais ou futuras.

Artigo 13.º

Comunicação

1. Como parte do quadro de gestão do risco associado às TIC referido no artigo 5.º, n.º 1, as entidades financeiras devem dispor de planos de comunicação que permitam divulgar de forma responsável os incidentes relacionados com as TIC ou as principais vulnerabilidade aos clientes e às contrapartes, bem como ao público, se for caso disso.

2. Como parte do quadro de gestão do risco associado às TIC referido no artigo 5.º, n.º 1, as entidades financeiras devem executar políticas de comunicação destinadas ao seu pessoal e às partes interessadas externas. As políticas de comunicação destinadas ao pessoal devem ter em conta a necessidade de diferenciar entre o pessoal envolvido na gestão de risco associado às TIC, em especial em matéria de resposta e recuperação, e o pessoal que necessita de ser informado.

3. Pelo menos uma pessoa deve ser responsável na entidade pela execução da estratégia de comunicação em caso de incidentes relacionados com as TIC e desempenhar o papel de porta-voz para o público e os meios de comunicação social para o efeito.

Artigo 14.º

Maior harmonização das ferramentas, dos métodos, dos processos e das políticas de gestão do risco associado às TIC

A Autoridade Bancária Europeia (EBA), a Autoridade Europeia dos Valores Mobiliários e dos Mercados (ESMA) e a Autoridade Europeia dos Seguros e Pensões Complementares de Reforma (EIOPA) devem, em consulta com a Agência da União Europeia para a Cibersegurança (ENISA), desenvolver projetos de normas técnicas de regulamentação para os seguintes efeitos:

(a) Especificar mais pormenorizadamente os elementos a incluir nas políticas, nos procedimentos, nos protocolos e nas ferramentas relacionadas com a segurança das TIC referidos no artigo 8.º, n.º 2, com vista a assegurar a segurança das redes, prever salvaguardas adequadas contra as intrusões e a utilização abusiva dos dados, preservar a autenticidade e a integridade dos dados, nomeadamente por via de técnicas criptográficas, e garantir uma transmissão fiável e rápida dos dados sem grandes interrupções;

(b) Determinar de que forma as políticas, os procedimentos e as ferramentas relacionadas com a segurança das TIC referidos no artigo 8.º, n.º 2, devem incorporar controlos de segurança nos sistemas desde a respetiva conceção (segurança desde a conceção), permitindo ajustamentos em função do contexto envolvente em termos de ameaças, e prever a utilização de tecnologias de «defesa em profundidade»;

(c) Especificar mais pormenorizadamente as técnicas, os métodos e os protocolos adequados referidos no artigo 8.º, n.º 4, alínea b);

(d) Desenvolver mais pormenorizadamente os componentes de controlo da gestão dos direitos de acessos referidos no artigo 8.º, n.º 4, alínea c), e a política de recursos humanos associada, especificando os direitos de acesso, os procedimentos para conceder e revogar esses direitos e a monitorização de comportamentos anómalos em relação com os riscos associados às TIC através dos indicadores adequados, nomeadamente os padrões de utilização das redes, as horas de acesso, a atividade informática e os dispositivos desconhecidos;

(e) Desenvolver mais pormenorizadamente os elementos especificados no artigo 9.º, n.º 1, que permitem uma deteção rápida de atividades anómalas, e os critérios referidos no artigo 9.º, n.º 2, que despoletam processos de deteção e resposta a incidentes relacionados com as TIC;

(f) Especificar mais pormenorizadamente os componentes da política de continuidade das atividades no domínio das TIC referida no artigo 10.º, n.º 1;

(g) Especificar mais pormenorizadamente a testagem dos planos de continuidade das atividades no domínio das TIC referidos no artigo 10.º, n.º 5, por forma a assegurar que esses planos têm devidamente em conta cenários em que a qualidade do desempenho de uma função crítica ou importante se deteriora a um nível inaceitável ou falha, e considerar devidamente o potencial impacto de uma insolvência ou de outras falhas de qualquer entidade terceira prestadora de serviços relevante no domínio das TIC e, quando pertinente, os riscos políticos nas respetivas jurisdições desses prestadores;

(h) Especificar mais pormenorizadamente os componentes do plano de recuperação em caso de catástrofe associada às TIC referido no artigo 10.º, n.º 3.

A EBA, a ESMA e a EIOPA devem apresentar à Comissão esses projetos de normas técnicas de regulamentação até [*Serviço das Publicações: inserir a data correspondente a um ano após a data de entrada em vigor*].

A Comissão fica habilitada a adotar as normas técnicas de regulamentação a que se refere o primeiro parágrafo nos termos dos artigos 10.º a 14.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, respetivamente.

CAPÍTULO III

INCIDENTES RELACIONADOS COM AS TIC

GESTÃO, CLASSIFICAÇÃO E COMUNICAÇÃO DE INFORMAÇÕES

Artigo 15.º

Processo de gestão de incidentes relacionados com as TIC

1. As entidades financeiras devem estabelecer e aplicar um processo de gestão de incidentes relacionados com as TIC que permita detetar, gerir e notificar esses mesmos incidentes e implementar alertas a partir de indicadores de alerta precoce.

2. As entidades financeiras devem estabelecer processos adequados para assegurar uma monitorização, um tratamento e um acompanhamento consistente e integrado dos incidentes relacionados com as TIC, por forma a garantir que as causas profundas são identificadas e erradicadas com vista a prevenir a sua ocorrência.

3. O processo de gestão de incidentes relacionados com as TIC a que se refere o n.º 1 deve:

(a) Estabelecer procedimentos para identificar, rastrear, registar, categorizar e classificar os incidentes relacionados com as TIC de acordo com a sua

prioridade e a gravidade e importância dos serviços afetados, em conformidade com os critérios referidos no artigo 16.º, n.º 1;

(b) Atribuir as funções e responsabilidades que será necessário ativar para os diferentes cenários e tipos de incidentes relacionados com as TIC;

(c) Definir planos de comunicação ao pessoal, às partes interessadas externas e aos meios de comunicação social em conformidade com o artigo 13.º, planos de notificação aos clientes, procedimentos internos em caso de agravamento da situação, nomeadamente perante queixas de clientes relacionadas com as TIC, bem como planos para o fornecimento de informações às entidades financeiras que atuam na qualidade de contrapartes, se for caso disso;

(d) Assegurar que os incidentes graves relacionados com as TIC são comunicados aos quadros superiores pertinentes e informar o órgão de gestão dos incidentes graves relacionados com as TIC, explicando o impacto, a resposta e os controlos adicionais que devem ser estabelecidos em resultado dos incidentes relacionados com as TIC;

(e) Estabelecer procedimentos de resposta a incidentes relacionados com as TIC para atenuar os respetivos impactos e assegurar que os serviços recomeçam a funcionar atempadamente e de forma segura.

Artigo 16.º

Classificação dos incidentes relacionados com as TIC

1. As entidades financeiras devem classificar os incidentes relacionados com as TIC e devem determinar o seu impacto com base nos seguintes critérios:

(a) O número de utilizadores ou contrapartes financeiras afetadas pela perturbação causada pelo incidente relacionado com as TIC e se o incidente relacionado com as TIC teve algum impacto em termos de reputação;

(b) A duração do incidente relacionado com as TIC, nomeadamente o tempo de inatividade do serviço;

(c) A distribuição geográfica relativamente às áreas afetadas pelo incidente relacionado com as TIC, em particular quando tiver afetado mais do que dois Estados-Membros;

(d) As perdas de dados decorrentes do incidente relacionado com as TIC, nomeadamente em termos de integridade, de confidencialidade ou de disponibilidade;

(e) A gravidade do impacto do incidente relacionado com as TIC nos sistemas TIC da entidade financeira;

(f) Até que ponto os serviços afetados, nomeadamente as transações e operações da entidade financeira, são críticos;

(g) O impacto económico do incidente relacionado com as TIC, tanto em termos absolutos como em termos relativos.

2. As AES devem, através do seu Comité Conjunto («Comité Conjunto») e após consulta do Banco Central Europeu (BCE) e a ENISA, desenvolver projetos de normas técnicas de regulamentação comuns, por forma a especificar melhor:

(a) Os critérios definidos no n.º 1, nomeadamente os limiares de materialidade para determinar os incidentes graves relacionados com as TIC que estão sujeitos à obrigação de comunicação de informações prevista no artigo 17.º, n.º 1;

(b) Os critérios a aplicar pelas autoridades competentes com o objetivo de avaliar a relevância dos incidentes graves relacionados com as TIC para as jurisdições de outros Estados-Membros, bem como os pormenores dos relatórios dos incidentes relacionados com as TIC que devem ser partilhados com outras autoridades competentes nos termos do artigo 17.º, n.os 5 e 6.

3. Aquando da elaboração dos projetos de normas técnicas de regulamentação comuns referidos no n.º 2, as AES devem tomar em conta as normas internacionais, bem como as especificações elaboradas e publicadas pela ENISA, incluindo, quando adequado, especificações para outros setores económicos.

As AES devem apresentar esses projetos de normas técnicas de regulamentação comuns à Comissão até [*Serviço das Publicações: inserir a data correspondente a um ano após a data de entrada em vigor*].

A Comissão fica habilitada a completar o presente regulamento através da adoção das normas técnicas de regulamentação a que se refere o n.º 2, nos termos dos artigos 10.º a 14.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010.

Artigo 17.º

Comunicação dos incidentes relacionados com as TIC

1. As entidades financeiras devem comunicar os incidentes graves relacionados com as TIC à autoridade competente pertinente, tal como referido no artigo 41.º, nos prazos definidos no n.º 3.

Para efeitos do primeiro parágrafo, as entidades financeiras devem elaborar, após recolha e análise de todas as informações relevantes, um relatório de incidentes utilizando o modelo referido no artigo 18.º e apresentá-lo à autoridade competente.

O relatório deve incluir todas as informações necessárias para que a autoridade competente determine o grau de importância do incidente grave relacionado com as TIC e avalie os seus possíveis impactos transfronteiriços.

2. Quando um incidente grave relacionado com as TIC tenha ou possa vir a ter impacto nos interesses financeiros dos utilizadores e clientes do serviço, as entidades financeiras devem, sem demora indevida, informar os utilizadores e clientes dos seus serviços acerca do incidente grave relacionado com as TIC e, o mais rapidamente possível, de todas as medidas que foram tomadas para atenuar os efeitos adversos desse incidente.

3. As entidades financeiras devem apresentar à autoridade competente, tal como referido no artigo 41.º:

(a) Uma notificação inicial, sem demora e o mais tardar no final do dia útil, ou, caso se trate de um incidente grave relacionado com as TIC ocorrido quando faltarem menos de duas horas para o final do dia útil, o mais tardar quatro horas a contar do início do dia útil seguinte, ou, caso não estejam disponíveis os canais de comunicação de informações, logo que estes estejam disponíveis;

(b) Um relatório intercalar, o mais tardar uma semana após a notificação inicial referida na alínea a), seguido, se for caso disso, de notificações atualizadas sempre que fique disponível uma atualização relevante da situação, bem como mediante pedido específico da autoridade competente;

(c) Um relatório final, quando concluída a análise das causas subjacentes, independentemente de já terem sido aplicadas ou não medidas de atenuação, e quando os valores reais do impacto estejam disponíveis para substituir as estimativas, mas o mais tardar um mês a contar do momento em que foi enviado o relatório inicial.

4. As entidades financeiras só podem delegar as obrigações de comunicação de informações previstas no presente artigo a uma entidade terceira prestadora de serviços mediante a aprovação dessa delegação pela autoridade competente pertinente referida no artigo 41.º.

5. Aquando da receção do relatório referido no n.º 1, a autoridade competente deve, sem demora indevida, fornecer pormenores sobre o incidente:

(a) À EBA, à ESMA ou à EIOPA, se for caso disso;

(b) Ao BCE, se for caso disso, no caso das entidades financeiras referidas no artigo 2.º, n.º 1, alíneas a), b) e c); e

(c) Ao ponto de contacto único designado nos termos do artigo 8.º da Diretiva (UE) 2016/1148.

6. A EBA, a ESMA ou a EIOPA e o BCE devem avaliar a relevância do incidente grave relacionado com as TIC para outras autoridades públicas pertinentes e devem notificá-las em conformidade o mais rapidamente possível. O BCE deve notificar os membros do Sistema Europeu de Bancos Centrais das questões relevantes para o sistema de pagamentos. Com base nessa notificação as autoridades competentes devem, se for caso disso, tomar todas as medidas necessárias para proteger a estabilidade imediata do sistema financeiro.

Artigo 18.º

Harmonização do conteúdo a comunicar e dos modelos

1. As AES, através do Comité Conjunto e após consulta da ENISA e do BCE, devem elaborar:

(a) Projetos de normas técnicas de regulamentação comuns com vista a:

(1) estabelecer o conteúdo da comunicação de informações sobre os incidentes graves relacionados com as TIC,

(2) especificar mais pormenorizadamente as condições em que as entidades financeiras podem delegar a uma entidade terceira prestadora de serviços, mediante aprovação prévia da autoridade competente, as obrigações de comunicação de informações definidas no presente capítulo;

(b) Projetos de normas técnicas de execução comuns com vista a estabelecer os formulários, os modelos e os procedimentos normalizados para as entidades financeiras comunicarem um incidente relacionado com as TIC.

As AES devem apresentar os projetos de normas técnicas de regulamentação comuns referidos no n.º 1, alínea a), e os projetos de normas técnicas de execução referidos

no n.º 1, alínea b), à Comissão até xx 202x [*Serviço das Publicações: inserir a data correspondente a um ano após a data de entrada em vigor*].

A Comissão fica habilitada a complementar o presente regulamento através da adoção das normas técnicas de regulamentação comuns a que se refere o n.º 1, alínea a), nos termos dos artigos 10.º a 14.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1095/2010 e (UE) n.º 1094/2010, respetivamente.

São conferidos à Comissão poderes para adotar as normas técnicas de execução comuns a que se refere o n.º 1, alínea b), nos termos do artigo 15.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1095/2010 e (UE) n.º 1094/2010, respetivamente.

Artigo 19.º

Centralização da comunicação de incidentes graves relacionados com as TIC

1. As AES devem preparar, através do Comité Conjunto e em consulta com o BCE e a ENISA, um relatório conjunto que avalie a viabilidade de aumentar a centralização da comunicação de incidentes através da criação de uma plataforma única na UE (a seguir designada por «plataforma») para a comunicação de incidentes graves relacionados com as TIC pela entidades financeiras. O relatório deve explorar formas de facilitar o fluxo de comunicação de incidentes relacionados com as TIC, reduzir os custos associados e sustentar análises temáticas com vista a melhorar a convergência em termos de supervisão.

2. O relatório referido no n.º 1 deve incluir no mínimo os seguintes elementos:

   (a) Pré-requisitos para a criação da referida plataforma;

   (b) Benefícios, limitações e possíveis riscos;

   (c) Elementos de gestão operacional;

   (d) Condições de participação;

   (e) Modalidades de acesso à plataforma pelas entidades financeiras e pelas autoridades nacionais competentes;

   (f) Uma avaliação preliminar dos custos financeiros inerentes à criação da estrutura operacional que servirá de base à plataforma, incluindo nomeadamente os necessários conhecimentos especializados.

3. As AES devem apresentar o relatório referido no n.º 1 à Comissão, ao Parlamento Europeu e ao Conselho até xx de 202x [*Serviço das Publicações: inserir a data correspondente a três anos após a data de entrada em vigor*].

Artigo 20.º

Observações em termos de supervisão

1. Aquando da receção de um relatório referido no artigo 17.º, n.º 1, a autoridade competente deve acusar a receção da notificação e enviar o mais rapidamente possível todas as observações ou orientações necessárias à entidade financeira, em especial para discussão das correções ao nível da entidade ou das formas de minimizar os impactos adversos nos diversos setores.

2. As AES, através do Comité Conjunto, devem comunicar anualmente informações, numa base anónima e agregada, sobre as notificações dos incidentes relacionados

com as TIC recebidas das autoridades competentes, indicando no mínimo o número de incidentes graves relacionados com as TIC, a sua natureza, o impacto nas operações das entidades financeiras ou nos clientes, os custos e as medidas corretivas adotadas.

As AES devem emitir alertas e produzir estatísticas de elevada qualidade para apoiar as avaliações das ameaças e das vulnerabilidades no domínio das TIC.

CAPÍTULO IV

Realização de testes da resiliência operacional digital

Artigo 21.º

Requisitos gerais para a realização de testes da resiliência operacional digital

1. Com o intuito de avaliar a preparação para os incidentes relacionados com as TIC, identificar pontos fracos, deficiências ou lacunas na resiliência operacional digital e adotar rapidamente medidas corretivas, as entidades financeiras devem estabelecer, manter e rever, atendendo devidamente à sua dimensão, atividades e perfil de risco, um programa sólido e abrangente de realização de testes da resiliência operacional digital como parte integrante do quadro de gestão de risco associado às TIC referido no artigo 5.º.

2. O programa de realização de testes da resiliência operacional digital deve incluir um leque de avaliações, testes, metodologias, práticas e ferramentas a aplicar em conformidade com as disposições dos artigos 22.º e 23.º.

3. As entidades financeiras devem adotar uma abordagem baseada no risco aquando da execução do programa de realização de testes da resiliência operacional digital referido no n.º 1, tendo em conta a evolução contextual dos riscos associados às TIC, quaisquer riscos específicos a que a entidade esteja ou possa vir a estar exposta, o grau de importância dos ativos de informação e dos serviços prestados, bem como qualquer outro fator que a entidade financeira considere adequado.

