Parlamento Europeu
2019-2024

Documento de sessão

A9-0341/2021

7.12.2021

***I
RELATÓRIO

sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro e que altera os regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 e (UE) n.º 909/2014
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

Comissão dos Assuntos Económicos e Monetários

Relator: Billy Kelleher

Legenda dos símbolos utilizados

*	Processo de consulta
***	Processo de aprovação
***I	Processo legislativo ordinário (primeira leitura)
***II	Processo legislativo ordinário (segunda leitura)
***III	Processo legislativo ordinário (terceira leitura)

(O processo indicado tem por fundamento a base jurídica proposta no projeto de ato,)

Alterações a um projeto de ato

Alterações do Parlamento apresentadas em duas colunas

As supressões são assinaladas em itálico e a negrito na coluna da esquerda. As substituições são assinaladas em itálico e a negrito na coluna da esquerda e na coluna da direita. O texto novo é assinalado em itálico e a negrito na coluna da direita.

A primeira e a segunda linhas do cabeçalho de cada alteração identificam o passo relevante do projeto de ato em apreço. Se uma alteração disser respeito a um ato já existente, que o projeto de ato pretenda modificar, o cabeçalho comporta ainda uma terceira e uma quarta linhas, que identificam, respetivamente, o ato existente e a disposição visada do ato em causa.

Alterações do Parlamento apresentadas sob a forma de texto consolidado

Os trechos novos são assinalados em itálico e a negrito. Os trechos suprimidos são assinalados pelo símbolo ▌ ou rasurados. As substituições são assinaladas formatando o texto novo em itálico e a negrito e suprimindo, ou rasurando, o texto substituído.
Exceção: as modificações de natureza estritamente técnica introduzidas pelos serviços com vista à elaboração do texto final não são assinaladas.

ÍNDICE

Página

PROJETO DE RESOLUÇÃO LEGISLATIVA DO PARLAMENTO EUROPEU

sobre a proposta de regulamento do Parlamento Europeu e do Conselho relativo à resiliência operacional digital do setor financeiro e que altera os regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 e (UE) n.º 909/2014
(COM(2020)0595 – C9-0304/2020 – 2020/0266(COD))

(Processo legislativo ordinário: primeira leitura)

O Parlamento Europeu,

– Tendo em conta a proposta da Comissão ao Parlamento Europeu e ao Conselho (COM(2020)0595),

– Tendo em conta o artigo 294.º, n.º 2, e o artigo 114.º do Tratado sobre o Funcionamento da União Europeia, nos termos dos quais a proposta lhe foi apresentada pela Comissão (C9-0304/2020),

– Tendo em conta o artigo 294.º, n.º 3, do Tratado sobre o Funcionamento da União Europeia,

– Tendo em conta o parecer do Comité Económico e Social Europeu de 24 de fevereiro de 2021[1],

– Tendo em conta o artigo 59.º do seu Regimento,

– Tendo em conta o relatório da Comissão dos Assuntos Económicos e Monetários (A9-0341/2021),

1. Aprova a posição em primeira leitura que se segue;

2. Requer à Comissão que lhe submeta de novo a sua proposta, se a substituir, se a alterar substancialmente ou se pretender alterá-la substancialmente;

3. Encarrega o seu Presidente de transmitir a posição do Parlamento ao Conselho, à Comissão e aos parlamentos nacionais.

[1] JO C 155 de 30.4.2021, p. 38.

Alteração 1

ALTERAÇÕES DO PARLAMENTO EUROPEU*

à proposta da Comissão

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,[2]

Tendo em conta o parecer do Comité Económico e Social Europeu,[3]

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 ainda tem de ser incorporada de

* Alterações: o texto novo ou alterado é assinalado em itálico e a negrito; as supressões são indicadas pelo símbolo ▌.

2 [Inserir referência] JO C , p. .

3 JO L 155 de 30.4.2021, p. 38.

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 ▌ e as operações de processamento administrativo. ***O setor dos seguros também sofreu transformações devido à utilização das TIC, desde a emergência de mediadores de seguros digitais que operam com a InsurTech até à subscrição de seguros e à distribuição de contratos digitais.*** Não só o setor financeiro se tornou em grande medida 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[4], 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[5] 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. ***Por conseguinte, é necessário***

---

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

5 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.

considerar o risco no domínio das TIC no contexto de um sistema financeiro mundial altamente interligado, no qual se deve dar prioridade à coerência da regulamentação internacional e à cooperação entre as autoridades competentes a nível mundial.

(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.

(6) No seu Plano de Ação para a Tecnologia Financeira de 2018[6], a Comissão 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, ***reforçando*** os mandatos das autoridades de supervisão financeira ***para gerir os riscos no domínio das TIC no setor financeiro, proteger a integridade e a eficiência do mercado único e facilitar o seu funcionamento ordenado.***

(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

---

6 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

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 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.

(10-A) A criação e a manutenção de infraestruturas adequadas de redes e de sistemas de informação é também uma condição prévia fundamental para a agregação eficaz de dados sobre riscos e a prestação de informações sobre riscos, que são, por sua vez, um requisito fundamental para a solidez e a sustentabilidade da gestão dos riscos e para os processos de tomada de decisão das instituições de crédito. Em 2013, o Comité de Basileia de Supervisão Bancária (CBSB) publicou um conjunto de princípios para uma agregação eficaz de dados sobre riscos e a prestação de informações sobre riscos («CBSB 239»), com base em dois princípios orientadores, a saber, a governação e as infraestruturas informáticas, a serem aplicados até ao início de 2016. De acordo com o relatório do Banco Central Europeu (BCE), de maio de 2018, sobre a revisão temática sobre a agregação eficaz de dados sobre riscos e a prestação de informações sobre riscos, de maio de 2018, e com o relatório intercalar do CBSB, de abril de 2020, os progressos realizados pelos bancos de importância sistémica global foram insatisfatórios e fonte de preocupação. A fim de facilitar o cumprimento e o alinhamento com as normas internacionais, a Comissão, em estreita cooperação com o BCE e após ter consultado a EBA e o CERS, deve elaborar um relatório para avaliar a forma como os princípios do CBSB 239 interagem com as disposições do presente regulamento e, se for caso disso, a forma como esses princípios devem ser incorporados no direito da União.

(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. ***Esta iniciativa visa igualmente aumentar a sensibilização para os riscos das TIC e reconhece que os incidentes relacionados com as TIC e uma falta de resiliência operacional podem comprometer a solidez financeira das entidades financeiras.***

(13) As entidades financeiras devem adotar a mesma abordagem e as mesmas regras baseadas em princípios ao abordarem o risco no domínio das TIC, ***de acordo com a sua dimensão, natureza, complexidade e perfil de risco***. A coerência contribuirá para reforçar a confiança no sistema financeiro e preservar a sua estabilidade, em especial quando se verifica uma ***dependência elevada*** 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.

(14-A) No entanto, a aplicação do presente regulamento não deve comprometer a inovação no que diz respeito à forma como as entidades financeiras lidam com questões de resiliência operacional digital, cumprindo simultaneamente as suas disposições, e tampouco no que diz respeito aos serviços que oferecem ou aos serviços oferecidos por terceiros prestadores de serviços de TIC.

(15) Além da legislação em matéria de serviços financeiros, a Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho[7] 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, ***para as entidades financeiras,*** 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 ***para*** 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 únicos designados por força da Diretiva (UE) 2016/1148. ***O órgão conjunto de fiscalização, a autoridade fiscalizadora principal e 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.

Além disso, o presente regulamento deve zelar por que a rede de CSIRT criada pela Diretiva (UE) 2016/1148 receba informações circunstanciadas sobre incidentes

---

[7] 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).

graves relacionados com as TIC.

(18) Importa, ainda, garantir a coerência ***tanto*** 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, ***como com a Diretiva relativa à resiliência das entidades críticas***[8], com possíveis ramificações para o setor financeiro.

(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, ***e ambos os requisitos substantivos e processuais aplicáveis aos terceiros prestadores de serviços de TIC críticos, ao abrigo do presente regulamento, devem ser coerentes e sem descontinuidades face aos aplicáveis ao abrigo daquela diretiva.*** 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 ***e dentro do grupo TIC*** no domínio das TIC. É necessário elevar o nível da resiliência operacional digital no sistema financeiro, permitindo simultaneamente uma aplicação proporcionada dos requisitos ***tendo em conta a respetiva natureza, escala, complexidade e perfil de risco global***.

(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)[9] 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 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

---

[8] 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).

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

riscos no domínio das TIC em caso de ataques em grande escala com consequências potencialmente sistémicas.

(21-A) A fim de reduzir os encargos administrativos e evitar a complexidade e a duplicação dos requisitos de comunicação de informações para os prestadores de serviços de pagamento abrangidos pelo âmbito de aplicação do presente regulamento, os requisitos de comunicação de incidentes previstos na Diretiva (UE) 2015/2366 deverão deixar de se aplicar. Como tal, as instituições de crédito, as instituições de moeda eletrónica e as instituições de pagamento devem comunicar, nos termos do presente regulamento, todos os incidentes operacionais ou relacionados com pagamentos de títulos e não relacionados com pagamentos que tenham sido anteriormente comunicados ao abrigo da Diretiva (UE) 2015/2366, independentemente de os incidentes estarem ou não relacionados com as TIC.

(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 ***conseguir um*** regime ***robusto*** de comunicação dos incidentes relacionados com as TIC com os requisitos que ***resolvam as lacunas na legislação dos serviços financeiros setoriais*** 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 às respetivas autoridades competentes ***através de um quadro único simplificado, de acordo com o estabelecido no presente regulamento***. 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 vindo a ser desenvolvidos em alguns subsetores financeiros no âmbito de diversos quadros nacionais ***por vezes*** não coordenados, que tratam as mesmas questões de formas diferentes. Esta situação multiplica os custos para as entidades financeiras transfronteiriças e ***pode entravar*** 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[10], 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

[10] 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).

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 prestam ***serviços críticos a*** entidades financeiras. ***Uma vez que a prestação intragrupo de serviços de TIC não comporta os mesmos riscos, os prestadores de serviços que fazem parte do mesmo grupo ou sistema de proteção institucional não devem ser definidos como terceiros prestadores de serviços de TIC críticos.***

(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 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. ***Por conseguinte, é importante reforçar os mecanismos de cooperação e a comunicação de informações entre as entidades financeiras e as autoridades competentes, assim como a partilha de informações com o público, com vista a desenvolver um quadro aberto de partilha de informações e uma abordagem de «segurança desde a conceção», que são essenciais para aumentar a resiliência operacional e a preparação do setor financeiro no que diz respeito aos riscos das TIC. Os acordos de partilha de informações devem ter sempre em devida conta os potenciais riscos relacionados com a cibersegurança, a proteção de dados ou a confidencialidade comercial.***

(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. ***Por conseguinte, é importante reforçar esses canais de comunicação e obter contributos de autoridades não supervisoras, sempre que necessário e pertinente, ao longo de todo o ciclo de supervisão.***

(32) Importa ***também*** 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[11], 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[12], 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, ***incluindo os requisitos do quadro de gestão de risco,*** deve ter em consideração as significativas diferenças entre as entidades financeiras em termos de dimensão, ***natureza, complexidade e perfil de risco***. 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, ***natureza, complexidade, perfil de atividades e perfil de risco relativo***, enquanto as autoridades competentes deverão avaliar e rever de forma recorrente a abordagem de tal afetação. em termos de dimensão, perfil de atividades ou exposição ao risco digital.

(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 ***previstos*** provocados por perturbações ***significativas*** nas TIC, ***incidentes graves no***

---

11 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.

12 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).

domínio das TIC e os resultados das avaliações pós-incidentes na sequência de ***tais*** 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[13], 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

---

[13] 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

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***, tendo em consideração se a função é crítica ou importante***. 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.