4. As entidades financeiras devem assegurar que os testes são realizados por partes independentes, sejam elas internas ou externas.

5. As entidades financeiras devem estabelecer procedimentos e políticas para dar prioridade, classificar e corrigir todas as questões surgidas aquando da realização dos testes e devem estabelecer metodologias internas de validação para garantir que é dada uma resposta a todos os pontos fracos, deficiências ou lacunas.

6. As entidades financeiras devem testar pelo menos anualmente todos os sistemas e aplicações críticos no domínio das TIC.

Artigo 22.º

Testar os sistemas e as ferramentas no domínio das TIC

1. O programa de testes da resiliência operacional digital referido no artigo 21.º deve prever a execução de um conjunto completo de testes apropriados, nomeadamente avaliações e análises das vulnerabilidades, análises de fonte aberta, avaliações da segurança das redes, análises das lacunas, da segurança física, questionários e

soluções para averiguar os programas informáticos, revisões do código fonte quando tal for exequível, testes baseados em cenários, testes de compatibilidade, testes de desempenho, testes de extremo a extremo ou testes de penetração.

2. As entidades financeiras referidas no artigo 2.º, n.º 1, alíneas f) e g), devem realizar avaliações das vulnerabilidades antes de lançarem ou relançarem serviços novos ou existentes de apoio às funções críticas, às aplicações e aos componentes da infraestrutura da entidade financeira.

Artigo 23.º

Realização de testes avançados às ferramentas, aos sistemas e aos processos relacionados com as TIC com base nos testes de penetração motivados por ameaças

1. As entidades financeiras identificadas em conformidade com o n.º 4 devem realizar, pelo menos de três em três anos, testes avançados através da realização de testes de penetração motivados por ameaças.

2. Os testes de penetração motivados por ameaças devem abranger pelo menos as funções e os serviços críticos de uma entidade financeira e devem ser realizados em sistemas de produção ativos que apoiem essas funções. O âmbito exato dos testes de penetração motivados por ameaças, baseado na avaliação das funções e dos serviços críticos, deve ser determinado pelas entidades financeiras e validado pelas autoridades competentes.

   Para efeitos do primeiro parágrafo, as entidades financeiras deve identificar todos os processos, sistemas e tecnologias relacionados com as TIC que sejam relevantes e estejam subjacentes às funções e aos serviços críticos, nomeadamente funções e serviços externalizados ou subcontratados a entidades terceiras prestadoras de serviços no domínio das TIC.

   Quando as entidades terceiras prestadoras de serviços no domínio das TIC estiverem incluídas na esfera dos testes de penetração motivados por ameaças, a entidade financeira deve tomar as medidas necessárias para assegurar a participação desses prestadores de serviços.

   As entidades financeiras devem aplicar controlos eficazes de gestão do risco para reduzir os riscos de quaisquer potenciais impactos nos dados, danos nos ativos e perturbações nos serviços ou nas operações críticas da própria entidade financeira, das suas contrapartes ou do setor financeiro.

   No final do teste, depois de chegarem a acordo sobre os relatórios e os planos corretivos, a entidade financeira e os responsáveis externos pela realização dos testes devem fornecer à autoridade competente a documentação que confirma que os testes de penetração motivados por ameaças foram realizados em conformidade com os requisitos. As autoridades competentes devem validar a documentação e emitir um comprovativo.

3. As entidades financeiras devem contratar responsáveis externos pela realização dos testes em conformidade com o artigo 24.º para efeitos da realização dos testes de penetração motivados por ameaças.

   As autoridades competentes devem identificar as entidades financeiras que devem realizar os testes de penetração motivados por ameaças de uma forma que seja proporcional à dimensão, à escala, à atividade e ao perfil de risco global da entidade financeira, com base na avaliação dos seguintes elementos:

(a) Fatores relacionados com o impacto, em especial o grau de importância dos serviços prestados e das atividades desenvolvidas pela entidade financeira;

(b) Possíveis preocupações com a estabilidade financeira, nomeadamente o caráter sistémico da entidade financeiras a nível nacional ou da União, se for caso disso;

(c) Perfil específico de risco associado às TIC, nível de maturidade da entidade financeira em relação às TIC ou às questões tecnológicas envolvidas.

4. A EBA, a ESMA e a EIOPA devem, após consulta do BCE e tendo em conta os quadros pertinentes na União aplicáveis aos testes de penetração baseados em informações confidenciais, desenvolver projetos de normas técnicas de regulamentação que especifiquem mais pormenorizadamente:

(a) Os critérios utilizados para fins de aplicação do n.º 6 do presente artigo;

(b) Os requisitos relativos:

(a) ao âmbito da realização dos testes de penetração motivados por ameaças referidos no n.º 2 do presente artigo,

(b) à metodologia da realização dos testes e à abordagem a seguir em cada fase especifica do processo,

(c) aos resultados e às fases de conclusão e de correção na sequência da realização dos testes;

(c) O tipo de cooperação em matéria de supervisão necessária para a realização dos testes de penetração motivados por ameaças no contexto das entidades financeiras que operam em mais do que um Estado-Membro, para permitir um nível de envolvimento adequado das entidades de supervisão e uma execução flexível, de modo que permita atender às especificidades dos subsetores financeiros ou dos mercados financeiros locais.

As AES devem apresentar esses projetos de normas técnicas de regulamentação à Comissão até [*Serviço das Publicações: inserir a data correspondente a 2 meses após a data de entrada em vigor*].

A Comissão fica habilitada a complementar o presente regulamento através da adoção das normas técnicas de regulamentação a que se refere o segundo parágrafo, nos termos dos artigos 10.º a 14.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1095/2010 e (UE) n.º 1094/2010, respetivamente.

Artigo 24.º

Requisitos aplicáveis aos responsáveis pela realização dos testes

1. As entidades financeiras só devem recorrer para a realização dos testes de penetração motivados por ameaças a responsáveis que:

(a) Sejam os mais adequados e os mais idóneos;

(b) Possuam as capacidades técnicas e organizativas e demonstrem ter conhecimentos especializados em informações sensíveis sobre ameaças, testes de penetração ou testes de «equipa vermelha»;

(c) Sejam certificados por um organismo de acreditação num Estado-Membro ou sigam códigos de conduta ou quadros éticos formais;

(d) No caso dos responsáveis externos, forneçam uma garantia independente ou um relatório de auditoria em relação à boa gestão dos riscos associada à execução dos testes de penetração motivados por ameaças, nomeadamente a devida proteção das informações confidenciais da entidade financeira e vias de mitigação dos riscos comerciais da entidade financeira;

(e) No caso dos responsáveis externos, estejam devida e totalmente cobertos por seguros de indemnização profissional relevantes, nomeadamente contra riscos de conduta irregular e negligência.

2. As entidades financeiras devem assegurar que os contratos celebrados com responsáveis externos pela realização de testes exijam uma boa gestão dos resultados dos testes de penetração motivados por ameaças e que qualquer tratamento dos mesmos, nomeadamente qualquer produção, projeto, conservação, agregação, elaboração de relatórios, comunicação ou destruição de dados não acarrete riscos para a entidade financeira.

CAPÍTULO V

GESTÃO DO RISCO DE TERCEIROS NO DOMÍNIO DAS TIC

SECÇÃO I

PRINCÍPIOS FUNDAMENTAIS PARA UMA BOA GESTÃO DO RISCO DE TERCEIROS NO DOMÍNIO DAS TIC

Artigo 25.º

Princípios gerais

As entidades financeiras devem gerir o risco de terceiros no domínio das TIC como parte integrante a título próprio do quadro de gestão do risco no domínio das TIC e em conformidade com os seguintes princípios:

1. As entidades financeiras que celebraram acordos contratuais relativos à utilização dos serviços no domínio das TIC para gerir as suas operações comerciais devem sempre assumir a responsabilidade pelo cumprimento e observância de todas as obrigações previstas no presente regulamento e na legislação aplicável em matéria de serviços financeiros.

2. A gestão do risco de terceiros no domínio das TIC pelas entidades financeiras deve ser efetuada em consonância com o princípio da proporcionalidade, tendo em conta:

(a) A dimensão, a complexidade e a importância das dependências relativas às TIC;

(b) Os riscos decorrentes dos contratos relativos à utilização dos serviços no domínio das TIC celebrados com entidades terceiras prestadoras de serviços no domínio das TIC, tendo em conta o caráter crítico ou a importância do respetivo serviço, processo ou função, bem como o impacto potencial na continuidade e na qualidade das atividades e dos serviços financeiros, a nível individual e de grupo.

3. Como parte do seu quadro de gestão do risco associado às TIC, as entidades financeiras devem adotar e rever periodicamente uma estratégia para o risco de terceiros no domínio das TIC, tendo em conta a estratégia de múltiplos fornecedores referida no artigo 5.º, n.º 9, alínea g). A referida estratégia deve incluir uma política relativa à utilização dos serviços TIC prestados pelas entidades terceiras a aplicar numa base individual e, quando necessário, numa base subconsolidada e consolidada. O órgão de administração deve rever periodicamente os riscos identificados em relação à externalização de funções críticas ou importantes.

4. Como parte do seu quadro de gestão do risco associado às TIC, as entidades financeiras devem manter e atualizar, ao nível da entidade e aos níveis subconsolidado e consolidado, um registo de informações em relação a todos os contratos relativos à utilização dos serviços TIC prestados por entidades terceiras.

   Os contratos referidos no primeiro parágrafo devem ser devidamente documentados, estabelecendo uma distinção entre os que abrangem funções críticas ou importantes e os que não abrangem esses tipos de funções.

   As entidades financeiras devem comunicar pelo menos anualmente às autoridades competentes informações sobre o número de novos contratos relativos à utilização de serviços TIC, as categorias de entidades terceiras prestadoras de serviços no domínio das TIC, o tipo de contratos, assim como os serviços que estão a ser prestados e as funções que estão a ser realizadas.

   As entidades financeiras devem disponibilizar à autoridade competente, mediante pedido, o registo de informações completo ou, se solicitado, secções desse registo, juntamente com as informações consideradas necessárias para permitir uma supervisão eficaz da entidade financeira.

   As entidades financeiras devem informar atempadamente a autoridade competente sobre a subcontratação planeada de funções críticas ou importantes e quando uma determinada função passar a ser crítica ou importante.

5. Antes de celebrar um contrato relativo à utilização de serviços TIC, as entidades financeiras devem:

   (a) Avaliar se o contrato abrange uma função crítica ou importante;

   (b) Avaliar se as condições em matéria de supervisão relativamente à subcontratação estão satisfeitas;

   (c) Identificar e avaliar todos os riscos relevantes em relação ao contrato, nomeadamente a possibilidade de esse contrato poder contribuir para reforçar o risco de concentração no domínio das TIC;

   (d) Efetuar todas as diligências devidas quanto às potenciais entidades terceiras prestadoras de serviços no domínio das TIC e assegurar que, ao longo dos processos de seleção e avaliação, a entidade terceira prestadora de serviços no domínio das TIC é adequada;

   (e) Identificar e avaliar os conflitos de interesses que o contrato possa causar.

6. As entidades financeiras só podem celebrar contratos com entidades terceiras prestadoras de serviços no domínio das TIC que cumpram normas de segurança da informação exigentes, apropriadas e que sejam as mais recentes disponíveis.

7. Ao exercer direitos de acesso, inspeção e auditoria sobre a entidade terceira prestadora de serviços no domínio das TIC, as entidades financeiras devem

predeterminar, com base numa abordagem baseada no risco, a frequência das auditorias e das inspeções e as áreas a auditar, aderindo a normas de auditoria comummente aceites em consonância com qualquer instrução de supervisão sobre a utilização e incorporação dessas normas de auditoria.

Para contratos que impliquem um nível elevado de complexidade tecnológica, a entidade financeira deve verificar se os auditores, sejam eles internos, grupos de auditores ou auditores externos, possuem as aptidões e os conhecimentos adequados para realizar eficazmente as auditorias e as avaliações pertinentes.

8. As entidades financeiras devem assegurar que a cessação contratual dos contratos relativos à utilização de serviços no domínio das TIC esteja prevista pelo menos nas seguintes circunstâncias:

(a) Violação pela entidade terceira prestadora de serviços no domínio das TIC da legislação, regulamentação ou das condições contratuais aplicáveis;

(b) Circunstâncias identificadas aquando da monitorização do risco de terceiros no domínio das TIC que sejam consideradas como passíveis de alterar o desempenho das funções realizadas através do contrato, nomeadamente alterações materiais que afetem o contrato ou a situação da entidade terceira prestadora de serviços no domínio das TIC;

(c) Debilidades comprovadas da entidade terceira prestadora de serviços no domínio das TIC na sua gestão global do risco associado às TIC e, em particular, na forma como garante a segurança e a integridade dos dados confidenciais, pessoais ou sensíveis ou das informações não pessoais;

(d) Circunstâncias em que a autoridade competente deixa de poder supervisionar eficazmente a entidade financeira em resultado do acordo contratual respetivo.

9. As entidades financeiras devem dispor de estratégias de saída por forma a terem em conta riscos que possam surgir ao nível da entidade terceira prestadora de serviços no domínio das TIC, em especial uma possível falha desta última, uma deterioração da qualidade das funções desempenhadas, qualquer perturbação das atividades devido a falha ou desadequação da prestação dos serviços ou qualquer risco material relacionado com o desempenho adequado e contínuo da função.

As entidades financeiras devem assegurar que são capazes de rescindir acordos contratuais sem que isso implique:

(a) Perturbação das suas atividades comerciais;

(b) Limitação da observância dos requisitos regulamentares;

(c) Prejuízo para a continuidade e a qualidade da sua prestação de serviços aos clientes.

Os planos de saída devem ser abrangentes, documentados e, se for caso disso, devem ser suficientemente testados.

As entidades financeiras devem identificar soluções alternativas e desenvolver planos de transição que lhes permitam eliminar as funções subcontratadas e recolher os dados pertinentes junto da entidade terceira prestadora de serviços no domínio das TIC e transferi-los em segurança e na íntegra para prestadores de serviços alternativos ou reincorporá-los internamente.

As entidades financeiras devem adotar medidas de contingência adequadas para manter a continuidade dos serviços em todas as circunstâncias referidas no primeiro parágrafo.

10. As AES devem, através do Comité Conjunto, desenvolver projetos de normas técnicas de execução por forma a criar modelos normalizados para fins do registo de informações referido no n.º 4.

As AES devem apresentar esses projetos de normas técnicas de execução à Comissão até [*Serviço das Publicações: inserir a data correspondente a um ano após a data de entrada em vigor do presente regulamento*].

É conferido à Comissão o poder de adotar as normas técnicas de execução a que se refere o primeiro parágrafo, nos termos do artigo 15.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1095/2010 e (UE) n.º 1094/2010, respetivamente.

11. As AES devem, através do Comité Conjunto, desenvolver projetos de normas técnicas de regulamentação para especificar mais pormenorizadamente:

(a) O conteúdo da política referida no n.º 3 em relação aos acordos contratuais relativos à utilização de serviços no domínio das TIC prestados por entidades terceiras, com referência às principais fases do ciclo de vida dos respetivos acordos relativos à utilização desses mesmos serviços no domínio das TIC;

(b) Os tipos de informações a incluir no registo de informações referido no n.º 4.

As AES devem apresentar esses projetos de normas técnicas de regulamentação à Comissão até [*Serviço das Publicações: inserir a data correspondente a um ano após a data de entrada em vigor*].

A Comissão fica habilitada a complementar o presente regulamento através da adoção das normas técnicas de regulamentação a que se refere o segundo parágrafo, nos termos dos artigos 10.º a 14.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1095/2010 e (UE) n.º 1094/2010, respetivamente.

Artigo 26.º

Avaliação preliminar do risco de concentração no domínio das TIC e outras disposições relativas aos acordos de subcontratação

1. Quando procedem à identificação e avaliação do risco de concentração no domínio das TIC referido no artigo 25.º, n.º 5, alínea c), as entidades financeiras devem ter em conta se a celebração de um contrato em relação a serviços no domínio das TIC pode conduzir a qualquer um das situações seguintes:

(a) Celebração de um contrato com uma entidade terceira prestadora de serviços no domínio das TIC que não seja facilmente substituível; ou

(b) Celebração de vários contratos em relação à prestação de serviços no domínio das TIC com a mesma entidade terceira prestadora de serviços no domínio das TIC ou com entidades terceiras prestadoras de serviços no domínio das TIC com ligações estreitas entre si.

As entidades financeiras devem ponderar os benefícios e os custos de soluções alternativas como a utilização de entidades terceiras prestadoras de serviços no domínio das TIC diferentes, tendo em conta se e como as soluções previstas

satisfazem as necessidades comerciais e os objetivos definidos na sua estratégia de resiliência digital.

2. Quando o contrato relativo à utilização de serviços no domínio das TIC incluir a possibilidade de uma entidade terceira prestadora de serviços no domínio das TIC subcontratar uma função crítica ou importante a outra entidade terceira prestadora de serviços no domínio das TIC, as entidades financeiras devem ponderar os benefícios e os riscos que podem surgir associados a essa possível subcontratação ulterior, em especial no caso de um subcontratante ulterior no domínio das TIC estabelecido num país terceiro.