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 ***para a comunicação dos principais incidentes relacionados com as TIC***, 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, ***excluindo as microempresas***, 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. ***Além disso, a fim de reforçar a cooperação com países terceiros de confiança no domínio da resiliência das entidades financeiras, a Comissão e as autoridades competentes devem procurar estabelecer um quadro para o reconhecimento mútuo dos resultados dos testes de penetração com base em ameaças.***

Os Estados-Membros devem designar uma única autoridade pública responsável pelos testes de penetração com base em ameaças no setor financeiro a nível nacional. A autoridade pública única pode ser, nomeadamente, uma autoridade nacional competente ou uma autoridade pública designada em conformidade com o artigo 8.º da Diretiva (UE) 2016/1148 (SRI). A autoridade pública única deve ser responsável pela emissão dos atestados que indicam que os testes de penetração com base em ameaças foram realizados em conformidade com os requisitos. Tais atestados deverão facilitar o reconhecimento mútuo dos testes entre as autoridades competentes.

Algumas entidades financeiras têm a capacidade para realizar testes avançados internos, ao passo que outras contratarão verificadores externos da União ou de um país terceiro. Como tal, é importante que todos os verificadores estejam sujeitos aos mesmos requisitos claros. A fim de garantir a independência dos verificadores internos, a sua utilização deverá estar sujeita à aprovação pela autoridade competente.

A metodologia aplicável aos testes de penetração com base em ameaças não deve ser obrigatória, mas a utilização do quadro TIBER-UE existente deve ser considerada conforme com os requisitos dos testes de penetração com base em ameaças de acordo com o estabelecido no presente regulamento.

Até à entrada em vigor do presente regulamento e ao desenvolvimento e adoção pelas AES das normas técnicas regulamentares obrigatórias em matéria de testes de penetração com base em ameaças, as entidades financeiras devem seguir as orientações e os quadros da União aplicáveis aos testes de penetração baseados em informações, uma vez que estes continuarão a ser aplicáveis após a entrada em vigor do presente regulamento.

(44-A) A responsabilidade pela realização dos testes de penetração com base em ameaças — e pela gestão da cibersegurança em geral e pela prevenção de ciberataques — deve continuar a caber plenamente à entidade financeira, e os atestados fornecidos pelas autoridades devem ser exclusivamente para efeitos de reconhecimento mútuo e não devem impedir qualquer ação de acompanhamento sobre o nível de risco das TIC a que a entidade financeira está exposta, nem ser vista como uma aprovação das suas capacidades de gestão e atenuação dos riscos das TIC.

(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***, em especial no que respeita à prestação de funções críticas ou importantes por 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 natureza***, 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***, bem como se os serviços TIC são fornecidos por um prestador de serviços intragrupo ou terceiro***.

(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, ***ao mesmo tempo que devem ser tomadas medidas corretivas, que podem incluir a*** rescisão ***parcial ou total*** dos contratos, ***em caso de***, pelo menos, um conjunto de circunstâncias demonstrativas de insuficiências ***graves*** 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 ▌. 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. ***O órgão conjunto de fiscalização que realiza a*** fiscalização de cada terceiro prestador de serviços de TIC ***crítico e a AES incumbida da fiscalização diária*** (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[14].

(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, cessação da atividade do terceiro prestador de serviços de TIC ***ou a rescisão dos contratos celebrados*** devem ser considerados 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 ***pertinente para os serviços prestados pelo***

[14] 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.

terceiro prestador de serviços de TIC à instituição financeira de acordo com os níveis de serviço acordados sem custos adicionais ou a um custo previamente determinado. ***Os serviços de TIC auxiliares de que as entidades financeiras não dependam do ponto de vista operacional não são abrangidos pelo presente regulamento***.

Além disso, a definição de «função crítica ou importante» prevista no presente regulamento deve abranger a definição de «funções críticas» prevista no artigo 2.º, n.º 1, ponto (35), da Diretiva 2014/59/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014[15]***. Assim, as funções consideradas críticas nos termos da Diretiva 2014/59/UE deverão ser consideradas críticas ou importantes na aceção do presente regulamento.***

(53) ***No caso de disposições contratuais para funções críticas ou importantes, 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***, o órgão conjunto de fiscalização, a autoridade fiscalizadora principal*** da entidade financeira devem ter o direito, mediante notificação, de inspecionar e auditar o terceiro prestador de serviços de TIC, sob reserva da confidencialidade ***e mantendo a prudência para não perturbar os serviços prestados a outros clientes do terceiro prestador de serviços de TIC***. ***A entidade financeira e o terceiro prestador de serviços de TIC devem poder acordar que os direitos de acesso, inspeção e auditoria podem ser delegados a terceiros independentes***.

(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 efetivamente o terceiro prestador de serviços de TIC ou, em alternativa, recorrer a soluções internas, coerentes com a complexidade do serviço prestado. ***Além disso, as instituições de crédito devem assegurar que os contratos pertinentes no domínio das TIC são sólidos e plenamente aplicáveis em caso de resolução da instituição de crédito. Em consonância com as expectativas das autoridades de resolução, as instituições de crédito devem assegurar que os contratos pertinentes para serviços de TIC são resilientes à resolução. Enquanto continuarem a ser desempenhadas funções críticas ou importantes no domínio das TIC, essas entidades financeiras devem assegurar que os contratos contenham, entre outros requisitos, cláusulas de não rescisão, de não suspensão e de não alteração por motivos de reestruturação ou resolução.***

(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

[15] ***Diretiva 2014/59/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, que estabelece um enquadramento para a recuperação e a resolução de instituições de crédito e de empresas de investimento e que altera a Diretiva 82/891/CEE do Conselho, e as Diretivas 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE e 2013/36/UE e os Regulamentos (UE) n.º 1093/2010 e (UE) n.º 648/2012 do Parlamento Europeu e do Conselho (JO L 173 de 12.6.2014, p. 190)***.

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.

(55-A) As AES devem ser mandatadas para elaborar normas técnicas e regulamentares de execução que especifiquem as expectativas das políticas relativas à gestão do risco de terceiros no domínio das TIC e aos requisitos contratuais. Até à entrada em vigor dessas normas, as entidades financeiras deverão seguir as orientações relevantes e outras medidas emitidas pelas AES e pelas autoridades competentes.

(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 ***estabeleceriam os parâmetros de criticalidade como base para a inclusão no Quadro de Fiscalização***. 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 ***que apoiem o cumprimento das atribuições*** do Eurosistema***, tal como referido no*** artigo 127.º, n.º 2, do Tratado sobre o Funcionamento da União Europeia devem, consequentemente, estar isentos. ***Do mesmo modo, as empresas que fazem parte de um grupo financeiro e que prestam serviços TIC exclusivamente a entidades financeiras pertencentes ao mesmo grupo financeiro não devem estar sujeitas ao mecanismo de designação.***

(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. ***O requisito de ter uma empresa, tal como uma filial constituída na União ao abrigo da legislação de um Estado-Membro, destina-se a proporcionar um ponto de contacto entre o prestador de serviços de TIC a terceiros, por um lado, e a autoridade fiscalizadora principal e o órgão conjunto de fiscalização, por outro, e a assegurar que a autoridade fiscalizadora principal e o órgão conjunto de fiscalização possam desempenhar as suas funções e exercer os seus poderes de supervisão e execução, tal como previsto no presente regulamento***. ***Os serviços contratados pelo terceiro prestador de serviços de TIC não têm de ser***

prestados pela sua entidade na União.

(58-A) Tendo em conta o impacto significativo que a designação como crítica poderia ter nos terceiros prestadores de serviços de TIC, os direitos de audição prévia devem ser estabelecidos como uma obrigação imposta às AES e ao órgão conjunto de fiscalização de ter devidamente em conta quaisquer informações adicionais fornecidas por terceiros prestadores de serviços de TIC no decurso do processo de designação.

(59) O Quadro ***de Fiscalização*** 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, ***através do recém-criado órgão conjunto de fiscalização que emite*** decisões individuais dirigidas a terceiros prestadores de serviços de TIC críticos ***e*** 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, ***deve criar-se um órgão conjunto de fiscalização para efetuar a supervisão direta dos terceiros prestadores de serviços de TIC***. ***Além disso,*** uma das AES deve ser designada como Autoridade de Fiscalização Principal em relação a cada terceiro prestador de serviços de TIC crítico***, a fim de realizar e coordenar o trabalho de supervisão e investigação quotidianos, atuar como ponto de contacto único e assegurar a continuidade***. ***O órgão conjunto de fiscalização e a autoridade fiscalizadora principal devem trabalhar uniformemente para assegurar uma supervisão diária eficiente, bem como uma abordagem holística da tomada de decisões e das recomendações.***

(62) A Autoridade de Fiscalização Principal deve estar habilitada a realizar investigações e inspeções no local ▌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.

(62-A) Confiar ao ***órgão conjunto de fiscalização*** a fiscalização ***direta*** 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, ***o órgão conjunto de fiscalização deve poder formular*** 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, ***o órgão conjunto de fiscalização deve*** ponderar devidamente o cumprimento de tais recomendações importantes formuladas pelo órgão executivo conjunto de fiscalização. ***Antes da finalização dessas recomendações, os terceiros prestadores de serviços TIC críticos devem ter a oportunidade de fornecer informações em relação às quais tenham razões para elas serem tidas em conta antes de a recomendação ser finalizada e emitida***.

(63-A) A fim de evitar duplicações e contradições com as medidas técnicas e organizativas que são aplicáveis a terceiros prestadores de serviços de TIC críticos, a autoridade de fiscalização principal e o órgão conjunto de fiscalização devem ter devidamente em conta o quadro estabelecido pela Diretiva (UE) 2016/1148 no exercício dos seus poderes, de acordo com o Quadro de Fiscalização previsto no presente regulamento. Antes de exercer esses poderes, o órgão conjunto de fiscalização e a autoridade de fiscalização principal deve consultar as autoridades competentes com jurisdição ao abrigo da Diretiva (UE) 2016/1148.

(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. Tais medidas deverão ser previamente coordenadas e acordadas no contexto do Quadro de Supervisão.

(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***, aquando da realização de investigações de caráter geral ou inspeções no local,*** 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[16], bem como a consulta das AES, através do intercâmbio de informações e da prestação de assistência no contexto das atividades de supervisão. ***O Conselho Único de Resolução, embora não seja uma autoridade competente para efeitos do presente regulamento, deve participar nos mecanismos de intercâmbio mútuo de informações entre as entidades abrangidas pelo âmbito de aplicação do Regulamento (UE) n.º 806/2014 do Parlamento Europeu e do Conselho[17]***.

(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, de 13 de abril de 2016, sobre legislar melhor[18]. Em particular, a fim de assegurar a igualdade de participação na preparação dos atos delegados, o Parlamento Europeu e o Conselho recebem todos os documentos ao mesmo tempo que os peritos dos Estados-Membros, e os respetivos peritos têm sistematicamente acesso às reuniões dos grupos de peritos da Comissão que tratem da preparação dos atos delegados.

(69) Uma vez que o presente regulamento, juntamente com a Diretiva (UE) 20xx/xx do Parlamento Europeu e do Conselho[19], 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

---

[16] 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).

[17] ***Regulamento (UE) n.º 806/2014 do Parlamento Europeu e do Conselho, de 15 de julho de 2014, que estabelece regras e um procedimento uniformes para a resolução de instituições de crédito e de certas empresas de investimento no quadro de um Mecanismo Único de Resolução e de um Fundo Único de Resolução bancária e que altera o Regulamento (UE) n.º 1093/2010 (JO L 225 de 30.7.2014, p. 1).***

[18] JO L 123 de 12.5.2016, p. 1.

[19] [*Inserir referência completa*]

(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.

As orientações aplicáveis emitidas pelas AES ou que estão a ser preparadas pelas mesmas sobre a aplicação desses regulamentos e diretivas devem ser analisadas e revistas como parte do processo de consolidação, de modo a que a base jurídica dos requisitos em matéria de risco das TIC no direito da União decorra exclusivamente do presente regulamento, dos seus atos de execução e das decisões e recomendações adotadas em conformidade com esse regulamento, relativamente às entidades abrangidas pelo seu âmbito de aplicação.

(69-A) 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. ***Ao elaborarem projetos de normas técnicas de regulamentação, as AES devem ter devidamente em conta o seu mandato em relação aos aspetos da proporcionalidade e solicitar o parecer dos respetivos comités consultivos em matéria de proporcionalidade, em especial no que diz respeito à aplicação do quadro do presente regulamento às PME e às empresas de média capitalização.***

(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 natureza,*** a dimensão***,*** a complexidade ***e o perfil de atividades*** 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 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,

– ***comunicação de incidentes operacionais ou de segurança relacionados com os pagamentos às autoridades competentes pelas entidades financeiras referidas no artigo 2.º, n.º 1, alíneas a) a c);***

– realização de testes de resiliência operacional digital,

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

– (Não se aplica à versão portuguesa)

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

(c) Quadro de fiscalização para as entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas 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.

2-A. O presente regulamento não prejudica as competências dos Estados-Membros no domínio da manutenção da segurança pública, da defesa e da segurança nacional.

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 ***e oferentes*** de criptoativos, emitentes ***e oferentes*** de criptofichas ***referenciados*** a ativos e emitentes de criptofichas referenciadas a ativos significativas;

(f) Centrais de valores mobiliários e operadores de sistemas de liquidação 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***, que não sejam micro, pequenas ou médias empresas, a menos que essas micro, pequenas ou médias empresas dependam exclusivamente de sistemas de vendas automatizadas organizados***;

(o) Instituições de realização de planos de pensões profissionais ***(IRPPP) que não gerem planos de pensões com menos de 15 membros no seu conjunto***;

(p) Agências de notação de risco;

(q) Revisores oficiais de contas e sociedades de revisores oficiais de contas ***que não sejam micro, pequenas ou médias empresas, a menos que essas micro, pequenas ou médias empresas prestem serviços de auditoria às entidades enumeradas no presente artigo, com exceção das micro, pequenas ou médias empresas que sejam entidades de auditoria sem fins lucrativos na aceção do artigo 2.º, n.º 3, do Regulamento (UE) n.º 537/2014, a menos que a autoridade competente decida que a exceção não é válida***,

(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.

1-A. O presente regulamento, com exceção da Secção II do Capítulo V, é igualmente aplicável aos prestadores de serviços intragrupo no domínio das TIC.

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

2-A. Para efeitos do presente regulamento, com exceção da secção II do Capítulo V, os terceiros prestadores de serviços de TIC e os prestadores de serviços intragrupo no domínio das TIC são coletivamente referidos como "terceiros prestadores de serviços de TIC".

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 ▌, assegurando direta ou indiretamente, com recurso a serviços de terceiros prestadores de serviços de TIC, ▌ a contínua prestação de serviços financeiros e a qualidade dos mesmos ***face a perturbações operacionais com impacto nas capacidades de TIC da entidade financeira***;

(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 ▌ que, caso se materialize, pode comprometer a segurança das redes e dos sistemas de informação, de qualquer instrumento ou processo ***dependente de TIC***, do funcionamento e da execução de processos ou da prestação de serviços▌ ;

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

(6) «Incidente relacionado com as TIC», ***um incidente imprevisto, ou uma série de incidentes conexos***, que comprometa a segurança das redes e sistemas de informação ▌ ou tenha quaisquer efeitos adversos na disponibilidade continuidade***, integridade*** ou autenticidade dos serviços financeiros prestados pela entidade financeira;

(6-A) «Incidente operacional ou de segurança relacionado com o pagamento de títulos», uma ocorrência ou uma série de ocorrências conexas imprevistas pelas entidades financeiras, referidas no artigo, 2.º, n.º 1, alíneas a) a c), que tenha ou seja suscetível de ter um impacto negativo na integridade, disponibilidade, confidencialidade, autenticidade ou continuidade dos serviços relacionados com o pagamento de títulos;

(7) «Incidente grave relacionado com as TIC», um incidente relacionado com as TIC ***que tenha ou seja suscetível de ter*** um impacto negativo ▌ elevado nas redes e sistemas de informação que apoiam as funções críticas da entidade financeira;

(7-A) «Incidente operacional ou relacionado com pagamentos de títulos grave», um incidente operacional ou relacionado com pagamentos de títulos que satisfaça os critérios estabelecidos no artigo 16.º;

(8) «Ciberameaça», uma ciberameaça na aceção do artigo 2.º, ponto 8, do Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho[20];

(8-A) «Ciberameaça significativa», uma ciberameaça cujas características indiquem

[20] 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).

claramente que é suscetível de resultar num incidente grave relacionado com as TIC;

(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;

(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 ***ciberameaça***;

(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 ***de TIC***, nomeadamente ***uma entidade financeira que presta serviços de TIC que faz parte de uma empresa que fornece uma gama mais vasta de produtos ou serviços***, mas com exclusão dos fornecedores de componentes de equipamento informático e as empresas autorizadas ao abrigo do direito da União ***que prestam*** serviços de comunicações eletrónicas na aceção do artigo 2.º, ponto 4, da Diretiva (UE) 2018/1972 do Parlamento Europeu e do Conselho[21];

(15-A) «Prestador de serviços intragrupo no domínio das TIC», uma empresa que faz parte de um grupo financeiro e presta serviços de TIC exclusivamente a entidades financeiras do mesmo grupo ou a entidades financeiras pertencentes ao mesmo sistema de proteção institucional, incluindo às respetivas empresas-mãe, filiais, sucursais ou outras entidades que se encontrem sob propriedade ou controlo comuns;

(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, ***de forma contínua, com exceção de contratos de telecomunicações***;

(17) «Função crítica ou importante», uma ***atividade ou um serviço essencial para o funcionamento de uma entidade financeira, cuja perturbação prejudicaria a solidez ou a continuidade dos serviços e atividades da entidade financeira, ou*** cuja interrupção, anomalia ou falha debilitaria consideravelmente o contínuo cumprimento

[21] 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).

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, ***incluindo as «funções críticas», tal como definidas no artigo 2.º, n.º 1, ponto 35, da Diretiva 2014/59/UE***;

(18) «Terceiro prestador de serviços de TIC crítico», um terceiro prestador de serviços de TIC designado nos termos do artigo ***28.º*** e sujeito ao Quadro de Fiscalização a que se referem os artigos ***29.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 ▌ 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 ▌ e tenha celebrado um acordo contratual ou com um terceiro 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 ***estabilidade financeira da União no seu conjunto ou*** a capacidade de uma entidade financeira ▌ desempenhar funções críticas ***ou importantes***, 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[22] e do artigo 3.º, n.º 1, ***ponto 18***, do Regulamento (UE) 20xx/xx do Parlamento Europeu e do Conselho[23] [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[24];

(23-A) «Instituição de crédito isenta nos termos da Diretiva 2013/36/UE», uma instituição de crédito que beneficia de uma isenção nos termos do artigo 2.º, n.º 5, pontos 4 a 23, da Diretiva 2013/36/UE;

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

---

22 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).

23 [*Inserir título completo e informação do JO*]

24 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).

(24-A) «Empresa de investimento pequena dimensão e não interligada», uma empresa de investimento que cumpre as condições previstas no artigo 12.º, n.º 1, do Regulamento (UE) 2019/2033;

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

(25-A) «Instituição de pagamento isenta ao abrigo da Diretiva (UE) 2015/2366», uma instituição de pagamento que beneficia de uma isenção nos termos do artigo 32.º, n.º 1 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[25];

(26-A) «Instituição de moeda eletrónica isenta ao abrigo da Diretiva 2009/110/CE», uma instituição de moeda eletrónica que beneficia de uma isenção nos termos do artigo 9.º da Diretiva 2009/110/CE;

(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;

(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

---

[25] 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).

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, ***ponto 8***, 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, ***ponto 6***, do [Serviço das Publicações: inserir referência do MICAR];

(44-A) «Oferente», um oferente na aceção do [artigo 3.º, n.º 1, ponto XX] do [Serviço das Publicações: inserir referência do MICAR];

(44-B) «Oferente de criptoativos», um oferente de criptoativos na aceção do [artigo 3.º, n.º 1, ponto XX,] 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];

(45-A) «Oferente de criptofichas referenciadas a ativos», um oferente de criptofichas referenciadas a ativos na aceção do [artigo 3.º, n.º 1, ponto XX] 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, ***ponto XX***, 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 ***3***, ***ponto 25***, do Regulamento (UE) ***2016/1011*** [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 ***2.º, n.º 1***, alínea ***e)***, do Regulamento (UE) ***2020/1503*** [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) «Micro***, pequena e média*** empresa», uma entidade financeira na aceção do artigo 2.º do anexo da Recomendação 2003/361/CE***;***

(50-A) «Autoridade de resolução», uma autoridade designada por um Estado-Membro nos termos do artigo 3.º da Diretiva 2014/59/UE ou pelo Conselho Único de Resolução, criado nos termos do artigo 1.º do Regulamento (UE) 806/2014.

Artigo 3.º-A

Princípio da proporcionalidade

1. As entidades financeiras aplicam as regras introduzidas pelos capítulos II, III e IV, em conformidade com o princípio da proporcionalidade, tendo em conta a respetiva dimensão, a natureza, a escala e a complexidade dos seus serviços, atividades e operações, bem como o seu perfil de risco global.

2. Em virtude do princípio da proporcionalidade, os artigos 4.º a 14.º do presente regulamento não se aplicam a:

(a) empresas de investimento e instituições de pagamento de pequena dimensão e não interligadas isentas nos termos da Diretiva (UE) 2015/2366;

(b) instituições de crédito isentas nos termos da Diretiva 2013/36/UE;

(c) instituições de moeda eletrónica isentas nos termos da Diretiva 2009/110/CE; ou

(d) pequenas instituições de realização de planos de pensões profissionais.

3. Com base no relatório anual sobre a análise do quadro de gestão do risco associado às TIC, a que se referem o artigo 5.º, n.º 6, e o artigo 14.º-A, n.º 2, as autoridades competentes pertinentes devem analisar e avaliar a aplicação do princípio da proporcionalidade por parte da entidade financeira e determinar se o quadro de gestão do risco associado às TIC da entidade financeira garante uma gestão adequada e a resiliência operacional digital e a cobertura do risco no domínio das TIC. Assim, as autoridades competentes têm em conta a dimensão da entidade financeira, a natureza, a escala e a complexidade dos seus serviços, atividades e operações, bem como o seu perfil de risco global.

4. Caso a autoridade competente pertinente considere que o quadro de gestão do risco associado às TIC da entidade financeira é insuficiente ou desproporcionado, deve encetar um diálogo com a entidade financeira para solucionar os problemas e garantir a plena conformidade com o capítulo II.

5. As AES elaboram projetos de normas técnicas de regulamentação nas seguintes áreas:

(a) determinação do nível de aplicabilidade das obrigações de gestão do risco no domínio das TIC a cada uma das entidades financeiras a que se refere o n.º 1;

(b) melhoria da definição do conteúdo e do formato do relatório anual de análise do quadro de gestão do risco associado às TIC a que se refere o n.º 3;

(c) melhoria da definição das normas e dos procedimentos que as autoridades competentes e as entidades financeiras devem respeitar no âmbito do diálogo a que se refere o n.º 4.

6. As AES devem apresentar à Comissão os projetos de normas técnicas de regulamentação a que se refere o n.º 5 até [Serviço das Publicações: inserir a data correspondente a um ano após a data de entrada em vigor].

É delegado na Comissão o poder de adotar as normas técnicas de regulamentação a que se refere o n.º 5 do presente artigo, 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.

CAPÍTULO II

GESTÃO DO RISCO NO DOMÍNIO DAS TIC

SECÇÃO I

Artigo 4.º

Governação e organização

1. As entidades financeiras devem implantar ***um quadro*** de governação ***interna*** e ***de*** controlo que garanta uma gestão eficaz e prudente de todos os riscos no domínio das TIC***, com vista a alcançar um elevado nível de resiliência operacional digital***.