   Quando os contratos relativos à utilização de serviços no domínio das TIC são celebrados com uma entidade terceira prestadora de serviços no domínio das TIC estabelecida num país terceiro, as entidades financeiras devem considerar como relevantes pelo menos os seguintes fatores:

   (a) O respeito pela proteção de dados;

   (b) A efetiva aplicação da lei;

   (c) As disposições jurídicas relativas à insolvência aplicáveis em caso de falência do terceiro prestador de serviços no domínio das TIC;

   (d) Quaisquer constrangimentos que possam surgir em relação à recuperação urgente dos dados da entidade financeira.

   As entidades financeiras devem avaliar se e de que forma as cadeias de subcontratação ulterior potencialmente longas e complexas podem afetar a sua capacidade de monitorizar totalmente as funções subcontratadas e a capacidade da autoridade competente para supervisionar eficazmente a entidade financeira nesse aspeto.

Artigo 27.º

Principais disposições contratuais

1. Os direitos e obrigações da entidade financeira e da entidade terceira prestadora de serviços no domínio das TIC devem ser claramente identificados e especificados por escrito. O contrato na sua totalidade, que inclui os acordos de nível de serviço, deve constar de um documento escrito disponível para as partes em papel ou num formato que permita o acesso e a descarga.

2. Os contratos relativos à utilização de serviços no domínio das TIC deve incluir pelo menos:

   (a) Uma descrição clara e completa de todas as funções e serviços a prestar pela entidade terceira prestadora de serviços no domínio das TIC, indicando se a subcontratação ulterior de uma função crítica ou importante, ou de partes materiais da mesma, é permitida e, em caso afirmativo, as condições aplicáveis a essa subcontratação ulterior;

   (b) Os locais onde as funções e os serviços objeto de subcontratação ou subcontratação ulterior devem ser prestados e onde devem ser tratados os dados, nomeadamente o local de conservação dos dados, bem como o requisito, aplicável à entidade terceira prestadora de serviços no domínio das TIC, de notificar a entidade financeira se planear mudar de local;

(c) Disposições sobre a acessibilidade, disponibilidade, integridade, segurança e proteção dos dados pessoais e sobre a garantia de acesso, recuperação e devolução, num formato facilmente acessível, dos dados pessoais e dos dados não pessoais tratados pela entidade financeira em caso de insolvência, resolução ou descontinuação das operações comerciais da entidade terceira prestadora de serviços no domínio das TIC;

(d) Descrições completas dos acordos de nível de serviço, incluindo as respetivas atualizações e revisões, e metas de desempenho quantitativas e qualitativas rigorosas para os níveis de serviço acordados, por forma a permitir uma monitorização eficaz pela entidade financeira e permitir, sem demora indevida, a adoção de medidas corretivas quando os níveis de serviço acordados não forem cumpridos;

(e) Períodos de notificação e obrigações de comunicação de informações da entidade terceira prestadora de serviços no domínio das TIC à entidade financeira, nomeadamente quanto a quaisquer desenvolvimentos que possam ter impacto material na capacidade de a entidade terceira prestadora de serviços no domínio das TIC desempenhar eficazmente funções críticas ou importantes em consonância com os níveis de serviço acordados;

(f) A obrigação de a entidade terceira prestadora de serviços no domínio das TIC prestar assistência em caso de incidente relacionado com as TIC sem custos adicionais ou com um custo previamente determinado;

(g) Requisitos aplicáveis à entidade terceira prestadora de serviços no domínio das TIC no sentido de executar e testar planos de contingência para as suas atividades e de dispor de medidas, ferramentas e políticas de segurança no domínio das TIC que garantam adequadamente uma prestação de serviços segura pela entidade financeira em consonância com o seu quadro regulamentar;

(h) O direito de monitorizar numa base contínua o desempenho da entidade terceira prestadora de serviços no domínio das TIC, o que inclui:

i) direitos de acesso, inspeção e auditoria pela entidade financeira ou por um terceiro designado, bem como o direito a recolher cópias da documentação importante, cujo exercício efetivo não seja impedido nem limitado por outras disposições contratuais ou políticas de execução,

ii) o direito a acordar níveis de garantia alternativos caso os direitos de outros clientes sejam afetados,

iii) o compromisso de total cooperação durante as inspeções no local realizadas pela entidade financeira e pormenores sobre o âmbito, as modalidades e a frequência das auditorias à distância;

(i) A obrigação de o terceiro prestador de serviços no domínio das TIC cooperar totalmente com as autoridades competentes e as autoridades de resolução da entidade financeira e, nomeadamente, com pessoas designadas por essas autoridades;

(j) Direitos de rescisão e períodos mínimos de pré-aviso relacionados com a rescisão do contrato, em conformidade com as expectativas das autoridades competentes;

(k) Estratégias de saída, em especial a determinação de um período de transição obrigatório adequado:

(a) durante o qual a entidade terceira prestadora de serviços no domínio das TIC continuará a desempenhar as respetivas funções ou a prestar os respetivos serviços com vista a reduzir o risco de perturbações na entidade financeira,

(b) que permita à entidade financeira passar a utilizar outra entidade terceira prestadora de serviços no domínio das TIC ou soluções internas consistentes com a complexidade do serviço prestado.

3. Aquando da negociação dos contratos, as entidades financeiras e as entidades terceiras prestadoras de serviços no domínio das TIC devem considerar a utilização de cláusulas contratuais normalizadas desenvolvidas para serviços específicos.

4. As AES devem, através do Comité Conjunto, desenvolver projetos de normas técnicas de regulamentação que especifiquem mais pormenorizadamente os elementos de que uma entidade financeira necessita para determinar e avaliar quando é que deve proceder à subcontratação ulterior de funções críticas ou importantes para cumprir adequadamente as disposições do n.º 2, alínea a).

As AES devem apresentar esses projetos de normas técnicas de regulamentação à Comissão até [*Serviço das Publicações: inserir a data correspondente a um ano após a data de entrada em vigor*].

A Comissão fica habilitada a complementar o presente regulamento através da adoção das normas técnicas de regulamentação a que se refere o primeiro parágrafo, nos termos dos artigos 10.º a 14.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1095/2010 e (UE) n.º 1094/2010, respetivamente.

SECÇÃO II

QUADRO DE FISCALIZAÇÃO DAS ENTIDADES TERCEIRAS PRESTADORAS DE SERVIÇOS NO DOMÍNIO DAS TIC CONSIDERADAS CRÍTICAS

Artigo 28.º

Designação das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas

1. As AES, através do Comité Conjunto e mediante recomendação do Fórum de Fiscalização criado nos termos do artigo 29.º, n.º 1, devem:

(a) Designar as entidades terceiras prestadoras de serviços no domínio das TIC que são críticas para as entidades financeiras, tendo em conta os critérios especificados no n.º 2:

(b) Nomear a EBA, a ESMA ou a EIOPA como autoridade fiscalizadora principal para cada entidade terceira prestadora de serviços no domínio das TIC considerada crítica, consoante o valor total dos ativos das entidades financeiras que utilizam os serviços dessa entidade terceira prestadora de serviços no domínio das TIC considerada crítica e que estão abrangidas pelos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 ou (UE) n.º 1095/2010, respetivamente, represente mais de metade do valor dos ativos totais de todas as entidades financeiras que utilizam os serviços da entidade terceira prestadora

de serviços no domínio das TIC considerada crítica, tal como demonstrado nos balanços consolidados, ou nos balanços individuais quando não existem balanços consolidados, dessas entidades financeiras.

2. A designação a que se refere o n.º 1, alínea a), deve basear-se em todos os critérios seguintes:

(a) O impacto sistémico na estabilidade, continuidade ou qualidade da prestação dos serviços financeiros caso a entidade terceira prestadora de serviços no domínio das TIC pertinente venha a enfrentar uma falha operacional de grandes proporções que a impeça de prestar os seus serviços, tendo em conta o número de entidades financeiras que beneficiam dos serviços prestados por essa entidade considerada relevante;

(b) O caráter sistémico ou a importância das entidades financeiras que dependem da entidade terceira prestadora de serviços no domínio das TIC considerada relevante, avaliados de acordo com os parâmetros seguintes:

i) o número de instituições de importância sistémica global (G-SII) ou outras instituições de importância sistémica (O-SII) que dependem da respetiva entidade terceira prestadora de serviços no domínio das TIC,

ii) a interdependência entre as G-SII ou as O-SII referidas na subalínea i) e outras entidades financeiras, incluindo situações em que as G-SII ou as O-SII prestam serviços financeiros infraestruturais a outras entidades financeiras;

(c) A dependência das entidades financeiras em relação aos serviços prestados pela entidade terceira prestadora de serviços no domínio das TIC considerada relevante relativamente a funções críticas ou importantes das entidades financeiras que, em última análise, envolvam a mesma entidade terceira prestadora de serviços no domínio das TIC, independentemente do facto de as entidades financeiras dependerem desses serviços direta ou indiretamente, por intermédio ou através de subcontratação ulterior;

(d) A medida em que a entidade terceira prestadora de serviços no domínio das TIC poderá ser substituída, tendo em conta os seguintes parâmetros:

i) falta de alternativas reais, mesmo que parciais, devido ao número limitado de entidades terceiras prestadoras de serviços no domínio das TIC ativas num mercado especifico, à quota de mercado da entidade terceira prestadora de serviços no domínio das TIC considerada relevante, à complexidade ou sofisticação técnicas envolvidas, nomeadamente em relação a qualquer tecnologia patenteada, ou ainda às características específicas da organização ou atividade da entidade terceira prestadora de serviços no domínio das TIC,

ii) dificuldades em migrar parcial ou totalmente os dados pertinentes e os volumes de trabalho da entidade terceira prestadora de serviços no domínio das TIC considerada relevante para outra entidade idêntica, devido aos custos financeiros significativos, ao tempo ou a outro tipo de recursos envolvidos no processo de migração ou devido ao aumento dos riscos associados às TIC ou outros riscos operacionais a que a entidade financeira possa ficar exposta por via dessa migração.

(e) O número de Estados-Membros em que a entidade terceira prestadora de serviços no domínio das TIC considerada relevante presta serviços;

(f) O número de Estados-Membros em que as entidades financeiras que recorrem à entidade terceira prestadora de serviços no domínio das TIC considerada relevante estão a operar.

3. A Comissão fica habilitada a adotar atos delegados em conformidade com o artigo 50.º que complementem os critérios referidos no n.º 2.

4. O mecanismo de designação referido no n.º 1, alínea a), não pode ser utilizado até que a Comissão adote um ato delegado em conformidade com o n.º 3.

5. O mecanismo de designação referido no n.º 1, alínea a), não é aplicável em relação às entidades terceiras prestadoras de serviços no domínio das TIC que estejam sujeitas a quadros de fiscalização criados com a finalidade de apoiar as atribuições indicadas no artigo 127.º, n.º 2, do Tratado sobre o Funcionamento da União Europeia.

6. As AES, através do Comité Conjunto, devem criar, publicar e atualizar anualmente a lista de entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas a nível da União.

7. Para efeitos do n.º 1, alínea a), as autoridades competentes devem transmitir, anualmente e numa base agregada, os relatórios referidos no artigo 25.º, n.º 4, ao Fórum de Fiscalização criado nos termos do artigo 29.º. O Fórum de Fiscalização deve avaliar as dependências das entidades financeiras em relação a terceiros no domínio das TIC com base nas informações recebidas das autoridades competentes.

8. As entidades terceiras prestadoras de serviços no domínio das TIC que não estejam incluídas na lista referida no n.º 6 podem solicitar a sua inclusão nessa lista.

Para efeitos do primeiro parágrafo, a entidade terceira prestadora de serviços no domínio das TIC deve apresentar uma candidatura fundamentada à EBA, à ESMA ou à EIOPA, que, através do Comité Conjunto, deve decidir se inclui essa entidade terceira prestadora de serviços no domínio das TIC nessa lista em conformidade com o n.º 1, alínea a).

A decisão a que se refere o segundo parágrafo deve ser adotada e notificada à entidade terceira prestadora de serviços no domínio das TIC no prazo de seis meses a contar da receção da candidatura.

9. As entidades financeiras não devem recorrer a uma entidade terceira prestadora de serviços no domínio das TIC estabelecida num país terceiro que seria considerada crítica nos termos do n.º 1, alínea a), caso estivesse estabelecida na União.

Artigo 29.º

Estrutura do quadro de fiscalização

1. O Comité Conjunto, em conformidade com o artigo 57.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, deve criar o Fórum de Fiscalização, enquanto subcomité, com a finalidade de apoiar o trabalho do Comité Conjunto e da Autoridade Fiscalizadora Principal referida no artigo 28.º, n.º 1, alínea a), no domínio do risco de terceiros associado às TIC em todos os setores financeiros. O Fórum de Fiscalização deve preparar os projetos das posições comuns e dos atos comuns do Comité Conjunto nesse domínio.

O Fórum de Fiscalização deve debater periodicamente os desenvolvimentos mais importantes associados aos riscos e às vulnerabilidades das TIC e promover uma abordagem coerente na monitorização do risco de terceiros associado às TIC ao nível da União.

2. O Fórum de Fiscalização deve realizar anualmente uma avaliação coletiva dos resultados e das conclusões das atividades de fiscalização desenvolvidas em relação a todas as entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas e promover medidas de coordenação para aumentar a resiliência operacional digital das entidades financeiras, fomentar as boas práticas no que toca à resposta ao risco de concentração no domínio das TIC e explorar fatores atenuantes em relação às transferências de risco entre setores.

3. O Fórum de Fiscalização deve apresentar indicadores de referência abrangentes em relação às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas, a adotar pelo Comité Conjunto enquanto posições comuns das AES em conformidade com os artigos 56.º, n.º 1, dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010.

4. O Fórum de Fiscalização é constituído pelos presidentes das AES e por um representante de alto nível do pessoal atualmente em funções nas autoridades competentes relevantes de cada Estado-Membro. Os Administradores Executivos de cada AES e um representante da Comissão Europeia, do CERS, do BCE e da ENISA devem participar no Fórum de Fiscalização na qualidade de observadores.

5. Em conformidade com o artigo 16.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, as AES devem emitir orientações sobre a cooperação entre as AES e as autoridades competentes para efeitos da presente secção, sobre os procedimentos pormenorizados e as condições relacionadas com o exercício das atribuições das autoridades competentes e as AES e sobre os pormenores relativos aos intercâmbios de informações necessários para que as autoridades competentes possam assegurar o acompanhamento das recomendações das Autoridades Fiscalizadoras Principais nos termos do artigo 31.º, n.º 1, alínea d), dirigidas às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas.

6. Os requisitos definidos na presente secção não prejudicam a aplicação da Diretiva (UE) 2016/1148 e das outras regras da União em matéria de fiscalização aplicáveis aos prestadores de serviços de computação em nuvem.

7. As AES, através do Comité Conjunto e com base no trabalho preparatório realizado pelo Fórum de Fiscalização, devem apresentar anualmente ao Parlamento Europeu, ao Conselho e à Comissão um relatório sobre a aplicação da presente secção.

Artigo 30.º

Atribuições da Autoridade Fiscalizadora Principal

1. A Autoridade Fiscalizadora Principal deve avaliar se cada entidade terceira prestadora de serviços no domínio das TIC considerada crítica dispõe de regras, procedimentos, mecanismos e disposições abrangentes, sólidas e eficazes para gerir os riscos associados às TIC que possam acarretar para as entidades financeiras.

2. A avaliação referida no n.º 1 deve incluir:

(a) Os requisitos em matéria de TIC para assegurar, em especial, a segurança, a disponibilidade, a continuidade, a capacidade de redimensionamento e a qualidade dos serviços que a entidade terceira prestadora de serviços no domínio das TIC considerada crítica presta às entidades financeiras, bem como a capacidade para manter sempre níveis muito elevados de segurança, confidencialidade e integridade dos dados;

(b) A segurança física que contribui para assegurar a segurança no domínio das TIC, nomeadamente a segurança dos edifícios, das instalações, dos centros de dados;

(c) Os processos de gestão dos riscos, nomeadamente políticas de gestão do risco associado às TIC, continuidade das atividades no domínio das TIC e planos de recuperação em caso de catástrofe no domínio das TIC;

(d) Disposições de governação, nomeadamente uma estrutura organizativa com uma hierarquia clara, transparente e coerente em termos de responsabilidade e regras de responsabilização que permitam uma gestão eficaz do risco associado às TIC;

(e) A identificação, monitorização e comunicação rápida dos incidentes relacionados com as TIC às entidades financeiras, bem como a gestão e resolução desses incidentes, em especial no caso dos ciberataques;

(f) Mecanismos de portabilidade dos dados, das aplicações e de interoperabilidade que assegurem um exercício eficaz dos direitos de rescisão contratual pelas entidades financeiras;

(g) A realização de testes aos sistemas, à infraestrutura e aos controlos no domínio das TIC;

(h) Auditorias no domínio das TIC;

(i) A utilização das normas nacionais e internacionais pertinentes aplicáveis à prestação dos seus serviços no domínio das TIC a entidades financeiras.

3. Com base na avaliação referida no n.º 1, a Autoridade Fiscalizadora Principal deve adotar um plano de fiscalização individual claro, pormenorizado e fundamentado para cada entidade terceira prestadora de serviços no domínio das TIC considerada crítica. Esse plano deve ser comunicado todos os anos à entidade terceira prestadora de serviços no domínio das TIC considerada crítica.

4. Depois de os planos anuais de fiscalização referidos no n.º 3 estarem definidos e serem notificados às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas, as autoridades competentes só podem adotar medidas em relação a essas entidades de comum acordo com a Autoridade Fiscalizadora Principal.

Artigo 31.º

Poderes da Autoridade Fiscalizadora Principal

1. Para efeitos da execução das funções definidas na presente secção, a Autoridade Fiscalizadora Principal fica habilitada a:

(a) Solicitar todas as informações e toda a documentação pertinentes em conformidade com o artigo 32.º;

(b) Realizar investigações e inspeções de caráter geral em conformidade com os artigos 33.º e 34.º;

(c) Solicitar relatórios após a conclusão das atividades de fiscalização que especifiquem as medidas que foram adotadas ou as correções que foram implementadas pelas entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas em relação às recomendações referidas na alínea d) do presente número;

(d) Formular recomendações nos domínios referidos no artigo 30.º, n.º 2, especialmente em relação aos seguintes elementos:

i) utilização de requisitos ou processos de segurança e qualidade específicos no domínio das TIC, designadamente em relação à introdução de correções, atualizações, medidas de encriptação e outras medidas de segurança que a Autoridade Fiscalizadora Principal considere pertinentes para assegurar a segurança dos serviços prestados às entidades financeiras no domínio das TIC,

ii) utilização de condições e termos, incluindo a respetiva execução técnica, ao abrigo dos quais a entidade terceira prestadora de serviços no domínio das TIC considerada crítica presta serviços às entidades financeiras e que a Autoridade Fiscalizadora Principal considere pertinentes para prevenir a geração de falhas pontuais, ou a disseminação das mesmas, ou para minimizar o possível impacto sistémico no setor financeiro da União em caso de risco de concentração no domínio das TIC,

iii) com base no exame das disposições contratuais efetuado em conformidade com os artigos 32.º e 33.º, incluindo disposições relativas a subcontratação ulterior que as entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas planeiem entregar a outras entidades terceiras prestadoras de serviços no domínio das TIC ou a subcontratantes no domínio das TIC estabelecidos num país terceiro, qualquer subcontratação planeada, nomeadamente quando envolva uma subcontratação em cascata, sempre que a Autoridade Fiscalizadora Principal considere que essa subcontratação ulterior pode acarretar riscos para a prestação dos serviços à entidade financeira ou para a estabilidade financeira,

iv) abster-se de celebrar mais contratos de subcontratação, quando se verificarem as seguintes condições cumulativas:

– o subcontratante prevista é uma entidade terceira prestadora de serviços no domínio das TIC ou um subcontratante nesse domínio estabelecido num país terceiro,

– a subcontratação diz respeito a uma função crítica ou importante da entidade financeira.

2. A Autoridade Fiscalizadora Principal deve consultar o Fórum de Fiscalização antes de exercer os poderes referidos no n.º 1.

3. As entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas devem cooperar de boa-fé com a Autoridade Fiscalizadora Principal e auxiliá-la no exercício das suas atribuições.

4. A Autoridade Fiscalizadora Principal pode impor uma sanção pecuniária periódica para obrigar a entidade terceira prestadora de serviços no domínio das TIC considerada crítica a cumprir as alíneas a), b) e c), do n.º 1.

5. A sanção pecuniária periódica referida no n.º 4 deve ser imposta numa base diária até que se alcance o resultado pretendido, ou seja, o cumprimento das condições, mas nunca por um período superior a seis meses a contar da notificação da entidade terceira prestadora de serviços no domínio das TIC considerada crítica.

6. O montante da sanção pecuniária periódica, calculado a partir da data estipulada na decisão que a imponha, é de 1 % do volume de negócios mundial médio diário da entidade terceira prestadora de serviços no domínio das TIC considerada crítica no exercício anterior.

7. As sanções pecuniárias assumem uma natureza administrativa e devem ser efetivamente aplicáveis. A aplicação é regulada pelas normas de processo civil em vigor no Estado-Membro em cujo território se efetuam as inspeções e o acesso. Os tribunais do Estado-Membro em causa têm competência sobre as queixas relacionadas com a conduta irregular da aplicação da regulamentação. Os montantes das sanções pecuniárias são afetados ao orçamento geral da União Europeia.

8. As AES devem divulgar ao público todas as sanções pecuniárias periódicas que tenham imposto, a menos que tal divulgação possa afetar gravemente os mercados financeiros ou causar danos desproporcionados aos interessados.

9. Antes de impor uma sanção pecuniária periódica nos termos do n.º 4, a Autoridade Fiscalizadora Principal deve dar aos representantes da entidade terceira prestadora de serviços no domínio das TIC considerada crítica objeto do processo a oportunidade de serem ouvidos sobre as conclusões e deverá basear as suas decisões exclusivamente nas conclusões em relação às quais a entidade terceira prestadora de serviços no domínio das TIC considerada crítica tenha tido oportunidade de se pronunciar. Os direitos de defesa das pessoas objeto do processo devem ser plenamente respeitados no decurso do processo. Essas pessoas têm direito a consultar o processo, sob reserva do interesse legítimo de terceiros na proteção dos seus segredos comerciais. O direito de acesso ao processo não é extensível a informações confidenciais nem aos documentos preparatórios internos da Autoridade Fiscalizadora Principal.

Artigo 32.º
Pedidos de informação

1. A Autoridade Fiscalizadora Principal pode solicitar às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas, através de um pedido simples ou de uma decisão, que forneçam todas as informações necessárias para que a Autoridade Fiscalizadora Principal cumpra as suas obrigações ao abrigo do presente regulamento, nomeadamente todos os documentos comerciais ou operacionais, contratos, documentação sobre políticas, relatórios de auditorias à segurança no domínio das TIC ou relatórios de incidentes relacionados com as TIC que considere pertinentes, bem como quaisquer informações relacionadas com as partes a quem a entidade terceira prestadora de serviços no domínio das TIC considerada crítica subcontratou funções ou atividades operacionais.

2. Ao enviar um simples pedido de informações nos termos do n.º 1, a Autoridade Fiscalizadora Principal deve:

(a) Remeter para o presente artigo como base legal do pedido;

(b) Indicar a finalidade do pedido;

(c) Especificar as informações solicitadas;

(d) Fixar um prazo para a prestação das informações;

(e) Informar o representante da entidade terceira prestadora de serviços no domínio das TIC considerada crítica a quem as informações são solicitadas de que não é obrigado a fornecê-las mas que, caso aceda voluntariamente ao pedido, as informações prestadas não devem ser incorretas nem suscetíveis de induzir em erro.

3. Ao solicitar que lhe seja fornecida informação nos termos do n.º 1, a Autoridade Fiscalizadora Principal deve:

(a) Remeter para o presente artigo como base legal do pedido;

(b) Indicar a finalidade do pedido;

(c) Especificar as informações solicitadas;

(d) Fixar um prazo para a prestação das informações;

(e) Referir as sanções pecuniárias periódicas previstas no artigo 31.º, n.º 4, para o caso de as informações prestadas serem incompletas;

(f) Mencionar o direito a recorrer da decisão para a Câmara de Recurso das AES e o direito ao controlo da legalidade da decisão pelo Tribunal de Justiça da União Europeia («Tribunal de Justiça») em conformidade com os artigos 60.º e 61.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, respetivamente.

4. Os representantes das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas devem fornecer as informações solicitadas. Os advogados devidamente mandatados podem fornecer as informações pedidas em nome dos seus mandantes. A entidade terceira prestadora de serviços no domínio das TIC considerada crítica é plenamente responsável em caso de prestação de informações incompletas, incorretas ou que induzam em erro.

5. A Autoridade Fiscalizadora Principal deve, sem demora, enviar uma cópia da decisão de fornecer as informações às autoridades competentes das entidades financeiras que utilizam os serviços das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas.

Artigo 33.º

Investigações de caráter geral

1. Por forma a cumprir as suas obrigações ao abrigo do presente regulamento, a Autoridade Fiscalizadora Principal, auxiliada pela equipa de avaliação a que se refere o artigo 34.º, n.º 1, pode realizar as investigações necessárias junto das entidades terceiras prestadoras de serviços no domínio das TIC;

2. A Autoridade Fiscalizadora Principal fica habilitada a:

(a) Examinar registos, dados, procedimentos ou qualquer outro material relevante para o exercício das suas atribuições, independentemente do meio em que se encontrem armazenados;

(b) Recolher ou obter cópias autenticadas ou extratos desses registos, dados, procedimentos ou outro material;

(c) Convocar representantes das entidades terceiras prestadoras de serviços no domínio das TIC para prestarem esclarecimentos, oralmente ou por escrito, sobre factos ou documentos relacionados com o objeto e a finalidade da investigação, e registar as suas respostas;

(d) Inquirir quaisquer outras pessoas singulares ou coletivas que concordem em ser inquiridas a fim de recolher informações relacionadas com o objeto de uma investigação;

(e) Requerer a apresentação de registos telefónicos e de transmissão de dados.

3. Os funcionários e outras pessoas autorizadas pela Autoridade Fiscalizadora Principal para efeitos das investigações a que se refere o n.º 1 exercem os referidos poderes mediante a apresentação de uma autorização escrita que especifique o objeto e a finalidade da investigação.

A referida autorização deve também indicar as sanções pecuniárias periódicas previstas no artigo 31.º, n.º 4, para os casos em que não se proceda à apresentação dos registos, dados, procedimentos ou quaisquer outros materiais solicitados, ou quando as respostas às perguntas feitas aos representantes da entidade terceira prestadora de serviços no domínio das TIC não forem fornecidas ou estiverem incompletas.

4. Os representantes das entidades terceiras prestadoras de serviços no domínio das TIC são obrigados a colaborar com as investigações com base numa decisão da Autoridade Fiscalizadora Principal. A decisão deve especificar o objeto e a finalidade da investigação, as sanções pecuniárias periódicas previstas no artigo 31.º, n.º 4, as possibilidades de recurso previstas nos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, bem como o direito de requerer a apreciação da decisão pelo Tribunal de Justiça.

5. Com a devida antecedência em relação à investigação, as Autoridades Fiscalizadoras Principais devem informar as autoridades competentes das entidades financeiras que recorrem à entidade terceira prestadora de serviços no domínio das TIC da investigação e da identidade das pessoas autorizadas.

Artigo 34.º

Inspeções no local

1. Por forma a cumprir as suas obrigações ao abrigo do presente regulamento, a Autoridade Fiscalizadora Principal, auxiliada pelas equipas de avaliação a que se refere o artigo 35.º, n.º 1, pode entrar e realizar as necessárias inspeções no local em qualquer uma das instalações comerciais, terrenos ou propriedades das entidades terceiras prestadoras de serviços no domínio das TIC, tais como sedes, centros de operações, instalações secundárias, bem como realizar inspeções fora de linha.

2. Os funcionários e outras pessoas autorizadas pela Autoridade Fiscalizadora Principal para realizar uma inspeção no local podem entrar em quaisquer dessas instalações comerciais, terrenos ou propriedades e ficam habilitados, na medida do necessário, a selar quaisquer instalações comerciais, livros ou registos do período a que se refere a investigação.

Esses poderes podem ser exercidos mediante a apresentação de uma autorização escrita que especifique o objeto e a finalidade da inspeção e as sanções pecuniárias periódicas previstas no artigo 31.º, n.º 4, quando os representantes das entidades terceiras prestadoras de serviços no domínio das TIC em causa não colaborarem com a investigação.

3. Com a devida antecedência em relação à inspeção, as Autoridades Fiscalizadoras Principais devem informar as autoridades competentes das entidades financeiras que recorrem a essa entidade terceira prestadora de serviços no domínio das TIC.

4. As inspeções devem abranger todo o conjunto de sistemas, redes, dispositivos, informações e dados pertinentes no domínio das TIC que seja utilizado ou contribua para a prestação dos serviços às entidades financeiras.

5. Antes de qualquer visita planeada ao local, as Autoridades Fiscalizadoras Principais devem notificar com antecedência razoável as entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas, exceto se não for possível proceder a essa notificação devido a uma emergência ou situação de crise, ou se a notificação puder conduzir a uma situação em que a inspeção ou auditoria deixaria de ser eficaz.

6. A entidade terceira prestadora de serviços no domínio das TIC considerada crítica deve colaborar com as inspeções no local ordenadas por uma decisão da Autoridade Fiscalizadora Principal. A decisão deve especificar o objeto e a finalidade da inspeção, fixar a data em que esta se deve iniciar e indicar as sanções pecuniárias periódicas previstas no artigo 31.º, n.º 4, as possibilidades de recurso previstas nos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, bem como o direito de requerer a reapreciação da decisão pelo Tribunal de Justiça.

7. Quando os funcionários e outras pessoas autorizadas pela Autoridade Fiscalizadora Principal constatarem que uma entidade terceira prestadora de serviços no domínio das TIC considerada crítica se opõe a uma inspeção ordenada nos termos do presente artigo, a Autoridade Fiscalizadora Principal deve informar a entidade terceira prestadora de serviços no domínio das TIC considerada crítica das consequência dessa oposição, nomeadamente da possibilidade de as autoridades competentes das entidades financeiras pertinentes rescindirem os contratos celebrados com essa entidade terceira prestadora de serviços no domínio das TIC considerada crítica.

Artigo 35.º

Fiscalização corrente

1. Quando se encontram a realizar investigações de caráter geral ou inspeções no local, as Autoridades Fiscalizadoras Principais devem ser auxiliadas por uma equipa de avaliação criada para cada entidade terceira prestadora de serviços no domínio das TIC considerada crítica.

2. A equipa de avaliação conjunta referida no n.º 1 deve ser composta por membros do pessoal da Autoridade Fiscalizadora Principal e das autoridades competentes pertinentes que supervisionam as entidades financeiras a quem a entidade terceira prestadora de serviços no domínio das TIC considerada crítica presta serviços, que se juntarão à preparação e execução das atividades de fiscalização, com um máximo de dez elementos. Todos os membros da equipa de avaliação conjunta devem ter conhecimentos especializados em TIC e em risco operacional. A equipa de avaliação conjunta deve trabalhar sob a coordenação de um membro do pessoal da AES designada (o «coordenador da Autoridade Fiscalizadora Principal»).

3. As AES, através do Comité Conjunto, devem desenvolver projetos de normas técnicas de regulamentação comuns que especifiquem mais pormenorizadamente a designação dos membros da equipa de avaliação conjunta oriundos das autoridades competentes pertinentes, bem como as atribuições e a organização do trabalho da equipa de avaliação. As AES devem apresentar esses projetos de normas técnicas de regulamentação à Comissão até [*Serviço das Publicações: inserir a data correspondente a um ano após a data de entrada em vigor*].

A Comissão fica habilitada a adotar as normas técnicas de regulamentação a que se refere o primeiro parágrafo nos termos dos artigos 10.º a 14.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, respetivamente.

4. No prazo de três meses após a conclusão de uma investigação ou inspeção no local, a Autoridade Fiscalizadora Principal, após consulta do Fórum de Fiscalização, deve adotar as recomendações que a Autoridade Fiscalizadora Principal pretende dirigir à entidade terceira prestadora de serviços no domínio das TIC considerada crítica no âmbito dos poderes referidos no artigo 31.º.

5. As recomendações referidas no n.º 4 devem ser comunicadas imediatamente à entidade terceira prestadora de serviços no domínio das TIC considerada crítica e às autoridades competentes das entidades financeiras às quais aquela presta serviços.

Para efeitos da realização das atividades de fiscalização, as Autoridades Fiscalizadores Principais podem levar em consideração quaisquer certificações relevantes de terceiros e relatórios de auditorias internas ou externas de terceiros no domínio das TIC disponibilizadas pela entidade terceira prestadora de serviços no domínio das TIC considerada crítica.

Artigo 36.º

Harmonização das condições que permitem proceder a uma fiscalização

1. As AES devem, através do Comité Conjunto, elaborar projetos de normas técnicas de regulamentação a fim de especificar:

(a) As informações que devem ser facultadas pela entidade terceira prestadora de serviços no domínio das TIC considerada crítica no pedido de inclusão voluntária previsto no artigo 28.º, n.º 8.

(b) O conteúdo e o formato dos relatórios que podem ser solicitados para efeitos do artigo 31.º, n.º 1, alínea c);

(c) A forma, nomeadamente em termos de estrutura, formatos e métodos, de apresentação das informações que uma entidade terceira prestadora de serviços no domínio das TIC considerada crítica é obrigada a apresentar, divulgar ou comunicar nos termos do artigo 31.º, n.º 1;

(d) Os pormenores da avaliação pelas autoridades competentes das medidas tomadas pelas entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas com base nas recomendações das Autoridades Fiscalizadoras Principais nos termos do artigo 37.º, n.º 2.

2. As AES devem apresentar esses projetos de normas técnicas de regulamentação à Comissão até 1 de janeiro de 20xx [*Serviço das Publicações: inserir a data correspondente a um ano após a data de entrada em vigor*].

A Comissão fica habilitada a completar o presente regulamento através da adoção das normas técnicas de regulamentação a que se refere o primeiro parágrafo, nos termos do procedimento previsto no artigos 10.º a 14.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, respetivamente.

Artigo 37.º

Acompanhamento pelas autoridades competentes

1. No prazo de 30 dias úteis após a receção das recomendações formuladas pelas Autoridades Fiscalizadores Principais nos termos do artigo 31.º, n.º 1, alínea d), as entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas devem notificar à Autoridade Fiscalizadora Principal se pretendem ou não seguir essas recomendações. As Autoridades Fiscalizadoras Principais devem transmitir imediatamente essa informação às autoridades competentes.