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;

(a-A) Aplicar procedimentos e políticas que visem a preservação de elevados níveis de segurança, confidencialidade e integridade dos dados;

(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***, que pode ser adotado enquanto política distinta específica e enquanto parte do plano de continuidade das atividades e do plano de recuperação em caso de catástrofe mais geral da entidade financeira,*** a que se referem 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 ***pertinente*** sobre as competências e os riscos no domínio das TIC para todos os funcionários ▌;

(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 ***regularmente*** informado sobre***, pelo menos,*** os incidentes ***graves*** 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 ***existentes na entidade financeira para a*** utilização de serviços no domínio das TIC***, em especial os celebrados com terceiros prestadores 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 ***da entidade financeira*** devem ***atualizar ativamente*** conhecimentos e competências ***suficientes*** para compreender e avaliar os riscos no domínio das TIC e o respetivo impacto no funcionamento da entidade financeira***, inclusive frequentando regularmente formações específicas, adequadas aos riscos no domínio das TIC que são chamados a gerir***.

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 ▌.

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 ***e sobre o quadro de gestão do risco associado às TIC que aplicam,*** 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, quando disponível ***e adequado***, em conformidade com as orientações de supervisão,

incluindo as orientações de supervisão estabelecidas para o efeito pelas AES, que deverão rever periodicamente.

5. As entidades financeiras que não sejam microempresas devem ***atribuir a responsabilidade pela gestão e supervisão dos riscos no domínio das TIC a uma função de controlo e assegurar a independência e objetividade dessa função de controlo, a fim de evitar conflitos de interesses***. ***As entidades financeiras*** devem assegurar uma ***independência*** 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.

Deve ser apresentado anualmente à autoridade competente um relatório de análise do quadro de gestão do risco no domínio das TIC.

7. ***Relativamente às entidades financeiras que não sejam microempresas,*** 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 ▌.

9. O quadro de gestão do risco associado às TIC a que se refere o n.º 1 deve incluir uma estratégia de resiliência ***operacional*** 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 ▌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) ***Identificar*** as principais dependências de entidades terceiras prestadoras de serviços no domínio das TIC e explicar detalhadamente ***as estratégias de saída relacionadas com estas dependências principais***;

(h) Realizar testes à resiliência operacional digital***, em conformidade com o capítulo IV do presente regulamento***;

(i) Delinear uma estratégia de comunicação caso ocorram incidentes relacionados com as TIC***, cuja divulgação seja obrigatória nos termos do artigo 13.º***.

10. Mediante aprovação das autoridades competentes, as entidades financeiras podem ***externalizar*** as tarefas de verificação do cumprimento dos requisitos de gestão do risco associado às TIC a empresas ▌ externas.

Mediante notificação das autoridades competentes, as entidades financeiras podem delegar a tarefa de verificação do cumprimento dos requisitos de gestão do risco associado às TIC a empresas dentro do grupo.

Em caso de opção pela delegação a que se refere o segundo parágrafo, a entidade financeira deve continuar a ser plenamente responsável pela verificação do cumprimento dos requisitos de gestão dos riscos associados às TIC.

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***, a fim de dar resposta ao risco associado às TIC e gerir este risco,*** que satisfaçam as seguintes condições:

(a) Os sistemas e as ferramentas são adequados à ▌ 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 ***críticas ou importantes***, 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 ***em que medida as funções empresariais relacionadas com as TIC são críticas ou importantes, bem como*** 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 ***críticas ou importantes*** 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***, se necessário,*** 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 ***críticos ou importantes, tendo em conta a sua finalidade,*** e das ligações e interdependências entre ***esses*** diferentes ativos TIC.

5. As entidades financeiras devem identificar e documentar todos os processos ***críticos ou importantes*** 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 ***que apoiem funções críticas ou importantes***.

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, ***incluindo sistemas que ainda sejam utilizados e desempenhem as suas funções mas que:***

   (a) sejam antiquados ou estejam em final de vida, no caso de equipamentos informáticos;

   (b) já não beneficiem de apoio ou manutenção por parte do prestador; ou

   (c) sejam impossíveis ou economicamente impossíveis de atualizar. Devem ser efetuadas avaliações de risco no domínio das TIC anuais, em especial antes e depois ***da conexão de*** tecnologias, aplicações ou sistemas .

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***, apoiar funções críticas ou importantes*** 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 ▌ no domínio das TIC que permitam:

   (a) ***Maximizar*** 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 ***estejam*** protegidos contra riscos ***internos das TIC, incluindo*** má administração***, riscos relacionados com o tratamento e erros humanos***.

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

   (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, ***garantindo simultaneamente a plena proteção dos recursos TIC, dados e ativos em formato informático*** dos seus clientes***, caso façam parte dos sistemas TIC das entidades financeiras***;

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

   (c) Executar políticas***, procedimentos e controlos*** 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▌ ;

   (d) Executar políticas e protocolos que garantam mecanismos de autenticação robustos ***e a proteção de chaves criptográficas***, com base nas normas pertinentes e em sistemas de controlos dedicados▌ ;

   (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 ▌cortadas ***o mais rapidamente possível*** e ***devem*** 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 ***e, caso seja tecnologicamente possível***, identificando ***e controlando*** 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 ▌***despoletar*** a deteção de incidentes relacionados com as TIC e os processos de resposta aos mesmos, ***incluindo*** 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 ▌para monitorizar a atividade dos utilizadores e a ocorrência de anomalias e incidentes relacionados com as TIC, em especial ciberataques.

3-A. As entidades financeiras devem registar todos os incidentes relacionados com as TIC que tenham um impacto na estabilidade, na continuidade ou na qualidade dos serviços financeiros, incluindo quando o incidente tenha ou seja suscetível de ter um impacto nesses serviços.

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, ***as entidades financeiras devem implementar uma*** política de continuidade da atividade operacional ***abrangente, que pode ser aprovada enquanto política distinta específica e parte integrante da*** política operacional de continuidade das atividades ***geral da entidade financeira***.

O objetivo da política de continuidade das atividades no domínio das TIC deve consistir em gerir e atenuar os riscos que possam ter um efeito nocivo nos sistemas e serviços TIC das entidades financeiras e facilitar a rápida recuperação destas, se necessário. No âmbito da elaboração da política de continuidade das atividades no domínio das TIC, as entidades financeiras devem ponderar especificamente os riscos que possam ter um impacto negativo nos serviços e sistemas 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:

(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 ***críticos ou importantes***;

(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***, enquanto função específica ou integrada em funções com responsabilidades pela resposta e gestão em relação a incidentes. A função de gestão de crises deve,*** em caso de ativação da ▌política de continuidade das atividades no domínio das TIC ou do ▌plano de recuperação em caso de catástrofe associada às TIC ***das entidades***, ***estipular*** 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 ***relevantes*** 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 ***financeiros estimados*** e todas as perdas causados por perturbações ***significativas*** nas TIC e incidentes ***graves*** relacionados com as TIC.

9-A. As AES devem, através do Comité Conjunto, desenvolver orientações comuns relacionadas com a metodologia para o cálculo dos custos e a quantificação das perdas a que se refere o n.º 9.

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. ***Em conformidade com a política de cópias de segurança a que se refere o n.º 1, alínea (a),*** 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 ***separados física ou logicamente do seu*** sistema ***de TIC*** principal 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 ***avaliar a necessidade de*** manter capacidades de TIC redundantes equipadas com recursos, capacidade e funcionalidades suficientes e adequados para garantir as necessidades operacionais ***e satisfazer aos requisitos de resiliência operacional digital previstos no presente regulamento***.

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 ▌acessível ao pessoal da entidade financeira por forma a assegurar a continuidade ***das funções críticas ou importantes*** 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 ***se a função é crítica ou importante e*** 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 ***garantir o mais elevado nível de integridade dos dados, por exemplo realizando*** múltiplas verificações, nomeadamente conciliações de dados▌. ***Tais*** 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 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 ***graves*** 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 ***relacionadas com a resposta a riscos no domínio das TIC identificados na sequência de uma análise de um incidente grave relacionado com as TIC***, as entidades financeiras que não sejam microempresas devem comunicar ***todas as*** alterações ***significativas*** às autoridades competentes***, especificando as melhorias necessárias e a forma como visam prevenir ou atenuar perturbações no futuro***. ***A comunicação das alterações às entidades competentes pode ocorrer antes ou depois da introdução das alterações***.

   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***, inclusive a proximidade desses riscos de funções críticas ou importantes,*** 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. ***Os programas de sensibilização no domínio da segurança das TIC devem aplicar-se a todo o pessoal. As formações em matéria de resiliência operacional digital*** devem ser aplicáveis***, pelo menos,*** a todos os trabalhadores ***com direitos de acesso direto a sistemas de TIC, assim como*** aos quadros superiores. ***A complexidade dos módulos de formação deve ser proporcional ao nível de acesso direto aos sistemas TIC do trabalhador e, em especial, ter em conta o acesso deste a funções críticas ou importantes.***

As entidades financeiras***, que não sejam microempresas,*** 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***, no mínimo*** os incidentes ***graves*** relacionados com as TIC ou as principais vulnerabilidade aos clientes e às contrapartes, bem como ao público, se for caso disso.

   Os planos de comunicação a que se refere o primeiro parágrafo devem também garantir a divulgação, aos clientes e às contrapartes, numa base anual, de uma síntese de todos os incidentes relacionados com as TIC. Esta comunicação deve respeitar plenamente o segredo profissional da entidade financeira e dos respetivos clientes e contrapartes e não deve colocar em perigo o quadro de gestão do risco associado às TIC a que se refere o artigo 5.º, n.º 1.
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 ***graves*** relacionados com as TIC***, no mínimo,*** 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***, e sem atrasos injustificados***;

(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.

Artigo 14.º-A

Quadro de gestão do risco associado às TIC para as entidades de pequena dimensão, não interligadas e isentas

1. Nos termos do artigo 3.º-A, as pequenas empresas de investimento ou instituições de

pagamento não interligadas isentas ao abrigo da Diretiva (UE) 2015/2366, as instituições de crédito isentas ao abrigo da Diretiva 2013/36/UE, as instituições de moeda eletrónica isentas ao abrigo da Diretiva 2009/110/CE e as pequenas instituições de planos de pensões profissionais devem implementar e manter um quadro de gestão do risco associado às TIC robusto e documentado, que deve:

(a) Especificar os mecanismos e as medidas destinados a uma gestão rápida, eficiente e abrangente de todos os riscos associados às TIC, incluindo para a proteção de componentes e infraestruturas físicas pertinentes;

(b) Controlar continuamente a segurança e o funcionamento de todos os sistemas TIC;

(c) Minimizar o impacto dos riscos associados às TIC através da utilização de sistemas, protocolos e ferramentas TIC sólidos, resilientes e atualizados que sejam adequados para apoiar o desempenho das suas atividades e a prestação de serviços;

(d) Proteger adequadamente a confidencialidade, a integridade e a disponibilidade das redes de dados e dos sistemas de informação;

(e) Permitir que as fontes de risco e anomalias na rede e nos sistemas de informação sejam rapidamente identificadas e detetadas e que os incidentes das TIC sejam tratados rapidamente.

2. 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.

Deve ser apresentado anualmente à autoridade competente um relatório de análise do quadro de gestão do risco no domínio das TIC.

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 ***procedimentos e*** 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 ***sanadas*** 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***, no mínimo,*** 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 ***graves*** 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 ▌;

(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 ***em coordenação com o*** 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 ***graves*** 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 ainda ter em conta que a gestão atempada e eficiente de um incidente por parte das micro e pequenas empresas não é limitada pela necessidade de respeitar os requisitos de classificação estabelecidos no presente artigo. As AES têm também em conta a dimensão das entidades financeiras, a natureza, a escala e a complexidade dos seus serviços, atividades e operações, bem como o seu perfil de risco global.***

As AES devem apresentar esses projetos de normas técnicas de regulamentação comuns à Comissão até [Serviço das Publicações: inserir a data correspondente ***a dois anos*** 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 graves 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.

1-A. As entidades financeiras podem, a título voluntário, notificar a autoridade competente pertinente da existência de ciberameaças significativas nos casos em que considerem essas ameaças relevantes para o sistema financeiro, os utilizadores ou os clientes do serviço. A autoridade competente pertinente pode fornecer essas informações a outras autoridades pertinentes, em conformidade com o n.º 5.

2. Quando um incidente grave relacionado com as TIC ***ocorra e tenha um impacto significativo*** nos interesses financeiros dos utilizadores e clientes do serviço, as entidades financeiras devem, sem demora indevida ***após terem tomado conhecimento do incidente***, informar os utilizadores e clientes dos seus serviços acerca do incidente grave relacionado com as TIC e ▌***das*** medidas ***pertinentes*** que foram tomadas para atenuar os efeitos adversos desse incidente. ***Se não se verificarem danos para os utilizadores e clientes do serviço devido às contramedidas tomadas pela entidade financeira, não se aplica o requisito de informar os utilizadores e os clientes do serviço.***

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

   (a) Uma notificação inicial ▌***do*** incidente grave relacionado com as TIC***, que deve conter as informações de que a entidade notificadora dispõe com base nos melhores esforços, como a seguir indicado:***

      i) no caso de incidentes que perturbem significativamente a disponibilidade dos serviços prestados pela entidade financeira, a autoridade competente deve ser notificada sem demora injustificada e, em qualquer caso, no prazo de 24 horas após ter tomado conhecimento do incidente,

      ii) no caso de incidentes que tenham um impacto significativo na entidade financeira, mas não na disponibilidade dos serviços prestados por essa entidade financeira, a autoridade competente deve ser notificada sem demora injustificada e, em qualquer caso, no prazo de 72 horas após ter tomado conhecimento do incidente,

      iii) no caso de incidentes que tenham impacto na integridade, confidencialidade ou segurança dos dados pessoais conservados por essa entidade financeira, a autoridade competente deve ser notificada sem demora injustificada e, em qualquer caso, no prazo de 24 horas após ter tomado conhecimento do incidente;

(b) Um relatório intercalar, ***assim que se verifique uma evolução significativa do estado do incidente ou se tenha conhecimento de novas informações suscetíveis de ter um grande impacto na forma como o incidente relacionado com as TIC é resolvido pela autoridade competente,*** 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 ***da data*** em que foi enviado o relatório inicial;

(c-A) Caso o incidente esteja em curso no momento da apresentação do relatório final referido na alínea c), deve ser apresentado um relatório final um mês depois de o incidente ser resolvido.

A autoridade competente pertinente a que se refere o artigo 41.º deve prever que, em casos devidamente justificados, uma entidade financeira seja autorizada a desviar-se dos prazos estabelecidos nas alíneas a), b), c) e c-A) do presente número, tendo devidamente em conta a capacidade das entidades financeiras de facultar informações exatas e pertinentes em relação a incidentes graves relacionados com as TIC.

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. ***Em caso de delegação, a entidade financeira continua a ser plenamente responsável pelo cumprimento dos requisitos de comunicação de incidentes.***

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

(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 ***ou às CSIRT designadas nos termos do artigo 9.º da Diretiva (UE) 2016/1149;***

(c-A) À autoridade de resolução responsável pela entidade financeira em causa. Ao Conselho Único de Resolução (CUR), para as entidades a que se refere o artigo 7.º, n.º 2, do Regulamento (UE) n.º 806/2014, e para as entidades e os grupos referidos no artigo 7.º, n.º 4, alínea b), e no artigo 7.º, n.º 5, do Regulamento (UE) n.º 806/2014, se estiverem reunidas as condições para a aplicação desses números;

(c-B) Às autoridades nacionais de resolução, em relação às entidades e aos grupos a que se refere o artigo 7.º, n.º 3, do Regulamento (UE) n.º 806/2014. As autoridades nacionais de resolução devem apresentar ao CUR, trimestralmente, uma síntese dos relatórios que tenham recebido nos termos da presente alínea em relação às entidades e aos grupos a que se refere o artigo 7.º, n.º 3, do Regulamento (UE) n.º 806/2014;

(c-C) A outras autoridades públicas pertinentes, incluindo as de outros Estados-Membros.

6. A EBA, a ESMA ou a EIOPA e o BCE***, em cooperação com a ENISA,*** 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,

(3) especificar mais pormenorizadamente os critérios para determinar o impacto de um incidente grave relacionado com as TIC numa entidade financeira para efeitos do artigo 17.º, n.º 3, alínea a);

(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 ***primeiro parágrafo***, alínea a), e os projetos de normas técnicas de execução referidos no ***primeiro parágrafo***, alínea b), à Comissão até xx 202x [Serviço das Publicações: inserir a data correspondente a ***dois anos*** 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 ***primeiro parágrafo***, 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 ***primeiro parágrafo***, 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.

2. Na pendência do resultado do relatório de viabilidade a que se refere o artigo 19.º sobre uma maior centralização da comunicação de incidentes, as AES, através do Comité Conjunto e em colaboração com as autoridades competentes, o BCE, o CUR e a ENISA, devem elaborar orientações para o intercâmbio de informações no âmbito da comunicação de incidentes graves relacionados com as TIC, em conformidade com o artigo 17.º, n.º 5.

As orientações a que se refere o primeiro parágrafo devem ter em conta pelo menos o seguinte:

(a) as linhas de comunicação mais eficazes;

(b) a preservação da segurança, confidencialidade e integridade dos dados objeto de intercâmbio;

(c) a possível participação das entidades financeiras para complementar o intercâmbio de informações a que se refere o artigo 40.º.

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 pelas 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 ***de uma*** plataforma ***única***;

(b) Benefícios, limitações e possíveis riscos;

(b-A) Capacidade para estabelecer a interoperabilidade e avaliar o seu valor acrescentado em relação a outros sistemas de comunicação de informações pertinentes, tais como a Diretiva (UE) 2016/1148;

(c) Elementos de gestão operacional;

(d) Condições de participação;

(e) Modalidades de acesso à plataforma ***única*** 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 ***única***, 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 como o 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***, e também enviar observações, conhecimentos e informações devidamente anonimizados a todas as entidades financeiras pertinentes nos casos em que tal possa ser vantajoso, com base na comunicação de qualquer incidente grave relacionado com as TIC que receba***.

2. As AES, através do Comité Conjunto, devem comunicar anualmente informações, numa base anónima e agregada, sobre as notificações ***relativas a relatórios de*** incidentes ***graves*** 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 ***estimados*** 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.

Artigo 20.º-A

Incidentes operacionais ou de segurança relacionados com os pagamentos que digam respeito a determinadas entidades financeiras

Os requisitos estabelecidos no presente capítulo são igualmente aplicáveis aos incidentes operacionais ou de segurança relacionados com os pagamentos, independentemente da sua gravidade, que digam respeito às entidades financeiras a que se refere o artigo 2.º, n.º 1, alíneas a), b) e c).

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***, excluindo as microempresas,*** devem estabelecer, manter e rever ▌ 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. ***Se for um responsável interno a realizar os testes, as entidades financeiras devem afetar recursos suficientes e garantir que são evitados conflitos de interesses ao longo das fases de conceção e execução dos testes.***

5. As entidades financeiras devem estabelecer procedimentos e políticas para dar prioridade, classificar e ***abordar*** 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 ***assegurar-se de que são realizados testes apropriados*** pelo menos anualmente ***a*** 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.

Estes testes podem incluir 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 ***3, segundo parágrafo,*** 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 ***ou importantes*** de uma entidade financeira e devem ser realizados em sistemas de produção ativos que apoiem essas funções***, se possível, ou em sistemas de pré-produção com uma configuração de segurança idêntica***. O âmbito exato dos testes de penetração motivados por ameaças, baseado na avaliação das funções e dos serviços críticos ***ou importantes***, deve ser determinado pelas entidades financeiras e validado pelas autoridades competentes. ***Não deve exigir-se que um único teste de penetração motivado por ameaças abranja todas as funções críticas ou importantes.***

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

   Quando as entidades terceiras prestadoras de serviços ***críticos*** no domínio das TIC ***e, se necessário, as entidades terceiras prestadoras de serviços não críticos 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. ***Essas entidades terceiras prestadoras de serviços no domínio das TIC não devem ser obrigadas a comunicar informações ou a fornecer quaisquer pormenores em relação a elementos que não sejam pertinentes para os controlos da gestão de riscos das funções críticas ou importantes das entidades financeiras pertinentes. Esses testes não devem afetar negativamente outros clientes das entidades terceiras prestadoras de serviços no domínio das TIC.***

   Nos casos em que a participação de uma entidade terceira prestadora de serviços no domínio das TIC nos testes de penetração motivados por ameaças possa ter potencial impacto na qualidade, confidencialidade ou segurança dos serviços prestados por essa entidade a outros clientes que não estejam abrangidos pelo âmbito de aplicação do presente regulamento, ou na integridade global das operações da entidade terceira prestadora de serviços no domínio das TIC, esta e a entidade financeira podem acordar contratualmente que a primeira está autorizada a celebrar diretamente acordos contratuais com um responsável externo pela realização dos testes. As entidades terceiras prestadoras de serviços no domínio das TIC podem celebrar tais acordos em nome de todos os seus utilizadores de serviços de entidades financeiras a fim de realizar testes conjuntos.

   As entidades financeiras devem aplicar controlos eficazes de gestão do risco para ***atenuar*** os riscos de quaisquer potenciais impactos nos dados, danos nos ativos e perturbações ***nas funções*** ou nas operações críticas ***ou importantes*** 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 pública única, designada em conformidade com o n.º 3-A, ou, caso as entidades terceiras prestadoras de serviços no domínio das TIC celebrem diretamente acordos contratuais com responsáveis externos pela realização dos testes, à ENISA, uma síntese confidencial dos resultados do teste e*** a documentação que confirma que os testes de penetração motivados por ameaças foram realizados em conformidade com os requisitos. ***A autoridade pública única ou a ENISA, consoante o caso, deve*** emitir um comprovativo ***que certifique que o teste foi realizado em conformidade com os requisitos estabelecidos na documentação, a fim de permitir o reconhecimento mútuo, por parte das autoridades competentes, dos testes de penetração motivados por ameaças***. ***O comprovativo deve ser enviado à autoridade competente da entidade financeira e, se for caso disso, à autoridade fiscalizadora principal da entidade terceira prestadora de serviços críticos no domínio das TIC.***

3. As entidades financeiras***, ou as entidades terceiras prestadoras de serviços no domínio das TIC autorizadas a celebrar diretamente acordos contratuais com um responsável externo pela realização dos testes nos termos do n.º 2 do presente artigo,*** 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.

Sem prejuízo da sua capacidade para delegar atribuições e competências ao abrigo do presente artigo noutras autoridades competentes responsáveis pelos 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 ***proporcionada*** ▌, 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.

3-A. Os Estados-Membros devem designar uma autoridade pública única responsável pelos testes de penetração motivados por ameaças no setor financeiro a nível nacional, exceto no que se refere à identificação das entidades financeiras em conformidade com o n.º 3, incluindo os testes de penetração motivados por ameaças realizados por entidades financeiras e por entidades terceiras prestadoras de serviços no domínio das TIC que celebrem diretamente acordos contratuais com responsáveis externos pela realização dos testes. São confiadas à autoridade pública única designada todas as competências e atribuições para esse efeito.

4. ***As AES*** devem, ***em coordenação com a ENISA,*** após consulta do BCE e tendo em conta os quadros pertinentes na União aplicáveis aos testes de penetração ***motivados por ameaças e*** baseados em informações confidenciais, ***incluindo o quadro TIBER-UE,*** desenvolver ***um conjunto de*** projetos de normas técnicas de regulamentação que especifiquem mais pormenorizadamente:

(a) Os critérios utilizados para fins de aplicação do n.º ***3, segundo parágrafo,*** do presente artigo;

(b) Os requisitos relativos:

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

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

iii) 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 ***e o pleno reconhecimento mútuo*** dos testes de penetração motivados por ameaças no contexto das entidades financeiras que operam em mais do que um Estado-Membro ***e dos testes efetuados por responsáveis externos que tenham celebrado diretamente acordos contratuais com entidades terceiras prestadoras de serviços no domínio das TIC em conformidade com o n.º 2 do presente artigo***, 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 ***6*** 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 ***e as entidades terceiras prestadoras de serviços no domínio das TIC autorizadas a celebrar diretamente acordos contratuais com um responsável externo pela realização dos testes nos termos do artigo 23.º, n.º 2,*** 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***, independentemente de serem provenientes da União ou de um país terceiro***;

(d) ▌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) ▌Estejam devida e totalmente cobertos por seguros de indemnização profissional relevantes, nomeadamente contra riscos de conduta irregular e negligência;

(e-A) No caso dos responsáveis internos, tenham sido aprovados pela autoridade competente pertinente e pela autoridade pública única designada em conformidade com o artigo 23.º, n.º 3-A, devendo essas autoridades verificar que a entidade financeira afetou recursos suficientes e garantiu que são evitados conflitos de interesses ao longo das fases de conceção e execução do teste.