2. As autoridades competentes devem verificar se as entidades financeiras têm em conta os riscos identificados nas recomendações dirigidas às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas pela Autoridade Fiscalizadora Principal em conformidade com o artigo 31.º, n.º 1, alínea d).

3. As autoridades competentes podem, em conformidade com o artigo 44.º, exigir que as entidades financeiras suspendam temporariamente, em parte ou na totalidade, a utilização ou o lançamento de um serviço prestado pela entidade terceira prestadora de serviços no domínio das TIC considerada crítica até que os riscos identificados nas recomendações dirigidas às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas sejam implementadas. Quando necessário, podem exigir que as entidades financeiras resolvam, em parte ou na totalidade, os contratos pertinentes celebrados com as entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas.

4. Quando tomam as decisões referidas no n.º 3, as autoridades competentes devem ter em conta o tipo e a dimensão do risco que não foi abordado pela entidade terceira prestadora de serviços no domínio das TIC considerada crítica, bem como a gravidade do incumprimento, tendo em conta os critérios seguintes:

   (a) A gravidade e a duração do incumprimento;

   (b) Se o incumprimento revelou debilidades graves nos procedimentos, nos sistemas de gestão, na gestão do risco e nos controlos internos da entidade terceira prestadora de serviços no domínio das TIC considerada crítica;

   (c) Se o incumprimento facilitou, ocasionou ou esteve de alguma forma na origem de atos de criminalidade financeira;

   (d) Se o incumprimento foi cometido com dolo ou por negligência.

5. As autoridades competentes devem informar regularmente as Autoridades Fiscalizadores Principais das abordagens e medidas adotadas nas suas atribuições de supervisão em relação às entidades financeiras, bem como das medidas contratuais adotadas por estas últimas quando a entidade terceira prestadora de serviços no domínio das TIC considerada crítica não tiver acatado, em parte ou na totalidade, as recomendações formuladas pelas Autoridades Fiscalizadores Principais.

Artigo 38.º

Taxas de fiscalização

1. As AES cobram às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas taxas que cubram as despesas necessárias para que as AES exerçam as suas atribuições de fiscalização nos termos do presente regulamento, nomeadamente o reembolso de eventuais custos em que possam incorrer em resultado do trabalho realizado pelas autoridades competentes que tenham participado nas atividades de fiscalização em conformidade com o artigo 35.º.

   O montante de uma taxa cobrada a uma entidade terceira prestadora de serviços no domínio das TIC considerada crítica deve cobrir todos os custos administrativos e deve ser proporcional ao seu volume de negócios.

2. A Comissão fica habilitada a adotar um ato delegado nos termos do artigo 50.º para complementar o presente regulamento determinando o montante das taxas e as modalidades de pagamento.

Artigo 39.º

Cooperação internacional

1. A EBA, a ESMA e a EIOPA podem, em conformidade com o artigo 33.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, respetivamente, celebrar acordos administrativos com autoridades de regulamentação e de supervisão de países terceiros para fomentar a cooperação internacional em matéria de risco de terceiros no domínio das TIC nos diferentes setores financeiros, designadamente desenvolvendo boas práticas para a apreciação das práticas e dos controlos de gestão do risco associado às TIC, das medidas de atenuação e da resposta aos incidentes nesse contexto.

2. As AES devem, através do Comité Conjunto, apresentar quinquenalmente um relatório conjunto confidencial ao Parlamento Europeu, ao Conselho e à Comissão que resuma as conclusões dos debates relevantes com as autoridades dos países terceiros referidos no n.º 1, centrados na evolução do risco de terceiros no domínio das TIC e nas suas implicações para a estabilidade financeira, a integridade do mercado, a proteção dos investidores ou o funcionamento do mercado único.

CAPÍTULO VI

DISPOSIÇÕES EM MATÉRIA DE PARTILHA DE INFORMAÇÕES

Artigo 40.º

Disposições em matéria de partilha de informações específicas e sensíveis relativas a ciberataques

1. As entidades financeiras podem proceder ao intercâmbio entre si de informações específicas e sensíveis relativas a ciberataques, nomeadamente indicadores de comprometimento dos sistemas ou dos dados, táticas, técnicas e procedimentos, alertas de cibersegurança e ferramentas de configuração, na medida em que essa partilha de informações específicas e sensíveis:

(a) Tenha como objetivo melhorar a resiliência operacional digital das entidades financeiras, em especial através da sensibilização em relação às ciberameaças, limitando ou impedindo a capacidade de disseminação das ciberameaças, apoiando o leque de capacidades defensivas das entidades financeiras, as técnicas de deteção de ameaças, as estratégias de atenuação ou as fases de resposta e recuperação;

(b) Ocorra no seio de comunidades de entidades financeiras de confiança;

(c) Seja implementada através de disposições em matéria de partilha de informações que protejam a natureza potencialmente sensível das informações partilhadas e sejam regidas por regras de conduta que respeitem totalmente a confidencialidade empresarial, a proteção dos dados pessoais[48] e as orientações sobre a política de concorrência[49].

2. Para efeitos do n.º 1, alínea c), as disposições em matéria de partilha de informações devem definir as condições de participação e, se for caso disso, os pormenores do envolvimento das autoridades públicas e a capacidade em que estas últimas podem estar associadas às disposições em matéria de partilha de informações, bem como os elementos operacionais, nomeadamente a utilização de plataformas TIC dedicadas.

3. As entidades financeiras devem notificar as autoridades competentes da sua participação nas disposições em matéria de partilha de informações referidas no n.º 1, após validação dessa mesma participação ou, quando aplicável, após a cessação da sua participação, assim que produza efeitos.

CAPÍTULO VII

AUTORIDADES COMPETENTES

Artigo 41.º
Autoridades competentes

Sem prejuízo das disposições sobre o quadro de fiscalização aplicável às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas a que se refere a secção II do capítulo V do presente regulamento, o cumprimento das obrigações previstas no presente regulamento deve ser assegurado pelas seguintes autoridades competentes em conformidade com os poderes conferidos pelos respetivos atos jurídicos:

(a) No caso das instituições de crédito, a autoridade competente designada em conformidade com o artigo 4.º da Diretiva 2013/36/UE, sem prejuízo das atribuições específicas conferidas ao BCE pelo Regulamento (UE) n.º 1024/2013;

[48] Em conformidade com o 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 e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados) (JO L 119 de 4.5.2016, p. 1).

[49] Comunicação da Comissão – Orientações sobre a aplicação do artigo 101.º do Tratado sobre o Funcionamento da União Europeia aos acordos de cooperação horizontal, 2011/C 11/01.

(b) No caso dos prestadores de serviços de pagamento, a autoridade competente designada em conformidade com o artigo 22.º da Diretiva (UE) 2015/2366;

(c) No caso das instituições de pagamento eletrónico, a autoridade competente designada em conformidade com o artigo 37.º da Diretiva 2009/110/CE;

(d) No caso das empresas de investimento, a autoridade competente designada em conformidade com o artigo 4.º da Diretiva (UE) 2019/2034;

(e) No caso dos prestadores de serviços de criptoativos, emitentes de criptoativos, emitentes de criptofichas referenciadas a ativos e emitentes de criptofichas referenciadas a ativos significativas, a autoridade competente designada em conformidade com o artigo 3.º, n.º 1, alínea ee), primeiro travessão, do [*Regulamento (UE) 20xx (Regulamento MICA)*];

(f) No caso das centrais de valores mobiliários, a autoridade competente designada em conformidade com o artigo 11.º do Regulamento (UE) n.º 909/2014;

(g) No caso das contrapartes centrais, a autoridade competente designada em conformidade com o artigo 22.º do Regulamento (UE) n.º 648/2012;

(h) No caso das plataformas de negociação e dos prestadores de serviços de comunicação de dados, a autoridade competente designada em conformidade com o artigo 67.º da Diretiva 2014/65/UE;

(i) No caso dos repositórios de transações, a autoridade competente designada em conformidade com o artigo 55.º do Regulamento (UE) n.º 648/2012;

(j) No caso dos gestores de fundos de investimento alternativos, a autoridade competente designada em conformidade com o artigo 44.º da Diretiva 2011/61/UE;

(k) No caso das sociedades gestoras, a autoridade competente designada em conformidade com o artigo 97.º da Diretiva 2009/65/CE;

(l) No caso das empresas de seguros e resseguros, a autoridade competente designada em conformidade com o artigo 30.º da Diretiva 2009/138/CE;

(m) No caso dos mediadores de seguros, mediadores de resseguros e mediadores de seguros a título acessório, a autoridade competente designada em conformidade com o artigo 12.º da Diretiva (UE) 2016/97;

(n) No caso das instituições de realização de planos de pensões profissionais, a autoridade competente designada em conformidade com o artigo 47.º da Diretiva 2016/2341;

(o) No caso das agências de notação de risco, a autoridade competente designada em conformidade com o artigo 21.º do Regulamento (CE) n.º 1060/2009;

(p) No caso dos revisores oficiais de contas e sociedades de revisores oficiais de contas, a autoridade competente designada em conformidade com o artigo 3.º, n.º 2, e com o artigo 32.º da Diretiva 2006/43/CE;

(q) No caso dos administradores de índices de referência críticos, a autoridade competente designada em conformidade com os artigos 40.º e 41.º do *Regulamento xx/202x*;

(r) No caso dos prestadores de serviços de financiamento colaborativo, a autoridade competente designada em conformidade com o *artigo x.º do Regulamento xx/202x*;

(s) No caso dos repositórios de titularizações, a autoridade competente designada em conformidade com o artigo 10.º e o artigo 14.º, n.º 1, do Regulamento (UE) 2017/2402.

Artigo 42.º

Cooperação com as estruturas e autoridades estabelecidas pela Diretiva (UE) 2016/1148

1. Para fomentar a cooperação e permitir intercâmbios em matéria de supervisão entre as autoridades competentes designadas nos termos do presente regulamento e o Grupo de Cooperação estabelecido pelo artigo 11.º da Diretiva (UE) 2016/1148, as AES e as autoridades competentes podem solicitar a sua participação nos trabalhos do Grupo de Cooperação.

2. As autoridades competentes podem consultar, se for caso disso, o ponto de contacto único e as equipas de resposta a incidentes de segurança informática nacionais referidas respetivamente nos artigos 8.º e 9.º da Diretiva (UE) 2016/1148.

Artigo 43.º

Exercícios, comunicação e cooperação transetorial no domínio financeiro

1. As AES, através do Comité Conjunto e em colaboração com as autoridades competentes, o BCE e CERS, podem estabelecer mecanismos que permitam a partilha de práticas eficazes entre os setores financeiros, para melhorar o conhecimento da situação e identificar as vulnerabilidades e os riscos cibernéticos comuns entre setores.

   Podem também desenvolver exercícios de gestão de crises e contingência que envolvam cenários de ciberataques com vista a desenvolver canais de comunicação e, gradualmente, permitir uma resposta coordenada eficaz a nível da UE caso ocorra um incidente grave transfronteiriço relacionado com as TIC ou caso uma ameaça conexa possa ter um impacto sistémico no setor financeiro da União como um todo.

   Estes exercícios podem igualmente, se for caso disso, testar as dependências do setor financeiro em relação a outros setores económicos.

2. As autoridades competentes, a EBA, a ESMA ou a EIOPA e o BCE devem cooperar estreitamente entre si e proceder ao intercâmbio de informações para efeitos do cumprimento das suas obrigações nos termos dos artigos 42.º a 48.º. As autoridades competentes devem coordenar estreitamente a sua supervisão de modo a identificarem e corrigirem as infrações ao presente regulamento, desenvolverem e promoverem as boas práticas, facilitarem a colaboração, promoverem a coerência da interpretação e facultarem avaliações transjurisdicionais em caso de diferendo.

Artigo 44.º

Sanções administrativas e medidas corretivas

1. As autoridades competentes devem estar investidas de todos os poderes de supervisão, investigação e sancionatórios necessários para cumprirem as suas obrigações ao abrigo do presente regulamento.

2. Os poderes referidos no n.º 1 incluem, pelo menos, os poderes de:

   (a) Aceder a qualquer documento ou a quaisquer dados, independentemente da respetiva forma, que a autoridade competente considere relevantes para o exercício das suas funções, e receber ou obter uma cópia dos mesmos;

(b) Conduzir investigações ou inspeções no local;

(c) Exigir a aplicação de medidas corretivas em caso de violação dos requisitos do presente regulamento.

3. Sem prejuízo do direito dos Estados-Membros a imporem sanções penais de acordo com o artigo 46.º, os Estados-Membros devem estipular regras que estabeleçam sanções administrativas e medidas corretivas adequadas em caso de violação do presente regulamento e assegurar a sua aplicação efetiva.

As referidas sanções ou medidas devem ser eficazes, proporcionadas e dissuasivas.

4. Os Estados-Membros devem conferir às autoridades competentes o poder para aplicar, pelo menos, as seguintes sanções administrativas e medidas corretivas em caso de violação do presente regulamento:

(a) Uma injunção que exija à pessoa singular ou coletiva que cesse a conduta em causa e se abstenha de a repetir;

(b) Exigir a cessação temporária ou permanente de qualquer prática ou conduta que a autoridade competente considere contrária às disposições do presente regulamento e evitar a sua repetição;

(c) Adotar qualquer tipo de medida, nomeadamente de natureza pecuniária, que vise assegurar que as entidades financeiras continuem a cumprir os requisitos legais;

(d) Exigir, na medida em que o direito nacional o permita, os registos existentes do tráfego de dados detidos por um operador de telecomunicações, se houver motivos razoáveis para suspeitar de uma violação do presente regulamento e se esses registos puderem ser relevantes para uma investigação sobre essas violações; e

(e) Emitir comunicações ao público, incluindo comunicados públicos, que indiquem a identidade da pessoa singular ou coletiva e a natureza da violação.

5. Quando as disposições a que se refere o n.º 2, alínea c), e o n.º 4 sejam aplicáveis a pessoas coletivas, os Estados-Membros conferem às autoridades competentes o poder de aplicarem as sanções administrativas e medidas corretivas, sob reserva das condições estabelecidas no direito nacional, aos membros do órgão de administração e a outras pessoas que, nos termos do direito nacional, sejam responsáveis pela violação.

6. Os Estados-Membros devem assegurar que qualquer decisão relativa à aplicação das sanções administrativas ou medidas corretivas estabelecidas no n.º 2, alínea c), é devidamente fundamentada e passível de recurso.

Artigo 45.º

Exercício do poder de aplicar sanções administrativas e medidas corretivas

1. As autoridades competentes devem exercer os poderes para impor as sanções administrativas e as medidas corretivas a que se refere o artigo 44.º em conformidade com os respetivos regimes jurídicos nacionais, se for caso disso:

(a) Diretamente;

(b) Em colaboração com outras autoridades;

(c) Sob a sua responsabilidade, por delegação noutras autoridades;

(d) Mediante pedido dirigido às autoridades judiciais competentes.

2. Ao determinarem o tipo e o nível de uma sanção administrativa ou medida corretiva aplicada nos termos do artigo 44.º, as autoridades competentes devem ter em conta a medida em que a violação tem caráter doloso ou resulta de negligência, e todas as outras circunstâncias relevantes, incluindo, se for caso disso:

(a) O caráter material, a gravidade e a duração da violação;

(b) O grau de responsabilidade da pessoa singular ou coletiva responsável pela violação;

(c) A capacidade financeira da pessoa singular ou coletiva responsável;

(d) O montante dos lucros obtidos ou dos prejuízos evitados pela pessoa singular ou coletiva responsável, na medida em que possam ser determinados;

(e) Os prejuízos causados a terceiros pela violação, na medida em que possam ser determinados;

(f) O nível de colaboração com a autoridade competente da pessoa singular ou coletiva responsável, sem prejuízo da necessidade de assegurar a restituição dos lucros ganhos ou das perdas evitadas por essa pessoa;

(g) Anteriores violações por parte da pessoa singular ou coletiva responsável.

Artigo 46.º
Sanções penais

1. Os Estados-Membros podem decidir não estabelecer um regime de sanções administrativas ou medidas corretivas para as violações que estejam sujeitas a sanções penais nos termos do seu direito nacional.

2. Caso tenham decidido estabelecer sanções penais por violações do presente regulamento, os Estados-Membros devem assegurar a existência de medidas adequadas para que as autoridades competentes disponham de todos os poderes necessários para assegurar a ligação com as autoridades judiciais, as autoridades competentes para o exercício da ação penal ou as autoridades de justiça penal na sua jurisdição, a fim de receberem informações específicas relacionadas com as investigações ou processos penais instaurados pelas violações do presente regulamento, e fornecerem essas mesmas informações a outras autoridades competentes, bem como à EBA, à ESMA ou à EIOPA, em cumprimento das suas obrigações de cooperação para efeitos do presente regulamento.

Artigo 47.º
Deveres de notificação

Os Estados-Membros devem notificar as disposições legislativas, regulamentares e administrativas que dão execução ao presente capítulo, incluindo quaisquer disposições de direito penal aplicáveis, à Comissão, à ESMA, à EBA e à EIOPA até [*Serviço das Publicações: inserir a data correspondente a um ano após a data de entrada em vigor*]. Os Estados-Membros devem notificar à Comissão, à ESMA, à EBA e à EIOPA, sem demora injustificada, quaisquer alterações subsequentes dessas disposições.

Artigo 48.º

Publicação das sanções administrativas

1. As autoridades competentes devem publicar nos respetivos sítios Web oficiais, sem demora injustificada, qualquer decisão que imponha uma sanção administrativa em relação à qual não haja possibilidade de apresentar recurso depois de o destinatário da sanção ter sido notificado dessa decisão.

2. A publicação a que se refere o n.º 1 deve incluir pelo menos informações sobre o tipo e a natureza da violação, a identidade das pessoas responsáveis e as sanções aplicadas.

3. Quando a autoridade competente, no seguimento de uma avaliação casuística, considerar que a publicação da identidade, no caso das pessoas coletivas, ou da identidade e dos dados pessoais, no caso de pessoas singulares, pode ser desproporcionada, pôr em perigo a estabilidade dos mercados financeiros ou a condução de uma investigação penal em curso, ou provocar, na medida em que estes possam ser determinados, danos desproporcionados para a pessoa envolvida, a referida autoridade deve adotar uma das seguintes soluções em relação à decisão que impõe uma sanção administrativa:

   (a) Adiar a sua publicação até ao momento em que todas as razões para a não publicação deixem de existir;

   (b) Publicar a decisão numa base anónima, em conformidade com o direito nacional; ou

   (c) Abster-se de publicar a decisão, quando considerar que as opções indicadas nas alíneas a) e b) são insuficientes para garantir a inexistência de perigo para a estabilidade dos mercados financeiros ou quando essa publicação não seja proporcionada à indulgência da sanção imposta.

4. Caso se decida pela publicação anónima de uma sanção administrativa, em conformidade com o n.º 3, alínea b), é possível adiar a publicação dos dados relevantes.

5. Caso as autoridades competentes publiquem as decisões de aplicação de sanções administrativas em instância de recurso perante as autoridades judiciais relevantes, as referidas autoridades devem publicar imediatamente no seu sítio Web oficial essa informação e, numa fase posterior, quaisquer informações conexas subsequentes sobre o resultado de tal recurso. É também publicada qualquer decisão judicial que anule uma decisão de aplicação de uma sanção administrativa.

6. As autoridades competentes devem assegurar que todas as publicações referidas nos n.os 1 a 4 permanecem no seu sítio Web oficial durante pelo menos cinco anos a contar da sua publicação. Os dados pessoais contidos na publicação apenas são mantidos no sítio Web oficial da autoridade competente durante o período necessário em conformidade com as regras aplicáveis em matéria de proteção dos dados.

Artigo 49.º
Sigilo profissional

1. As informações confidenciais recebidas, trocadas e transmitidas ao abrigo do presente regulamento ficam sujeitas às condições de sigilo profissional estabelecidas no n.º 2.

2. Todas as pessoas que trabalhem ou tenham trabalhado por conta de autoridades competentes ao abrigo do presente regulamento ou para qualquer autoridade, empresa do mercado, pessoa singular ou coletiva na qual essas autoridades competentes tenham delegado as suas competências, incluindo os auditores ou peritos mandatados por essas autoridades, ficam sujeitas à obrigação de sigilo profissional.

3. As informações abrangidas pelo sigilo profissional não podem ser comunicadas a qualquer outra pessoa ou autoridade, exceto por força de disposições do direito da União ou do direito nacional.

4. Todas as informações trocadas entre as autoridades competentes nos termos do presente regulamento que digam respeito a condições comerciais ou operacionais ou a outros assuntos económicos ou pessoais são consideradas confidenciais e ficam sujeitas ao dever de sigilo profissional, salvo se a autoridade competente declarar, no momento da sua comunicação, que a informação em causa pode ser divulgada, ou se a divulgação for necessária para efeitos de processos judiciais.

CAPÍTULO VIII

ATOS DELEGADOS

Artigo 50.º
Exercício da delegação

1. O poder de adotar atos delegados é conferido à Comissão nas condições estabelecidas no presente artigo.

2. O poder de adotar atos delegados referido no artigo 28.º, n.º 3, e no artigo 38.º, n.º 2, é conferido à Comissão por um prazo de cinco anos a contar de [Serviço das Publicações: inserir a data correspondente a cinco anos após a data de entrada em vigor do presente regulamento].

3. A delegação de poderes referida no artigo 28.º, n.º 3, e no artigo 38.º, n.º 2, pode ser revogada em qualquer momento pelo Parlamento Europeu ou pelo Conselho. A decisão de revogação põe termo à delegação de poderes nela especificada. A decisão de revogação produz efeitos no dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia* ou numa data posterior nela própria especificada. A decisão de revogação não afeta os atos delegados já em vigor.

4. Antes de adotar um ato delegado, a Comissão consulta os peritos designados por cada Estado-Membro de acordo com os princípios estabelecidos no Acordo Interinstitucional «Legislar Melhor», de 13 de abril de 2016.

5. Logo que adotar um ato delegado, a Comissão notifica-o simultaneamente ao Parlamento Europeu e ao Conselho.

6. Os atos delegados adotados em aplicação do disposto no artigo 28.º, n.º 3, e no artigo 38.º, n.º 2, só entram em vigor se nem o Parlamento Europeu nem o Conselho formularem objeções no prazo de dois meses a contar da notificação do ato a estas duas instituições ou se, antes do termo desse prazo, tanto o Parlamento Europeu como o Conselho informarem a Comissão de que não formularão objeções. Esse prazo é prorrogado por dois meses por iniciativa do Parlamento Europeu ou do Conselho.

CAPÍTULO IX

DISPOSIÇÕES TRANSITÓRIAS E FINAIS

SECÇÃO I

Artigo 51.º

Cláusula de reexame

Até [*Serviço das Publicações: inserir a data correspondente a cinco anos após a data de entrada em vigor do presente regulamento*], a Comissão deve, após consulta da EBA, da ESMA, da EIOPA e do CERS, se for caso disso, proceder a um reexame e apresentar um relatório ao Parlamento Europeu e ao Conselho, acompanhado, se necessário, de uma proposta legislativa, relativo aos critérios aplicáveis à designação das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas que constam do artigo 28.º, n.º 2.

SECÇÃO II

ALTERAÇÕES

Artigo 52.º

Alterações do Regulamento (CE) n.º 1060/2009

No anexo I do Regulamento (CE) n.º 1060/2009, o primeiro parágrafo do ponto 4 da secção A passa a ter a seguinte redação:

«As agências de notação de risco devem aplicar procedimentos administrativos e contabilísticos corretos e mecanismos de controlo interno e procedimentos eficazes para a avaliação do risco, bem como mecanismos eficazes de controlo e salvaguarda dos seus sistemas de gestão das TIC, de acordo com o Regulamento (UE) 2021/xx do Parlamento Europeu e do Conselho* [DORA].

* Regulamento (UE) 2021/xx do Parlamento Europeu e do Conselho [...] (JO L XX de DD.MM.AAAA, p. X).».

Artigo 53.º

Alterações do Regulamento (UE) n.º 648/2012

O Regulamento (UE) n.º 648/2012 é alterado do seguinte modo:

(1) O artigo 26.º é alterado do seguinte modo:

(a) O n.º 3 passa a ter a seguinte redação:

«3. As CCP devem manter e utilizar uma estrutura organizativa que garanta a continuidade e o correto funcionamento dos seus serviços e atividades. Para esse efeito, devem pôr em prática sistemas, recursos e procedimentos adequados e proporcionados, nomeadamente sistemas de TIC geridos em conformidade com o Regulamento (UE) 2021/xx do Parlamento Europeu e do Conselho* [DORA].

* Regulamento (UE) 2021/xx do Parlamento Europeu e do Conselho [...] (JO L XX de DD.MM.AAAA, p. X).»;

(b) É suprimido o n.º 6;

(2) O artigo 34.º é alterado do seguinte modo:

(a) O n.º 1 passa a ter a seguinte redação:

«1. As CCP devem estabelecer, aplicar e manter uma política adequada de continuidade das atividades e planos de recuperação em caso de catástrofe, que devem incluir os planos de continuidade das atividades no domínio das TIC e os planos de recuperação em caso de catástrofe no domínio das TIC estabelecidos em conformidade com o Regulamento (UE) 2021/xx [DORA], destinados a garantir a continuidade das suas funções, a recuperação atempada das operações e o cumprimento das suas obrigações.»;

(b) No n.º 3, o primeiro parágrafo passa a ter a seguinte redação:

«A fim de assegurar uma aplicação coerente do presente artigo, a ESMA, após consulta dos membros do SEBC, redige projetos de normas técnicas de regulamentação destinadas a especificar o teor e os requisitos mínimos da política de continuidade das atividades e do plano de recuperação, excluindo os planos de continuidade das atividades no domínio das TIC e os planos de recuperação em caso de catástrofe no domínio das TIC.»;

(3) No artigo 56.º, o primeiro parágrafo do n.º 3 passa a ter a seguinte redação:

«3. A fim de assegurar uma aplicação coerente do presente artigo, a ESMA redige projetos de normas técnicas de regulamentação destinadas a especificar os pormenores, que não sejam relativos aos requisitos relacionados com a gestão do risco associado às TIC, dos pedidos de registo a que se refere o n.º 1.»;

(4) No artigo 79.º, os n.os 1 e 2 passam a ter a seguinte redação:

«1. Os repositórios de transações devem identificar as fontes de risco operacional e limitar esse risco também através do desenvolvimento de sistemas, controlos e procedimentos adequados, incluindo sistemas no domínio das TIC geridos em conformidade com o Regulamento (UE) 2021/xx *[DORA]*.

2. Os repositórios de transações devem estabelecer, aplicar e manter uma política adequada de continuidade das atividades e planos de recuperação em caso de catástrofe, incluindo os planos de continuidade das atividades no domínio das TIC e os planos de recuperação em caso de catástrofe no domínio das TIC estabelecidos em conformidade com o Regulamento (UE) 2021/xx *[DORA]*, destinados a garantir a manutenção das suas

funções, a recuperação atempada das operações e o cumprimento das suas obrigações.»;

(5) No artigo 80.º, é suprimido o n.º 1.

Artigo 54.º

Alterações do Regulamento (UE) n.º 909/2014

O artigo 45.º do Regulamento (UE) n.º 909/2014 é alterado do seguinte modo:

(1) O n.º 1 passa a ter a seguinte redação:

«1. As CSD identificam as fontes de risco operacional, internas e externas, e minimizam o seu impacto também por meio de ferramentas, de processos e de políticas adequados no domínio das TIC criados e geridos em conformidade com o Regulamento (UE) 2021/xx do Parlamento Europeu e do Conselho* [*DORA*], bem como por meio de quaisquer outras ferramentas, controlos e procedimentos relevantes adequados para outros tipos de risco operacional, designadamente para todos os sistemas de liquidação de valores mobiliários que gerem.

* Regulamento (UE) 2021/xx do Parlamento Europeu e do Conselho [...] (JO L XX de DD.MM.AAAA, p. X).»;

(2) O n.º 2 é suprimido;

(3) Os n.os 3 e 4 passam a ter a seguinte redação:

«3. Para os serviços que prestam, bem como para cada um dos sistemas de liquidação de valores mobiliários que gerem, as CSD estabelecem, executam e mantêm uma política adequada de continuidade das atividades e planos de recuperação na sequência de catástrofes, incluindo os planos de continuidade das atividades no domínio das TIC e os planos de recuperação em caso de catástrofe no domínio das TIC estabelecidos em conformidade com o Regulamento (UE) 2021/xx [DORA], a fim de garantir a manutenção dos seus serviços, a recuperação atempada das operações e o cumprimento das obrigações da CSD em situações que representem um risco significativo de perturbação das operações.

4. O plano a que se refere o n.º 3 prevê a recuperação da totalidade das transações e das posições dos participantes no momento do incidente, de modo a que os participantes da CSD possam continuar a funcionar de forma segura e completar as liquidações nas datas previstas, inclusive garantindo que os sistemas críticos de tecnologias de informação possam retomar as operações a partir do momento do incidente, tal como previsto no artigo 11.º, n.os 5 e 7, do Regulamento (UE) 2021/xx [DORA].»;

(4) No n.º 6, o primeiro parágrafo passa a ter a seguinte redação:

«As CSD identificam, controlam e gerem os riscos que poderão representar para as suas atividades os participantes-chave nos sistemas de liquidação de valores mobiliários que gerem, bem como os prestadores de serviços e fornecedores e outras CSD ou infraestruturas de mercado. Quando tal lhes for solicitado, as CSD prestam às autoridades competentes e às autoridades relevantes informações sobre os riscos dessa natureza que tenham identificado. As CSD informam igualmente sem demora a autoridade competente e as autoridades relevantes de quaisquer incidentes

operacionais, que não estejam relacionados com os riscos associados às TIC, resultantes desses riscos.»;

(5) No n.º 7, o primeiro parágrafo passa a ter a seguinte redação:

«A ESMA elabora, em estreita cooperação com os membros do SEBC, projetos de normas técnicas de regulamentação que especifiquem os riscos operacionais a que se referem os n.os 1 e 6, que não sejam riscos associados às TIC, e os métodos a utilizar para testar, tratar ou reduzir esses riscos, incluindo a política de continuidade das atividades e os planos de recuperação na sequência de catástrofes a que se referem os n.os 3 e 4, bem como os métodos de avaliação dos mesmos.».

Artigo 55.º

Alterações do Regulamento (UE) n.º 600/2014

O Regulamento (UE) n.º 600/2014 é alterado do seguinte modo:

(1) O artigo 27.º-G é alterado do seguinte modo:

(a) O n.º 4 é suprimido;

(b) O n.º 8, alínea c), passa a ter a seguinte redação:

(c) «c) Os requisitos concretos em matéria de organização estabelecidos nos n.os 3 e 5.»;

(2) O artigo 27.º-H é alterado do seguinte modo:

(a) O n.º 5 é suprimido;

(b) O n.º 8, alínea e), passa a ter a seguinte redação:

«e) Os requisitos concretos em matéria de organização estabelecidos no n.º 4.»;

(3) O artigo 27.º-I é alterado do seguinte modo:

(a) O n.º 3 é suprimido;

(b) O n.º 5, alínea b), passa a ter a seguinte redação:

«b) Os requisitos concretos em matéria de organização estabelecidos nos n.os 2 e 4.».

Artigo 56.º

Entrada em vigor e aplicação

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é aplicável a partir de [*Serviço das Publicações: inserir a data correspondente a 12 meses após a data de entrada em vigor*].

Todavia, os artigos 23.º e 24.º são aplicáveis a partir de [*Serviço das Publicações: inserir a data correspondente a 36 meses após a data de entrada em vigor do presente regulamento*].

O presente regulamento é vinculativo em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em

Pelo Parlamento Europeu	*Pelo Conselho*
O Presidente	*O Presidente*

FICHA FINANCEIRA LEGISLATIVA

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

1.2. Domínio(s) de intervenção abrangido(s)

1.3. Natureza da proposta/iniciativa

1.4. Objetivo(s)

1.5. Justificação da proposta/iniciativa

1.6. Duração e impacto financeiro da proposta/iniciativa

1.7. Modalidade(s) de gestão prevista(s)

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e comunicação de informações

2.2. Sistema(s) de gestão e de controlo

2.3. Medidas de prevenção de fraudes e irregularidades

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(ais) de despesas envolvida(s)

3.2. Impacto estimado nas despesas

3.2.1. Síntese do impacto estimado nas despesas

3.2.2. Impacto estimado nas dotações

3.2.3. Impacto estimado nos recursos humanos

3.2.4. Compatibilidade com o atual quadro financeiro plurianual

3.2.5. Participação de terceiros no financiamento

3.3. Impacto estimado nas receitas

Anexo

Pressupostos gerais

Poderes de fiscalização

FICHA FINANCEIRA LEGISLATIVA «AGÊNCIAS»

1. CONTEXTO DA PROPOSTA/INICIATIVA

1.1. Denominação da proposta/iniciativa

Proposta de Regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro

1.2. Domínio(s) de intervenção abrangido(s)

Domínio de intervenção: Estabilidade financeira, serviços financeiros e união de mercados de capitais

Atividade: Resiliência operacional digital

1.3. A proposta refere-se a:

☑ **uma nova ação**

☐ **uma nova ação na sequência de um projeto-piloto/ação preparatória**[50]

☐ **uma prorrogação de uma ação existente**

☐ **uma fusão de uma ou mais ações noutra/numa nova ação**

1.4. Objetivo(s)

1.4.1. Objetivo(s) geral(is)

O objetivo geral da iniciativa consiste em fortalecer a resiliência operacional digital das entidades do setor financeiro da UE através da simplificação e atualização das regras e da introdução de novos requisitos quando existam lacunas. Serviria também para melhorar o conjunto único de regras na sua dimensão digital.

O objetivo global pode ser estruturado em três objetivos gerais: 1) reduzir o risco de perturbação e instabilidade financeiras, 2) reduzir o encargo administrativo e aumentar a eficácia da supervisão e 3) reforçar a proteção dos consumidores e dos investidores.

1.4.2. Objetivo(s) específico(s)

A proposta tem os seguintes objetivos específicos:

Dar uma resposta mais abrangente aos riscos associados às tecnologias da informação e comunicação («TIC») e reforçar o nível global de resiliência digital do setor financeiro;

Simplificar a comunicação de incidentes relacionados com as TIC e dar resposta à sobreposição de requisitos de comunicação de informações;

Permitir o acesso das autoridades de supervisão financeira a informações sobre incidentes relacionados com as TIC;

[50] Como referidos no artigo 58.º, n.º 2, alíneas a) ou b), do Regulamento Financeiro.