2. As entidades financeiras ***e as entidades terceiras prestadoras de serviços no domínio das TIC autorizadas a celebrar diretamente acordos contratuais com um responsável externo pela realização dos testes em conformidade com o artigo 23.º, n.º 2,*** 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 ***natureza, 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;

(b-A) Se uma entidade prestadora de serviços no domínio das TIC é uma entidade intragrupo.

3. Como parte do seu quadro de gestão do risco associado às TIC, as entidades financeiras***, excluindo as microempresas,*** devem adotar e rever periodicamente uma estratégia para o risco de terceiros no domínio das TIC ▌. 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 ***de apoio a funções críticas ou importantes*** prestados por entidades terceiras.

Os contratos referidos no primeiro parágrafo devem ser devidamente documentados ▌.

Quando disponíveis, as entidades financeiras devem seguir as orientações e outras medidas emitidas pelas AES e pelas autoridades competentes até à entrada em vigor das normas técnicas de execução a que se refere o n.º 10.

As entidades financeiras devem comunicar pelo menos anualmente às autoridades competentes informações sobre o número de novos contratos relativos à utilização de serviços TIC ***de apoio a funções críticas ou importantes***, 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 ***atualizadas***. ***Devem também ser tidas em conta as normas mais recentes para determinar se as normas de segurança em vigor são apropriadas.***

7. Ao exercer direitos de acesso, inspeção e auditoria sobre a entidade terceira prestadora de serviços no domínio das TIC ***relativamente a funções críticas ou importantes***, 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 ***uma detalhada*** 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 ▌***os*** contratos relativos à utilização de

serviços no domínio das TIC ***permitam que as entidades financeiras tomem as medidas corretivas adequadas, que podem incluir a rescisão total dos contratos, se não for possível qualquer retificação, ou a sua rescisão parcial, se tal for possível, nos termos da legislação aplicável,*** pelo menos nas seguintes circunstâncias:

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

(a-A) Recomendação emitida pelo órgão conjunto de fiscalização, nos termos do artigo 37.º, a uma entidade terceira prestadora de serviços no domínio das TIC considerada crítica;

(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 ***que digam respeito à*** gestão global do risco associado às TIC ***prevista no seu contrato com a entidade financeira*** 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***, claramente,*** de poder supervisionar com eficácia a entidade financeira em resultado do acordo contratual respetivo.

8-A. A fim de reduzir o risco de perturbações a nível da entidade financeira, em circunstâncias devidamente justificadas e com o acordo das respetivas autoridades competentes, a entidade financeira pode decidir não rescindir o acordo contratual com a entidade terceira prestadora de serviços no domínio das TIC até poder substituir esta última ou recorrer a soluções internas, coerentes com a complexidade do serviço prestado, em conformidade com a estratégia de saída a que se refere o n.º 9.

8-B. Nos casos em que os acordos contratuais com entidades terceiras prestadoras de serviços no domínio das TIC sejam rescindidos em qualquer das circunstâncias enumeradas no n.º 8, alíneas a) a d), as entidades financeiras não devem suportar o custo da transferência de dados de uma entidade terceira prestadora de serviços no domínio das TIC, se essa transferência exceder o custo da transferência de dados previsto no contrato inicial.

9. ***No que respeita aos serviços no domínio das TIC relacionados com funções críticas ou importantes,*** as entidades financeiras devem dispor de estratégias de saída***, que devem ser revistas regularmente***. ***As estratégias de saída devem ter*** em conta riscos que possam surgir ao nível das entidades terceiras prestadoras 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***, ou em caso de rescisão dos acordos contratuais com as entidades terceiras prestadoras de serviços no domínio das TIC em qualquer das circunstâncias enumeradas no n.º 8, alíneas a) a d)***.

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 ***18 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 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 ***de apoio a funções críticas ou importantes*** pode conduzir a qualquer uma 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 ***de apoio a funções críticas ou importantes*** 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 ***de apoio a funções críticas ou importantes*** 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 ▌ .

Quando os contratos relativos à utilização de serviços no domínio das TIC ***de apoio a funções críticas ou importantes*** são celebrados com uma entidade terceira prestadora de serviços no domínio das TIC ▌ , as entidades financeiras devem considerar como relevantes pelo menos os seguintes fatores:

(a) ▌

(b) ▌

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

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

Quando os contratos relativos à utilização de serviços no domínio das TIC de apoio a funções críticas ou importantes são celebrados com uma entidade terceira prestadora de serviços no domínio das TIC estabelecida num país terceiro, as entidades financeiras devem ter igualmente em conta, para além das considerações referidas no primeiro e no segundo parágrafos, o seguinte:

i) o respeito pelas normas da União em matéria de proteção de dados, e

ii) a efetiva aplicação das normas estipuladas no presente regulamento.

Quando os referidos contratos prevejam a subcontratação de funções críticas ou importantes, 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 ***analisar os fatores enunciados no segundo e no terceiro parágrafos para*** 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 ***ser formalizado por escrito e colocado à disposição das*** partes em papel ou num formato que permita o acesso e a descarga.

2. ***As entidades financeiras e as entidades terceiras prestadoras de serviços no domínio das TIC devem assegurar que*** os contratos relativos à utilização de serviços no domínio das TIC ***incluem*** 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***, nomeadamente as regiões ou os países,*** onde as funções e os serviços ***no domínio das TIC*** 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 ***antecipadamente*** a entidade financeira se planear mudar de local;

   (c) Disposições sobre a acessibilidade, disponibilidade, integridade, segurança***, confidencialidade*** e proteção dos ***dados, incluindo os*** dados pessoais;

   (c-A) Disposições 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***, ou em caso de rescisão dos contratos***;

   (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) ▌

   (f) A obrigação de a entidade terceira prestadora de serviços no domínio das TIC prestar assistência em caso de incidente ***de TIC relacionado com o serviço prestado,*** 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 ***um nível adequado de segurança na*** prestação de serviços ▌ por parte da entidade financeira em consonância com o seu quadro regulamentar;

(h) ▌

(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 ***e das autoridades de resolução, e, quando esse contrato afete uma entidade prestadora de serviços intragrupo no domínio das TIC pertencente ao mesmo grupo, uma análise efetuada de acordo com uma abordagem baseada no risco***;

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

i) 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 ***ou assegurar a sua resolução e reestruturação efetivas***,

ii) 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,

ii-A) se esse contrato afetar uma entidade prestadora de serviços intragrupo no domínio das TIC pertencente ao mesmo grupo, deve ser analisado de acordo com uma abordagem baseada no risco;

(k-A) Uma disposição sobre o tratamento de dados pessoais pela entidade terceira prestadora de serviços no domínio das TIC em conformidade com o Regulamento (UE) 2016/679.

2-A. Os contratos celebrados para o exercício de funções críticas ou importantes incluem, para além do disposto no n.º 2, pelo menos os seguintes elementos:

(a) 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;

(b) 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 examinar cópias da documentação importante no local, caso seja crítica para as operações da entidade terceira prestadora de serviços no domínio das TIC, 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 por parte da entidade terceira prestadora de serviços no domínio das TIC durante as inspeções e auditorias no local realizadas pelas autoridades competentes, pela autoridade fiscalizadora principal, pela entidade financeira ou por um terceiro designado e pormenores sobre o âmbito, as modalidades e a frequência das referidas inspeções e auditorias.

Em derrogação da alínea b), a entidade terceira prestadora de serviços no domínio das TIC e a entidade financeira podem decidir que os direitos de acesso, inspeção e auditoria podem ser delegados num terceiro independente, nomeado pela entidade terceira prestadora de serviços no domínio das TIC, e que a entidade financeira pode requerer, a qualquer momento, informações e garantias sobre o desempenho da entidade terceira prestadora de serviços no domínio das TIC.

2-B. Para além do disposto nos n.os 2 e 2-A do presente artigo, os acordos contratuais para a prestação de serviços no domínio das TIC por uma entidade terceira prestadora de serviços no domínio das TIC estabelecida num país terceiro e designada como crítica nos termos do artigo 28.º, n.º 9, devem:

(a) Estipular que o contrato é regido pelo direito de um Estado-Membro; e

(b) Garantir que o órgão conjunto de fiscalização e a autoridade fiscalizadora principal possam desempenhar as suas funções especificadas no artigo 30.º com base nas competências que lhes são atribuídas no artigo 31.º.

Não é exigido que os serviços para os quais são celebrados os acordos contratuais sejam prestados pela empresa constituída na União ao abrigo do direito de um Estado-Membro.

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.

3-A. ***As autoridades competentes devem poder aceder aos acordos contratuais a que se refere o presente artigo. As partes nesses acordos contratuais podem acordar em ocultar informações comercialmente sensíveis ou confidenciais antes de conceder esse acesso às autoridades competentes, desde que estas últimas sejam plenamente informadas do alcance e da natureza das ocultações.***

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). ***Ao elaborarem esses projetos de normas técnicas de regulamentação, as AES devem ter em conta a dimensão das entidades financeiras, a natureza, a escala e a complexidade dos seus serviços, atividades e operações, bem como o seu perfil de risco global.***

As AES devem apresentar esses projetos de normas técnicas de regulamentação à Comissão até [Serviço das Publicações: inserir a data correspondente a ***18 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 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 ***Órgão*** de Fiscalização criado nos termos do artigo 29.º, n.º 1, devem ***,após consulta da ENISA***:

   (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.

   A autoridade fiscalizadora principal nomeada nos termos do n.º 1, alínea b), é responsável pela supervisão diária da entidade terceira prestadora de serviços no domínio das TIC considerada crítica.

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;

(f-A) A materialidade e a importância dos serviços prestados pela entidade terceira prestadora de serviços no domínio das TIC pertinente.

2-A. O órgão conjunto de fiscalização notifica a entidade terceira prestadora de serviços no domínio das TIC antes de iniciar a sua avaliação para efeitos da designação a que se refere o n.º 1, alínea a).

O órgão conjunto de fiscalização notifica a entidade terceira prestadora de serviços no domínio das TIC do resultado da avaliação a que se refere o primeiro parágrafo, apresentando um projeto de recomendação relativo à criticidade. No prazo de 6 semanas a contar da data de receção do projeto de recomendação, a entidade terceira prestadora de serviços no domínio das TIC pode apresentar ao órgão conjunto de fiscalização uma declaração fundamentada sobre a avaliação. Essa declaração fundamentada deve conter todas as informações adicionais pertinentes consideradas adequadas pela entidade terceira prestadora de serviços no domínio das TIC, a fim de confirmar a exaustividade e a exatidão do procedimento de designação ou contestar o projeto de recomendação relativo à criticidade. O Comité Conjunto das AES tem devidamente em conta a declaração fundamentada e pode solicitar informações ou elementos de prova adicionais à entidade terceira prestadora de serviços no domínio das TIC antes de tomar uma decisão sobre a designação.

O Comité Conjunto das AES notifica a entidade terceira prestadora de serviços no

domínio das TIC da sua designação como crítica. A entidade terceira prestadora de serviços no domínio das TIC dispõe de pelo menos três meses, a contar da data de receção da notificação, para efetuar os ajustamentos necessários para permitir que o órgão conjunto de fiscalização desempenhe as suas funções nos termos do artigo 30.º, bem como para notificar as entidades financeiras a que a entidade terceira prestadora de serviços no domínio das TIC presta os seus serviços. O órgão conjunto de fiscalização pode permitir que o período de ajustamento seja prorrogado por um período máximo de três meses, mediante pedido devidamente justificado da entidade terceira prestadora de serviços no domínio das TIC designada.