Assegurar que as entidades financeiras abrangidas pela presente proposta avaliam a eficácia das suas medidas preventivas e de resiliência e identificam as vulnerabilidades relacionadas com as TIC; Reduzir a fragmentação do mercado único e viabilizar a aceitação transfronteiriça dos resultados dos testes. Reforçar as salvaguardas contratuais das entidades financeiras quando utilizam serviços no domínio das TIC, incluindo regras de subcontratação (que regem a monitorização das entidades terceiras prestadoras de serviços no domínio das TIC); Viabilizar a fiscalização das atividades das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas; Incentivar o intercâmbio de informações sobre as ameaças ao setor financeiro.

1.4.3. Resultados e impacto esperados

Especificar os efeitos que a proposta/iniciativa poderá ter nos beneficiários/na população visada.

Uma lei sobre a resiliência operacional digital para o setor financeiro poderia assegurar um quadro abrangente que englobasse todos os aspetos da resiliência operacional digital e seria eficaz para aumentar a resiliência operacional global do setor financeiro. Poderia salvaguardar a clareza e a coerência do conjunto único de regras.

Poderia também estabelecer a ligação com a Diretiva SRI e tornar a sua revisão mais clara e mais coerente. Poderia clarificar as diferentes regras sobre resiliência operacional digital que deverão ser cumpridas pelas entidades financeiras, em especial quando forem titulares de várias autorizações e operarem em diferentes mercados dentro da UE.

1.4.4. Indicadores de resultados

Especificar os indicadores que permitem acompanhar os progressos e os resultados.

Possíveis indicadores:

Número de incidentes relacionados com as TIC no setor financeiro da UE e o respetivo impacto

Número de incidentes graves relacionados com as TIC comunicados às autoridades de supervisão prudencial

Número de entidades financeiras que seriam obrigadas a realizar testes de penetração nos sistemas motivados por ameaças

Número de entidades financeiras que utilizam cláusulas contratuais normalizadas para celebrarem contratos com entidades terceiras prestadoras de serviços no domínio das TIC

Número de entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas fiscalizadas pelas AES ou pelas autoridades de supervisão prudencial

Número de entidades financeiras que participam em soluções de partilha de informações sensíveis sobre ameaças

Número de autoridades que recebem relatórios sobre os mesmos incidentes relacionados com as TIC

Número de testes de penetração nos sistemas com origem transfronteiriça

1.5. Justificação da proposta/iniciativa

1.5.1. Necessidade(s) a satisfazer a curto ou a longo prazo, incluindo um calendário pormenorizado de aplicação da iniciativa

O setor financeiro depende em grande medida das tecnologias da informação e comunicação (TIC). Apesar dos progressos significativos alcançados através das políticas e iniciativas legislativas específicas a nível nacional e europeu, os riscos associados às TIC constituem ainda um desafio para a resiliência operacional, o desempenho e a estabilidade do sistema financeiro da UE. A reforma que se seguiu à crise financeira de 2008 reforçou sobretudo a resiliência financeira do setor financeiro da UE e visava salvaguardar a competitividade e estabilidade da UE do ponto de vista económico, prudencial e da conduta do mercado. A segurança e a resiliência operacional digital global no domínio das TIC fazem parte do risco operacional, mas têm sido objeto de uma menor atenção na agenda regulamentar no período pós-crise, tendo-se desenvolvido apenas em alguns domínios das políticas e da

regulamentação dos mercados financeiros da UE ou apenas em alguns Estados-Membros. Tudo isto se traduz nos desafios seguintes, que a proposta procura abordar:

O quadro jurídico da UE que abrange o risco associado às TIC e a resiliência operacional no setor financeiro está fragmentado e não é totalmente coerente.

A falta de requisitos coerentes relativos à comunicação de incidentes relacionados com as TIC faz com que as autoridades de supervisão tenham uma perspetiva incompleta da natureza, frequência, importância e impacto dos incidentes.

Algumas entidades financeiras deparam-se com requisitos de comunicação de informações complexos, que se sobrepõem e são potencialmente incoerentes, para um mesmo incidente relacionado com as TIC.

Uma partilha de informações e uma cooperação insuficientes no que toca a informações sensíveis relativas a ciberameaças ao nível estratégico, tático e operacional impedem que as entidades financeiras, em termos individuais, avaliem, monitorizem, se defendam e respondam às ciberameaças.

Em certos subsetores financeiros, podem existir vários quadros para testar a resiliência e a penetração nos sistemas, sem coordenação entre si, associados à falta de reconhecimento de resultados a nível transfronteiriço, ao passo que noutros setores pode não existir qualquer quadro para a realização de testes.

O facto de haver falta de supervisão das atividades das entidades financeiras que são prestadas por entidades terceiras prestadoras de serviços no domínio das TIC faz com que as entidades financeiras individualmente, e o sistema financeiro no seu todo, fiquem expostos aos riscos operacionais.

As autoridades de supervisão financeira não estão suficientemente habilitadas nem dispõem das ferramentas necessárias para monitorizar e gerir os riscos de concentração e sistémicos decorrentes da eventual dependência de algumas entidades financeiras de terceiros no domínio das TIC.

1.5.2. Valor acrescentado da participação da União (que pode resultar de diferentes fatores como, por exemplo, ganhos de coordenação, segurança jurídica, maior eficácia ou complementaridades). Para efeitos do presente ponto, entende-se por «valor acrescentado da intervenção da União», o valor resultante da intervenção da União que se acrescenta ao valor que teria sido criado pelos Estados-Membros de forma isolada.

Razões para uma ação a nível europeu (*ex ante*):

A resiliência operacional digital é um assunto de interesse comum para os mercados financeiros da UE. Uma ação ao nível da UE poderia proporcionar mais vantagens e um maior valor do que ações adotadas isoladamente a nível nacional. Se não forem acrescentadas estas disposições operacionais sobre o risco associado às TIC, o conjunto único de regras forneceria as ferramentas necessárias para dar resposta a todos os outros tipos de riscos a nível europeu, mas deixaria de fora os aspetos da resiliência operacional digital ou sujeitá-los-ia a iniciativas fragmentadas e não coordenadas a nível nacional. A proposta proporcionaria segurança jurídica sobre a eventual aplicação, e de que forma, das disposições operacionais digitais, em especial às entidades financeiras transfronteiriças, e eliminaria a necessidade de os Estados-Membros melhorarem em termos individuais as regras, as normas e as expectativas relativas à resiliência operacional e à cibersegurança como resposta à atual cobertura limitada das regras da UE e à natureza genérica da Diretiva SRI.

Valor acrescentado previsto da ação da União (*ex post*): A intervenção da União aumentaria significativamente a eficácia da política, ao passo que também reduziria a complexidade e aliviaria os encargos financeiros e administrativos para todas as entidades financeiras. Harmonizaria uma área da economia que está profundamente interligada e integrada e que já beneficia de um conjunto único de regras e de supervisão. Em termos de comunicação de incidentes relacionados com as TIC, a proposta reduziria os encargos inerentes à comunicação de informações - bem como os custos implícitos - sobre um mesmo incidente relacionado com as TIC a diferentes autoridades nacionais e/ou da UE. Também facilitaria o reconhecimento/aceitação mútuos dos resultados dos testes das entidades que operam a nível transfronteiriço e que estão sujeitas a vários quadros em matéria de testes nos diferentes Estados-Membros.

1.5.3. Lições retiradas de experiências anteriores semelhantes

Nova iniciativa

1.5.4. Compatibilidade com o quadro financeiro plurianual e eventuais sinergias com outros instrumentos adequados

O objetivo da presente proposta é coerente com várias outras políticas e iniciativas em curso na UE, nomeadamente a Diretiva Segurança das Redes e das Informações (SRI) e a Diretiva Infraestruturas Críticas Europeias (ICE). A proposta conservaria os benefícios associados ao quadro horizontal em matéria de cibersegurança ao manter os três subsetores financeiros dentro do âmbito da Diretiva SRI. Ao permanecerem associadas ao ecossistema SRI, as autoridades de supervisão financeira poderiam proceder ao intercâmbio de informações relevantes com as autoridades SRI e participar no Grupo de Cooperação SRI. A proposta não afetaria a Diretiva SRI, iria sim tirar partido dela e colmatar as possíveis lacunas através de uma exceção *lex specialis*. A interação entre o regulamento relativo aos serviços financeiros e a Diretiva SRI continuaria a ser regida por uma cláusula *lex specialis*, isentando assim as entidades financeiras dos requisitos substantivos da Diretiva SRI e evitando sobreposições entre os dois atos. Adicionalmente, a iniciativa é coerente com a Diretiva Infraestruturas Críticas Europeias (ICE), atualmente em processo de revisão para reforçar a proteção e resiliência das infraestruturas críticas contra ameaças não cibernéticas.

Esta proposta não afetaria o Quadro Financeiro Plurianual (QFP). Em primeiro lugar, o quadro de fiscalização das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas será totalmente financiado pelas taxas cobradas a essas entidades; em segundo lugar, as atribuições regulamentares adicionais relacionadas com a resiliência operacional digital confiadas às AES serão asseguradas através da reafetação interna do pessoal existente.

Isto traduzir-se-á numa proposta de aumento do pessoal autorizado da agência durante o futuro processo orçamental anual. A agência continuará a trabalhar no sentido de maximizar sinergias e ganhos de eficiência (através de sistemas de TI, entre outros), e a acompanhar de perto o volume de trabalho adicional associado à presente proposta, que se refletiria no nível de pessoal autorizado solicitado pela agência no processo orçamental anual.

1.5.5. Avaliação das diferentes opções de financiamento disponíveis, incluindo possibilidades de reafetação

Foram consideradas várias opções de financiamento:

Em primeiro lugar, os custos adicionais poderiam ser financiados através do mecanismo de financiamento habitual das AES. Contudo, tal implicaria um aumento substancial do contributo da UE para os recursos financeiros das AES.

Esta opção é escolhida devido aos custos relacionados com as atribuições regulamentares associadas a esta proposta. Na verdade, será pedido às AES que reafetem o pessoal existente com vista ao desenvolvimento de várias normas técnicas. Contudo, os custos adicionais relacionados com a fiscalização das entidades terceiras consideradas críticas não poderiam ser cobertos através da reafetação dos recursos dentro das AES, que também têm outras atribuições para além das previstas na presente proposta, bem como nos termos de outros atos legislativos da União. Além disso, as atribuições de supervisão relacionadas com a resiliência operacional digital exigem conhecimentos técnicos e conhecimentos especializados específicos. Como o atual nível desses recursos nas AES é insuficiente, seriam necessários recursos adicionais.

Por último, de acordo com a proposta, as taxas seriam cobradas às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas objeto de supervisão. Estas

taxas teriam como finalidade cobrir todos os recursos adicionais necessários para que as AES desempenhem as suas novas funções e exerçam os seus novos poderes.

1.6. Duração e impacto financeiro da proposta/iniciativa

☐ **duração limitada**

☐ Proposta/iniciativa válida entre [DD/MM]AAAA e [DD/MM]AAAA

☐ Impacto financeiro no período compreendido entre AAAA e AAAA

☑ **duração ilimitada**

Aplicação com um período de arranque progressivo a partir de 2021

seguido de um período de aplicação a um ritmo de cruzeiro.

1.7. Modalidade(s) de gestão prevista(s)[51]

Gestão direta pela Comissão através de

☐ agências de execução

☐ **Gestão partilhada** com os Estados-Membros

☑ **Gestão indireta** confiando tarefas de execução orçamental:

☐ a organizações internacionais e respetivas agências (a especificar);

☐ ao BEI e ao Fundo Europeu de Investimento;

☑ aos organismos referidos nos artigos 70.º e 71.º;

☐ a organismos de direito público;

☐ a organismos regidos pelo direito privado com uma missão de serviço público na medida em que prestem garantias financeiras adequadas;

☐ a organismos regidos pelo direito privado de um Estado-Membro com a responsabilidade pela execução de uma parceria público-privada e que prestem garantias financeiras adequadas;

☐ a pessoas encarregadas da execução de ações específicas no quadro da PESC por força do título V do Tratado da União Europeia, identificadas no ato de base pertinente.

Observações

N/A

[51] As explicações sobre as modalidades de gestão e as referências ao regulamento financeiro estão disponíveis no sítio BudgWeb: https://myintracomm.ec.europa.eu/budgweb/EN/man/budgmanag/Pages/budgmanag.aspx.

2. MEDIDAS DE GESTÃO

2.1. Disposições em matéria de acompanhamento e comunicação de informações

Especificar a periodicidade e as condições.

Em consonância com as disposições já em vigor, as ESA elaboram regularmente relatórios sobre a sua atividade (incluindo relatórios internos enviados à direção, relatórios aos conselhos e preparação do relatório anual) e são objeto de auditorias por parte do Tribunal de Contas e do Serviço de Auditoria Interna da Comissão quanto à utilização dos seus recursos e ao seu desempenho. O acompanhamento e a prestação de informações sobre as medidas constantes da proposta cumprirão os requisitos já existentes, bem como quaisquer novos requisitos decorrentes da presente proposta.

2.2. Sistema(s) de gestão e de controlo

2.2.1. Justificação da(s) modalidade(s) de gestão, do(s) mecanismo(s) de execução do financiamento, das modalidades de pagamento e da estratégia de controlo propostos

A gestão será indireta através das AES. O mecanismo de financiamento seria executado através da cobrança de taxas às entidades terceiras prestadoras de serviços informáticos críticos visadas.

2.2.2. Informações sobre os riscos identificados e o(s) sistema(s) de controlo interno criado(s) para os atenuar

No que respeita à utilização legal, económica, eficiente e eficaz das dotações resultantes da proposta, não se prevê que esta última suscite novos riscos significativos que não sejam abrangidos por um quadro de controlo interno existente. Contudo, poderá colocar-se um novo desafio relacionado com a cobrança atempada das taxas às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas visadas.

2.2.3. Estimativa e justificação da relação custo-eficácia dos controlos (rácio «custos de controlo/valor dos respetivos fundos geridos») e avaliação dos níveis previstos de risco de erro (no pagamento e no encerramento)

Os sistemas de gestão e de controlo previstos nos regulamentos das AES já estão a ser aplicados. As AES trabalham em estreita colaboração com o Serviço de Auditoria Interna da Comissão, a fim de assegurar que sejam respeitadas normas adequadas em todos os domínios do quadro de controlos internos. Estas disposições serão igualmente aplicáveis no que respeita ao papel das AES conforme definido na presente proposta. Além disso, em cada exercício, o Parlamento Europeu, sob recomendação do Conselho, dá quitação a cada AES pela execução do seu orçamento.

2.3. Medidas de prevenção de fraudes e irregularidades

Especificar as medidas de prevenção e de proteção existentes ou previstas, como, por exemplo, a título da estratégia antifraude.

Para efeitos de combate à fraude, à corrupção e a outros atos ilegais, são aplicáveis às AES, sem restrições, as disposições do Regulamento (UE, Euratom) n.º 883/2013 do Parlamento Europeu e do Conselho, de 11 de setembro de 2013, relativo aos inquéritos efetuados pelo Organismo Europeu de Luta Antifraude (OLAF).

As AES têm uma estratégia de luta antifraude específica e um plano de ação decorrente da mesma. As medidas reforçadas das AES no domínio da luta antifraude serão conformes com as regras e orientações previstas pelo Regulamento Financeiro (medidas antifraude no âmbito da boa gestão financeira), as políticas de prevenção da fraude do OLAF, as disposições da Estratégia Antifraude da Comissão (COM(2011) 376), bem como com o disposto na abordagem comum aplicável às agências descentralizadas da UE (julho de 2012) e no roteiro conexo.

Além disso, os regulamentos que criam as AES, bem como os Regulamentos Financeiros das AES, estabelecem as disposições em matéria de execução e controlo do orçamento das AES e as regras financeiras aplicáveis, designadamente as que visam prevenir fraudes e irregularidades.

3. IMPACTO FINANCEIRO ESTIMADO DA PROPOSTA/INICIATIVA

3.1. Rubrica(s) do quadro financeiro plurianual e rubrica(s) orçamental(ais) de despesas envolvida(s)

Atuais rubricas orçamentais

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

Rubrica do quadro financeiro plurianual	Rubrica orçamental	Type of despesa	Participação			
	Número	DD/DND[52]	dos países da EFTA[53]	dos países candidatos [54]	de países terceiros	na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro

Novas rubricas orçamentais, cuja criação é solicitada

Segundo a ordem das rubricas do quadro financeiro plurianual e das respetivas rubricas orçamentais.

Rubrica do quadro	Rubrica orçamental	Type of despesa	Participação

[52] DD = dotações diferenciadas / DND = dotações não diferenciadas.

[53] EFTA: Associação Europeia de Comércio Livre.

[54] Países candidatos e, se for caso disso, países candidatos potenciais dos Balcãs Ocidentais.

financeiro plurianual	Número	DD/DND	dos países da EFTA	dos países candidatos	de países terceiros	na aceção do artigo 21.º, n.º 2, alínea b), do Regulamento Financeiro

3.2. Impacto estimado nas despesas

3.3. Síntese do impacto estimado nas despesas

Em milhões de EUR (três casas decimais)

Rubrica do quadro financeiro plurianual	Número	Rubrica

DG: <..>			2020	2021	2022	2023	2024	2025	2026	2027	**TOTAL**
	Autorizações	(1)									
	Pagamentos	(2)									
TOTAL das dotações por DG <>	Autorizações										
	Pagamentos										

Rubrica do quadro financeiro plurianual		

Em milhões de EUR (três casas decimais)

		2022	2023	2024	2025	2026	2027	**TOTAL**
DG:								
• Recursos humanos								
• Outras despesas administrativas <>								
TOTAL DG	Dotações							

TOTAL das dotações da RUBRICA do quadro financeiro plurianual	(Total das autorizações = Total dos pagamentos)							

Em milhões de EUR (3 casas decimais) a preços constantes

		2022	**2023**	**2024**	**2025**	**2026**	**2027**	**TOTAL**
TOTAL das dotações da RUBRICA 1 do quadro financeiro plurianual	Autorizações							
	Pagamentos							

3.3.1. Impacto estimado nas dotações

☑ A proposta/iniciativa não acarreta a utilização de dotações operacionais

☐ A proposta/iniciativa acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (3 casas decimais) a preços constantes

Indicar objetivos e realizações ⇩			2022		2023		2024		2025		2026		2027		**TOTAL**	
	REALIZAÇÕES															
	Tipo[55]	Custo médio	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 1[56] ...																
- Realização																
Subtotal objetivo específico n.º 1																
OBJETIVO ESPECÍFICO N.º 2…																
- Realização																
Subtotal objetivo específico n.º 2																
CUSTO TOTAL																

[55] As realizações dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[56] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)…»

3.3.2. Impacto estimado nos recursos humanos

3.3.2.1. Síntese

☐ A proposta/iniciativa não acarreta a utilização de dotações de natureza administrativa

☑ A proposta/iniciativa acarreta a utilização de dotações de natureza administrativa, tal como explicitado seguidamente:

Em milhões de EUR (3 casas decimais) a preços constantes

EBA, EIOPA, ESMA	2022	2023	2024	2025	2026	2027	**TOTAL**
Agentes temporários (graus AD)	1,188	2,381	2,381	2,381	2,381	2,381	13,093
Agentes temporários (Graus AST)	0,238	0,476	0,476	0,476	0,476	0,476	2,618
Agentes contratuais							
Peritos nacionais destacados							
TOTAL	1,426	2,857	2,857	2,857	2,857	2,857	15,711

Necessidades de pessoal (ETI):

EBA, EIOPA, ESMA e AEA	2022	2023	2024	2025	2026	2027	**TOTAL**
Agentes temporários (graus AD) EBA= 5, EIOPA= 5, ESMA= 5	15	15	15	15	15	15	15
Agentes temporários (Graus AST) EBA=1, EIOPA=1, AEA=1	3	3	3	3	3	3	3
Agentes contratuais							
Peritos nacionais destacados							
TOTAL	**18**	**18**	**18**	**18**	**18**	**18**	**18**

3.3.2.2. Necessidades estimadas de recursos humanos para as DG responsáveis

☑ A proposta/iniciativa não acarreta a utilização de recursos humanos.

☐ A proposta/iniciativa acarreta a utilização de recursos humanos, tal como explicitado seguidamente:

As estimativas devem ser expressas em termos de equivalente a tempo completo (ou, no máximo, com uma casa decimal)

		2022	2023	2024	2025	2026	2027
• **Lugares do quadro do pessoal (funcionários e agentes temporários)**							
• **Pessoal externo (em equivalente a tempo inteiro: ETI)**[57]							
XX 01 02 01 (AC, PND, TT da «dotação global»)							
XX 01 02 02 (AC, AL, PND, TT e JPD nas delegações)							
XX 01 04 ***yy***[58]	- na sede[59]						
	- nas delegações						
XX 01 05 02 (AC, END, INT - Pesquisa indireta)							
10 01 05 02 (AC, PND e TT - investigação direta)							
Outra rubrica orçamental (especificar)							
TOTAL							

XX constitui o domínio de intervenção ou título em causa.

As necessidades de recursos humanos serão cobertas pelos efetivos da DG já afetados à gestão da ação e/ou reafetados internamente a nível da DG, complementados, caso necessário, por eventuais dotações adicionais que sejam atribuídas à DG gestora no quadro do processo anual de atribuição e no limite das disponibilidades orçamentais.

Descrição das tarefas a executar:

Funcionários e agentes temporários	
Pessoal externo	

A descrição do cálculo do custo de um ETI deve figurar no anexo V, secção 3.

[57] AC = agente contratual; AL = agente local; PND = perito nacional destacado; TT = trabalhador temporário; JPD = jovem perito nas delegações.

[58] Sublimite para o pessoal externo coberto pelas dotações operacionais (antigas rubricas «BA»).

[59] Principalmente para os fundos estruturais, o Fundo Europeu Agrícola de Desenvolvimento Rural (FEADER) e o Fundo Europeu das Pescas (FEP).

3.3.3. Compatibilidade com o atual quadro financeiro plurianual

☑ A proposta/iniciativa é compatível com o atual quadro financeiro plurianual.

☐ A proposta/iniciativa requer uma reprogramação da rubrica relevante do quadro financeiro plurianual.

☐ A proposta/iniciativa requer a mobilização do Instrumento de Flexibilidade ou a revisão do quadro financeiro plurianual[60].

Explicitar as necessidades, especificando as rubricas orçamentais em causa e as quantias correspondentes. […]

3.3.4. Participação de terceiros no financiamento

☐ A proposta/iniciativa não prevê o cofinanciamento por terceiros.

☑ A proposta/iniciativa prevê o cofinanciamento estimado seguinte:

Em milhões de EUR (três casas decimais)

EBA

	2022	2023	2024	2025	2026	2027	Total
Os custos são integralmente cobertos por taxas cobradas às entidades supervisionadas[61]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL das dotações cofinanciadas	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Total
Os custos são integralmente cobertos por taxas cobradas às entidades supervisionadas[62]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAL das dotações cofinanciadas	1,305	1,811	1,611	1,611	1,611	1,611	9,560

60 Ver artigos 11.º e 17.º do Regulamento (UE, Euratom) n.º 1311/2013 do Conselho que estabelece o quadro financeiro plurianual para o período 2014-2020.

61 100 % do custo total estimado mais o total das contribuições do empregador para o regime de pensões.

62 100 % do custo total estimado mais o total das contribuições do empregador para o regime de pensões.

ESMA

	2022	2023	2024	2025	2026	2027	Total
Os custos são integralmente cobertos por taxas cobradas às entidades supervisionadas[63]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL das dotações cofinanciadas	1,373	1,948	1,748	1,748	1,748	1,748	10,313

3.4. Impacto estimado nas receitas

☑ A proposta/iniciativa não tem impacto financeiro nas receitas.

☐ A proposta/iniciativa tem o impacto financeiro a seguir descrito:

☐ nos recursos próprios

☐ noutras receitas

☐ indicar se as receitas são afetadas a rubricas de despesas

Em milhões de EUR (três casas decimais)

Rubrica orçamental das receitas:	Dotações disponíveis para o atual exercício	Impacto da proposta/iniciativa[64]						
		Ano **N**	Ano **N+1**	Ano **N+2**	Ano **N+3**	Inserir os anos necessários para refletir a duração do impacto (ver ponto 1.6)		
Artigo ….								

Relativamente às diversas receitas «afetadas», especificar a(s) rubrica(s) orçamental(is) de despesas envolvida(s).

[…]

Especificar o método de cálculo do impacto nas receitas.

[…]

63 100 % do custo total estimado mais o total das contribuições do empregador para o regime de pensões.

64 No que diz respeito aos recursos próprios tradicionais (direitos aduaneiros e quotizações sobre o açúcar), as quantias indicadas devem ser apresentadas em termos líquidos, isto é, quantias brutas após dedução de 20 % a título de despesas de cobrança.

ANEXO

Pressupostos gerais

Título I — Despesas com o pessoal

Foram aplicados os seguintes pressupostos específicos no cálculo das despesas com pessoal com base nas necessidades de efetivos identificadas nos termos adiante explicados:

- Os custos associados ao pessoal adicional contratado em 2022 são calculados para um período de 6 meses, tendo em conta o tempo presumivelmente necessário para o recrutamento
- O custo anual médio de um agente temporário é de 150 000 EUR, incluindo o montante de 25 000 EUR a título de custos de «*habillage*» (edifícios, TI, etc.)
- Os coeficientes de correção aplicáveis aos vencimentos do pessoal em Paris (EBA e ESMA) e Frankfurt (EIOPA) são de 117,7 e 99,4, respetivamente
- As contribuições dos empregadores para o regime de pensões dos agentes temporários foram calculadas com base nos vencimentos de base normais incluídos nos custos anuais médios normais, ou seja, 95 660 EUR
- Os agentes temporários adicionais são AD5 e AST.

Título II — Despesas relativas à infraestrutura e de funcionamento

Os custos são calculados multiplicando o número de membros do pessoal pela proporção do ano utilizada pelo custo normal para «*habillage*», ou seja, 25 000 EUR.

Título III — Despesas Operacionais

Os custos são estimados com base nos seguintes pressupostos:

- Os custos com tradução são fixados em 350 000 EUR por ano para cada uma das AES.
- Pressupõe-se que os custos de TI pontuais, correspondentes a 500 000 EUR por AES, serão repartidos em partes iguais pelos anos de 2022 e 2023. Os custos anuais de manutenção para 2024 são estimados em 50 000 EUR por AES
- Os custos anuais de supervisão no local por AES são estimados em 200 000 EUR.

As estimativas acima apresentadas resultam nos seguintes custos por ano:

Rubrica do quadro financeiro plurianual	Número	

Preços constantes

EBA			2022	2023	2024	2025	2026	2027	**TOTAL**
Título 1:	Autorizações	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Pagamentos	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Título 2:	Autorizações	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Pagamentos	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Título 3:	Autorizações	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Pagamentos	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL das dotações para a EBA	Autorizações	= 1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Pagamentos	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA:			2022	2023	2024	2025	2026	2027	**TOTAL**
Título 1:	Autorizações	(1)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
	Pagamentos	(2)	0,430	0,861	0,861	0,861	0,861	0,861	4,735
Título 2:	Autorizações	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Pagamentos	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Título 3:	Autorizações	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Pagamentos	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL das dotações	Autorizações	= 1+1a +3a	1,305	1,811	1,611	1,611	1,611	1,611	9,560

para a EIOPA	Pagamentos	=2+2a +3b	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA:			2022	2023	2024	2025	2026	2027	**TOTAL**
Título 1:	Autorizações	(1)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
	Pagamentos	(2)	0,498	0,998	0,998	0,998	0,998	0,998	5,488
Título 2:	Autorizações	(1a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
	Pagamentos	(2a)	0,075	0,150	0,150	0,150	0,150	0,150	0,825
Título 3:	Autorizações	(3a)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
	Pagamentos	(3b)	0,800	0,800	0,600	0,600	0,600	0,600	4,000
TOTAL das dotações para a ESMA	Autorizações	= 1+1a +3a	1,373	1,948	1,748	1,748	1,748	1,748	10,313
	Pagamentos	=2+2a +3b	1,373	1,948	1,748	1,748	1,748	1,748	10,313

A proposta acarreta a utilização de dotações operacionais, tal como explicitado seguidamente:

Dotações de autorização em milhões de EUR (3 casas decimais) a preços constantes

EBA

Indicar objetivos e realizações			2022		2023		2024		2025		2026		2027			
	REALIZAÇÕES															
⇩	Tipo[65]	Custo médio	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 1[66] Fiscalização direta das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas																
- Realização				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal objetivo específico n.º 1																
OBJETIVO ESPECÍFICO N.º 2…																
- Realização																
Subtotal objetivo específico n.º 2																
CUSTO TOTAL				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

EIOPA

Indicar objetivos e realizações			2022		2023		2024		2025		2026		2027			
	REALIZAÇÕES															
⇩	Tipo[67]	Custo médio	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 1[68] Fiscalização direta das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas																

[65] As realizações dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[66] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)…»

[67] As realizações dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[68] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)…»

- Realização				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal objetivo específico n.º 1																
OBJETIVO ESPECÍFICO N.º 2…																
- Realização																
Subtotal objetivo específico n.º 2																
CUSTO TOTAL				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

ESMA

Indicar objetivos e realizações ⇩			2022		2023		2024		2025		2026		2027			
	REALIZAÇÕES															
	Tipo[69]	Custo médio	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º	Custo	N.º total	Custo total
OBJETIVO ESPECÍFICO N.º 1[70] Fiscalização direta das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas																
- Realização				0,800		0,800		0,600		0,600		0,600		0,600		4,000
Subtotal objetivo específico n.º 1																
OBJETIVO ESPECÍFICO N.º 2…																
- Realização																
Subtotal objetivo específico n.º 2																
CUSTO TOTAL				**0,800**		**0,800**		**0,600**		**0,600**		**0,600**		**0,600**		**4,000**

[69] As realizações dizem respeito aos produtos fornecidos e serviços prestados (exemplo: número de intercâmbios de estudantes financiados, número de quilómetros de estradas construídas, etc.).

[70] Tal como descrito no ponto 1.4.2. «Objetivo(s) específico(s)…»

As atividades de fiscalização são integralmente financiadas por taxas cobradas às entidades fiscalizadas nos seguintes termos:

EBA

	2022	2023	2024	2025	2026	2027	Total
Os custos são integralmente cobertos por taxas cobradas às entidades fiscalizadas[71]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL das dotações cofinanciadas	1,373	1,948	1,748	1,748	1,748	1,748	10,313

EIOPA

	2022	2023	2024	2025	2026	2027	Total
Os custos são integralmente cobertos por taxas cobradas às entidades fiscalizadas[72]	1,305	1,811	1,611	1,611	1,611	1,611	9,560
TOTAL das dotações cofinanciadas	1,305	1,811	1,611	1,611	1,611	1,611	9,560

ESMA

	2022	2023	2024	2025	2026	2027	Total
Os custos são integralmente cobertos por taxas cobradas às entidades fiscalizadas[73]	1,373	1,948	1,748	1,748	1,748	1,748	10,313
TOTAL das dotações cofinanciadas	1,373	1,948	1,748	1,748	1,748	1,748	10,313

INFORMAÇÕES ESPECÍFICAS

Poderes de fiscalização direta

A título de introdução, importa recordar que as entidades objeto de supervisão direta pela ESMA lhe deverão pagar taxas (custos pontuais pelo registo e custos recorrentes pela supervisão contínua). É este

[71] 100 % do custo total estimado mais o total das contribuições do empregador para o regime de pensões.
[72] 100 % do custo total estimado mais o total das contribuições do empregador para o regime de pensões.
[73] 100 % do custo total estimado mais o total das contribuições do empregador para o regime de pensões.

o caso das agências de notação de risco (ver Regulamento Delegado (UE) n.º 272/2012 da Comissão) e dos repositórios de transações (ver Regulamento Delegado (UE) n.º 1003/2013 da Comissão).

Nos termos da presente proposta legislativa, serão atribuídas às AES novas funções destinadas a promover a convergência das abordagens de supervisão em matéria de risco de terceiros no domínio das TIC no setor financeiro, sujeitando as entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas a um quadro de fiscalização da União.

O quadro de fiscalização previsto na presente proposta assenta na arquitetura institucional existente no domínio dos serviços financeiros, mediante o qual o Comité Conjunto das AES assegura a coordenação transetorial em todas as matérias relativas ao risco associado às TIC, em conformidade com as suas atribuições em matéria de cibersegurança, com o apoio do subcomité pertinente (Fórum de Fiscalização), efetuando os trabalhos preparatórios de decisões individuais e das recomendações coletivas dirigidas a entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas.

Por meio deste quadro, as AES designadas como Autoridades de Fiscalização Principais para cada entidade terceira prestadora de serviços no domínio das TIC considerada crítica ficam habilitadas a assegurar que os prestadores de serviços tecnológicos que desempenham uma função crítica no funcionamento do setor financeiro são devidamente monitorizados a uma escala pan-europeia. As obrigações de fiscalização encontram-se definidas na proposta e clarificadas em pormenor na exposição de motivos. Essas obrigações incluem os direitos de solicitar todas as informações e toda a documentação relevantes para a realização das investigações e inspeções gerais, de formular recomendações e, subsequentemente, apresentar relatórios sobre as medidas adotadas ou as correções aplicadas para dar resposta a essas recomendações.

As AES, para desempenhar as novas funções previstas na presente proposta, deverão contratar pessoal adicional especializado no risco associado às TIC e centrado na avaliação das dependências de terceiros.

As necessidades de recursos humanos podem ser estimadas em 6 ETI por cada autoridade (5 AD e 1 AST para apoiar os AD). As AES também incorrerão em custos TI adicionais, estimados em 500 000 EUR (custos pontuais), bem como 50 000 EUR por ano por cada uma das três AES para custos de manutenção. Um elemento importante no desempenho das novas funções são as missões destinadas a realizar inspeções no local e auditorias, que podem ser estimadas em 200 000 EUR por ano por cada AES. Os custos de tradução dos diferentes documentos que as AES irão receber das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas também são incluídos na coluna relativa aos custos operacionais e representam 350 000 EUR anuais.

Todos os custos administrativos supramencionados serão integralmente financiados pelas taxas anuais cobradas pelas AES às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas (sem incidência no orçamento da UE).