3. A Comissão fica habilitada a adotar ***um ato delegado*** em conformidade com o artigo 50.º que ***especifique*** 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. ***O órgão conjunto de fiscalização, em consulta com a ENISA, deve*** 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 ***órgão conjunto de fiscalização*** criado nos termos do artigo 29.º. O ***órgão conjunto 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.

8-A. O Comité Conjunto das AES, sob recomendação do órgão conjunto de fiscalização, designa as entidades terceiras prestadoras de serviços no domínio das TIC estabelecidas num país terceiro que sejam consideradas críticas para as entidades financeiras nos termos do n.º 1, alínea a).

Ao procederem à designação a que se refere o primeiro parágrafo do presente número, as AES e o órgão conjunto de fiscalização devem seguir as etapas processuais estabelecidas no n.º 2-A.

9. As entidades financeiras não devem recorrer a uma entidade terceira prestadora de serviços no domínio das TIC ***considerada crítica que esteja*** estabelecida num país terceiro***, salvo se essa entidade terceira prestadora de serviços no domínio das TIC***

tiver uma empresa constituída na União ao abrigo do direito de um Estado-Membro e tiver celebrado acordos contratuais em conformidade com o artigo 27.º, n.º 2-B.

Artigo 29.º

Estrutura do quadro de fiscalização

1. O ***órgão conjunto de fiscalização é criado*** para efeitos de ***supervisão*** do risco de terceiros no domínio das TIC em todos os setores financeiros ***e de supervisão direta das entidades terceiras prestadoras de serviços no domínio das TIC designadas como críticas nos termos do artigo 28.º***.

   O papel do órgão conjunto de fiscalização deve limitar-se às competências de fiscalização relacionadas com os riscos associados às TIC no que respeita aos serviços no domínio das TIC prestados às entidades financeiras por entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas.

   O ***órgão conjunto de fiscalização*** debate periodicamente os desenvolvimentos mais importantes associados aos riscos e às vulnerabilidades das TIC e promove uma abordagem coerente na monitorização do risco de terceiros associado às TIC ao nível da União.

2. O ***órgão conjunto de fiscalização*** realiza, 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 promove 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.

   O ***órgão conjunto de fiscalização*** apresenta 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.

3. O ***órgão conjunto de fiscalização*** é composto pelos ***administradores executivos*** das AES, por um representante de alto nível do pessoal atualmente em funções nas ***AES e por um representante de alto nível de, pelo menos, oito das autoridades nacionais competentes***. Um representante da Comissão Europeia, do CERS, do BCE e da ENISA ***e, pelo menos, um perito independente designado em conformidade com o n.º 3 do presente artigo*** participam ▌ na qualidade de observadores.

   Após a designação anual de entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas nos termos do artigo 28.º, n.º 1, alínea a), o Comité Conjunto das AES decide quais as autoridades nacionais competentes que são membros do órgão conjunto de fiscalização, tendo em conta os seguintes fatores:

   (a) O número de entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas que estão estabelecidas ou que prestam serviços num Estado-Membro;

   (b) A dependência das entidades financeiras de um Estado-Membro em relação a entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas;

(c) Os conhecimentos especializados relativos de uma autoridade nacional competente;

(d) Os recursos e a capacidade disponíveis de uma autoridade nacional competente;

(e) A necessidade de racionalizar, simplificar e tornar eficiente o funcionamento e a tomada de decisões do órgão conjunto de fiscalização.

O órgão conjunto de fiscalização partilha a sua documentação e as suas decisões com todas as autoridades nacionais competentes que não sejam membros do órgão conjunto de fiscalização.

O trabalho do órgão conjunto de fiscalização beneficia do apoio e da assistência de pessoal especificamente destacado de todas as AES.

3 A. O perito independente a que se refere o n.º 3 do presente artigo é designado como observador pelo organismo comum de supervisão na sequência de um processo de candidatura público e transparente.

O perito independente é designado, com base nos seus conhecimentos especializados em matéria de estabilidade financeira, resiliência operacional digital e segurança das TIC, para um mandato de dois anos.

O perito independente designado não é titular de qualquer cargo a nível nacional, internacional ou da União. O perito independente age de forma independente e objetiva no interesse exclusivo da União no seu conjunto e não procura obter nem receber instruções das instituições ou órgãos da União, dos governos dos Estados-Membros nem de qualquer outro organismo público ou privado.

O órgão conjunto de fiscalização pode decidir designar mais do que um observador independente.

4. 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 ***até [Serviço das Publicações: inserir a data correspondente a 18 meses após a data de entrada em vigor],*** sobre a cooperação entre ***o órgão conjunto de fiscalização, a autoridade fiscalizadora principal*** 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 ***o órgão conjunto de fiscalização*** e sobre os pormenores relativos aos intercâmbios de informações necessários para que as autoridades competentes possam assegurar o acompanhamento das recomendações ***do órgão conjunto de fiscalização*** nos termos do artigo 31.º, n.º 1, alínea d), dirigidas às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas.

5. 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.

6. ***O órgão conjunto de fiscalização*** apresenta 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***, nomeada nos termos do artigo 28.º, n.º 1, alínea***

b), deve liderar e coordenar a fiscalização diária das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas e ser o principal ponto de contacto para essas entidades.

1-A. ***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. ***A referida avaliação centra-se principalmente nos serviços de TIC que apoiam as funções críticas ou importantes exercidas pelas entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas a entidades financeiras, mas pode também ser mais abrangente, se relevante para a avaliação dos riscos para essas funções.***

2. A avaliação referida no n.º ***1-A*** 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 ***graves*** 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, levada a cabo pela*** Autoridade Fiscalizadora Principal***, o órgão conjunto de fiscalização, sob a coordenação e orientação da Autoridade Fiscalizadora Principal, elabora e propõe*** um plano de fiscalização individual claro, pormenorizado e fundamentado para cada entidade terceira prestadora de serviços no domínio das TIC considerada crítica.

   Ao elaborar o projeto de plano de fiscalização, o órgão conjunto de fiscalização deve consultar todas as autoridades competentes pertinentes e os pontos únicos de contacto

a que se refere o artigo 8.º da Diretiva (UE) 2016/1148, a fim de assegurar que não existem incoerências ou duplicações com as obrigações da entidade terceira prestadora de serviços no domínio das TIC considerada crítica nos termos da referida diretiva.

O plano de fiscalização é adotado anualmente pelo conselho de administração da Autoridade Fiscalizadora Principal.

Antes da sua adoção, o projeto de plano de fiscalização é comunicado à entidade terceira prestadora de serviços no domínio das TIC considerada crítica.

Após a receção do projeto de plano de fiscalização, a entidade terceira prestadora de serviços no domínio das TIC considerada crítica dispõe de um período de seis semanas para rever o projeto de plano de fiscalização e apresentar uma declaração fundamentada. Essa declaração fundamentada só pode ser apresentada caso a entidade terceira prestadora de serviços no domínio das TIC considerada crítica possa apresentar provas de que a execução do plano de fiscalização produziria um impacto desproporcionado ou uma perturbação para os clientes não abrangidos pelo presente regulamento ou de que existe uma solução mais eficaz ou eficiente para gerir os riscos no domínio das TIC identificados. Caso uma tal declaração seja apresentada, a entidade terceira prestadora de serviços no domínio das TIC considerada crítica sugere ao órgão conjunto de fiscalização uma solução mais eficaz ou eficiente para alcançar os objetivos do projeto de plano de fiscalização.

Antes de adotar o plano de fiscalização, o conselho de administração da Autoridade Fiscalizadora Principal tem devidamente em conta a declaração fundamentada e pode solicitar informações ou elementos de prova adicionais ao terceiro prestador de serviços de TIC.

4. Depois de os planos anuais de fiscalização referidos no n.º 3 ***terem sido aprovados*** e 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 o ***órgão conjunto de fiscalização***.

Artigo 31.º

Poderes ***de fiscalização***

1. Para efeitos da execução das funções definidas na presente secção, a Autoridade Fiscalizadora Principal***, no que diz respeito aos serviços prestados a entidades financeiras por entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas,*** fica habilitada a:

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

   (b) Realizar investigações de caráter geral e inspeções ***no local*** 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 ***no n.º 1-A***;

1-A. Para efeitos da execução das funções definidas na presente secção e com base nas informações obtidas pela Autoridade Fiscalizadora Principal e nos resultados das

investigações realizadas pela Autoridade Fiscalizadora Principal, o órgão conjunto de fiscalização fica habilitado a: 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 ***o órgão conjunto de fiscalização*** 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 ***o órgão conjunto de fiscalização*** 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 ***o órgão conjunto de fiscalização*** 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 previsto é uma entidade terceira prestadora de serviços no domínio das TIC ou um subcontratante nesse domínio estabelecido num país terceiro ***e que não tem uma empresa constituída na União ao abrigo do direito de um Estado-Membro***,

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

– ***a subcontratação resultará em riscos graves e evidentes para a entidade financeira ou para a estabilidade financeira do sistema financeiro da União.***

1-B. Os poderes referidos nos n.os 1 e 1-A devem ser exercidos no que diz respeito aos serviços de TIC que apoiam funções não críticas ou importantes fornecidas pela entidade terceira prestadora de serviços no domínio das TIC considerada crítica, quando necessário.

1-C. No exercício dos poderes referidos nos n.os 1 e 1-A do presente artigo, a Autoridade Fiscalizadora Principal e o órgão conjunto de fiscalização devem ter devidamente em conta o quadro estabelecido pela Diretiva (UE) 2016/1148 e, se necessário,

consultar as autoridades competentes pertinentes estabelecidas por essa diretiva, a fim de evitar uma duplicação desnecessária de medidas técnicas e organizativas que possam ser aplicadas às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas nos termos dessa diretiva.

2. ***Antes de finalizar e emitir recomendações em conformidade com o n.º 1-A, o órgão conjunto de fiscalização deve informar a entidade terceira prestadora de serviços no domínio das TIC considerada crítica a respeito das suas intenções e dar a oportunidade a essa entidade de fornecer informações sempre que esta esteja razoavelmente convencida de que tais informações devem ser tidas em conta antes de a recomendação ser finalizada ou a fim de contestar as recomendações previstas. Os motivos para contestar uma recomendação podem incluir o potencial impacto desproporcionado dessa recomendação ou a existência de uma perturbação para os clientes não abrangidos pelo presente regulamento ou a existência de uma solução mais eficaz ou eficiente para gerir o risco identificado***.

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

4. A Autoridade Fiscalizadora Principal pode***, em caso de incumprimento total ou parcial das medidas que teriam de ser tomadas nos termos do n.º 1, alíneas a), b) ou c), no prazo de 60 dias de calendário a contar da data em que a entidade terceira prestadora de serviços no domínio das TIC considerada crítica recebeu a notificação da medida, decidir*** impor uma sanção pecuniária periódica para obrigar a entidade terceira prestadora de serviços no domínio das TIC considerada crítica a cumprir.

4-A. A sanção pecuniária periódica referida no n.º 4 deve ser imposta pela Autoridade Fiscalizadora Principal apenas em último recurso e nos casos em que a entidade terceira prestadora de serviços no domínio das TIC considerada crítica não tenha cumprido as medidas exigidas nos termos do n.º 1, alíneas a), b) ou c).

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 ***até*** 1 % do volume de negócios mundial médio diário ***relativo aos serviços prestados às entidades financeiras abrangidas pelo presente regulamento*** 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.

   As entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas só devem ser obrigadas a prestar as informações referidas no primeiro parágrafo relativamente às entidades financeiras abrangidas pelo presente regulamento que utilizem os serviços das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas para funções críticas ou importantes. As entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas notificam a entidade financeira pertinente dos pedidos que dizem respeito a essa entidade financeira.

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***, mediante uma decisão,*** 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 ***razoável*** 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 ***ou não serem fornecidas no prazo referido na alínea d)***;

(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 ***35.º***, n.º 1, pode realizar as investigações necessárias junto das entidades terceiras prestadoras de serviços no domínio das TIC***, em conformidade com o princípio da proporcionalidade. Ao realizar investigações, a Autoridade Fiscalizadora Principal deve exercer prudência e assegurar a proteção dos direitos dos clientes da entidade terceira prestadora de serviços no domínio das TIC considerada crítica que não são abrangidos pelo presente regulamento, nomeadamente em relação ao impacto nos níveis de serviço, na disponibilidade dos dados e na confidencialidade.***

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) ***Analisar, de forma segura,*** 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.

O poder de realizar as inspeções no local referidas no primeiro parágrafo não se limita aos sítios na União, na condição de a inspeção de um sítio num país terceiro cumprir cumulativamente os seguintes requisitos:

- ***Ser necessária para que a Autoridade Fiscalizadora Principal cumpra as suas obrigações ao abrigo do presente regulamento;***
- ***Ter uma ligação direta com a prestação de serviços no domínio das TIC a entidades financeiras da União;***
- ***Ser pertinente para uma investigação em curso.***

1-A. Ao realizar inspeções no local, a Autoridade Fiscalizadora Principal e a equipa de avaliação devem exercer prudência e assegurar a proteção dos direitos dos clientes das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas que não são abrangidos pelo presente regulamento, nomeadamente em relação ao impacto nos níveis de serviço, na disponibilidade dos dados e na confidencialidade.

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 a Autoridade Fiscalizadora Principal considere adequados e tecnologicamente pertinentes,*** que seja utilizado ou contribua para a prestação dos serviços às entidades financeiras.

5. Antes de qualquer ***inspeção*** no local planeada, 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***, de outras AES*** 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, ***o órgão conjunto de fiscalização*** deve adotar as recomendações a 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 Fiscalizadoras Principais ***e o órgão conjunto de fiscalização*** 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 ***do órgão conjunto de fiscalização*** 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 ***pelo órgão conjunto de fiscalização*** nos termos do artigo 31.º, n.º ***1-A***, as entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas devem notificar ***ao órgão conjunto de fiscalização*** se pretendem ou não seguir essas recomendações. ***O órgão conjunto de fiscalização deve*** transmitir imediatamente essa informação às autoridades competentes ***das entidades financeiras em causa***.

2. As autoridades competentes devem ***informar as entidades financeiras que tenham celebrado contratos com entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas sobre os riscos identificados nas recomendações dirigidas a essas entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas pelo órgão conjunto de fiscalização em conformidade com o artigo 31.º, n.º 1, e*** verificar se as entidades financeiras têm em conta os riscos identificados ▌ . ***O órgão conjunto de fiscalização deve verificar se as entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas deram resposta aos riscos identificados nessas recomendações.***

3. ***Caso os objetivos regulamentares não possam ser assegurados através de outras medidas e as autoridades nacionais competentes tenham emitido avisos dirigidos às***

entidades financeiras afetadas com base em informações comunicadas pelo órgão conjunto de fiscalização, o conselho de administração da Autoridade Fiscalizadora Principal pode decidir, mediante recomendação do órgão conjunto de fiscalização e após consulta das autoridades competentes ***das*** entidades financeiras ***afetadas, suspender*** temporariamente, em parte ou na totalidade, a utilização ou o lançamento de um serviço prestado ***a entidades financeiras expostas aos*** riscos identificados nas recomendações dirigidas às entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas ***até que esses riscos*** sejam ***abordados***. Quando necessário ***e como medida de último recurso***, podem exigir que as ***entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas*** resolvam, em parte ou na totalidade, os contratos pertinentes celebrados com as ***entidades financeiras expostas aos riscos identificados***.

4. Quando ***toma*** as decisões referidas no n.º 3, ***o conselho de administração da Autoridade Fiscalizadora Principal deve*** 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;

   (d-A) **Se a suspensão ou cessação introduz um risco de continuidade para as operações comerciais do utilizador dos serviços da entidade terceira prestadora de serviços no domínio das TIC considerada crítica.**

4-A. As decisões previstas no n.º 3 só podem ser aplicadas depois de todas as entidades financeiras afetadas terem sido devidamente notificadas das mesmas. As entidades financeiras afetadas devem dispor de um período de tempo, que não deve exceder o estritamente necessário, para ajustar os acordos de subcontratação e acordos contratuais que tenham celebrado com entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas, de forma a não comprometer a resiliência operacional digital e a executar as estratégias de saída e planos de transição referidos no artigo 25.º.

As entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas sujeitas às decisões previstas no n.º 3 devem cooperar plenamente com as entidades financeiras afetadas.

5. As autoridades competentes devem informar regularmente ***o órgão conjunto de fiscalização*** das abordagens e medidas adotadas nas suas atribuições de supervisão em relação às entidades financeiras ▌.

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 ***decorrentes do cumprimento dos deveres previstos na presente secção*** e deve ser proporcional ao seu volume de negócios.

1-A. Se um mecanismo administrativo tiver sido celebrado com uma autoridade reguladora e de supervisão de um país terceiro nos termos do n.º 1 do presente artigo, essa autoridade pode fazer parte da equipa de avaliação a que se refere o artigo 35.º, n.º 1.

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 ***diligenciam no sentido de*** proceder ao intercâmbio entre si ***e com as entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas*** 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 ***e das entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas***, em especial através da sensibilização em relação às ciberameaças, limitando ou impedindo a capacidade de disseminação das ciberameaças, apoiando as capacidades defensivas, as técnicas de deteção de ameaças, as estratégias de atenuação ou as fases de resposta e recuperação;

   (b) Ocorra no seio de comunidades de confiança de entidades financeiras ***e de entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas***;

   (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[26] e as orientações sobre a política de concorrência[27].

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.

---

26 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).

27 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.

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;

(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 ***e oferentes*** de criptoativos, emitentes ***e oferentes*** 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 ***e dos operadores de sistemas de liquidação 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 ***(UE) 2016/1011***;

(r) No caso dos prestadores de serviços de financiamento colaborativo, a autoridade competente designada em conformidade com o artigo ***29.º*** do Regulamento ***(UE) 2020/1503***;

(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 ***são convidadas a participar*** nos trabalhos do Grupo de Cooperação***, na medida em que esses trabalhos digam respeito a atividades de supervisão e fiscalização, respetivamente, em relação às entidades enumeradas no anexo II, ponto 7, da Diretiva (UE) 2016/1148, que também tenham sido designadas como entidades terceiras prestadoras de serviços no domínio das TIC consideradas críticas nos termos do artigo 28.º do presente regulamento***.

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.

2-A. A Autoridade Fiscalizadora Principal informa as autoridades competentes designadas nos termos da Diretiva (UE) 2016/1148 e coopera com estas antes de proceder a investigações gerais e a inspeções no local em conformidade com os artigos 33.º e 34.º do presente regulamento.

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, ***o Conselho Único de Resolução, para informações sobre as entidades que se inserem no âmbito do Regulamento (UE) n.º 806/2014,*** e o 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 ***ciberameaça significativa*** 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, o BCE***, as autoridades nacionais de resolução e o Conselho Único de Resolução, para informações sobre as entidades que se inserem no âmbito do Regulamento (UE) n.º 806/2014,*** 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 ***considerada*** 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 ***doze meses*** 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, ***as sanções aplicadas e, excecionalmente,*** a identidade das

pessoas responsáveis ▌ .

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]. ***A Comissão elabora um relatório relativo à delegação de poderes pelo menos nove meses antes do final do prazo de cinco anos. A delegação de poderes é tacitamente prorrogada por períodos de igual duração, salvo se o Parlamento Europeu ou o Conselho a tal se opuserem pelo menos três meses antes do final de cada prazo.***

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 dos poderes nela especificados. A decisão de revogação produz efeitos a partir do dia seguinte ao da sua publicação no Jornal Oficial da União Europeia ou de uma data posterior nela 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, de 13 de abril de 2016, sobre legislar melhor.

5. Assim 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 ***três*** 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 ***três*** 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 ▌. ***O relatório deve analisar, pelo menos, os seguintes elementos:***

(a) ***A possibilidade de alargar o âmbito de aplicação do presente regulamento aos operadores de sistemas de pagamentos;***

(b) ***A natureza voluntária da comunicação de ciberameaças significativas;***

(c) Os 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; e

(d) ***A eficácia da tomada de decisões do órgão conjunto de fiscalização e o intercâmbio de informações entre o órgão conjunto de fiscalização e as autoridades nacionais competentes de países terceiros.***

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].»;

▌

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 ***24*** 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.

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
O Presidente

Pelo Conselho
O Presidente

PROCESSO DA COMISSÃO COMPETENTE QUANTO À MATÉRIA DE FUNDO

Título	Resiliência operacional digital do setor financeiro e alteração dos Regulamentos (CE) nº 1060/2009, (UE) nº 648/2012, (UE) nº 600/2014 e (UE) nº 909/2014
Referências	COM(2020)0595 – C9-0304/2020 – 2020/0266(COD)
Data de apresentação ao PE	24.9.2020
Comissão competente quanto ao fundo Data de comunicação em sessão	ECON 17.12.2020
Comissões encarregadas de emitir parecer Data de comunicação em sessão	ITRE IMCO 17.12.2020 17.12.2020
Comissões que não emitiram parecer Data da decisão	ITRE IMCO 15.10.2020 27.10.2020
Relatores Data de designação	Billy Kelleher 15.10.2020
Exame em comissão	14.4.2021 14.6.2021
Data de aprovação	1.12.2021
Resultado da votação final	+: 44 –: 5 0: 5
Deputados presentes no momento da votação final	Gerolf Annemans, Gunnar Beck, Marek Belka, Isabel Benjumea Benjumea, Stefan Berger, Gilles Boyer, Engin Eroglu, Markus Ferber, Jonás Fernández, Raffaele Fitto, Frances Fitzgerald, Luis Garicano, Sven Giegold, Valentino Grant, Claude Gruffat, José Gusmão, Enikő Győri, Eero Heinäluoma, Danuta Maria Hübner, Stasys Jakeliūnas, France Jamet, Billy Kelleher, Ondřej Kovařík, Georgios Kyrtsos, Aurore Lalucq, Philippe Lamberts, Aušra Maldeikienė, Pedro Marques, Costas Mavrides, Jörg Meuthen, Csaba Molnár, Siegfried Mureşan, Caroline Nagtegaal, Luděk Niedermayer, Lefteris Nikolaou-Alavanos, Lídia Pereira, Kira Marie Peter-Hansen, Sirpa Pietikäinen, Evelyn Regner, Antonio Maria Rinaldi, Alfred Sant, Martin Schirdewan, Joachim Schuster, Ralf Seekatz, Pedro Silva Pereira, Paul Tang, Irene Tinagli, Ernest Urtasun, Inese Vaidere, Johan Van Overtveldt, Stéphanie Yon-Courtin, Marco Zanni, Roberts Zīle
Suplentes presentes no momento da votação final	Lefteris Christoforou
Data de entrega	7.12.2021

VOTAÇÃO NOMINAL FINAL
NA COMISSÃO COMPETENTE QUANTO À MATÉRIA DE FUNDO

44	+
ECR	Raffaele Fitto, Johan Van Overtveldt, Roberts Zīle
NI	Enikő Győri
PPE	Isabel Benjumea Benjumea, Stefan Berger, Lefteris Christoforou, Markus Ferber, Frances Fitzgerald, Danuta Maria Hübner, Georgios Kyrtsos, Aušra Maldeikienė, Siegfried Mureşan, Luděk Niedermayer, Lídia Pereira, Sirpa Pietikäinen, Ralf Seekatz, Inese Vaidere
Renew	Gilles Boyer, Engin Eroglu, Luis Garicano, Billy Kelleher, Ondřej Kovařík, Caroline Nagtegaal, Stéphanie Yon-Courtin
S&D	Marek Belka, Jonás Fernández, Eero Heinäluoma, Aurore Lalucq, Pedro Marques, Costas Mavrides, Csaba Molnár, Evelyn Regner, Alfred Sant, Joachim Schuster, Pedro Silva Pereira, Paul Tang, Irene Tinagli
Verts/ALE	Sven Giegold, Claude Gruffat, Stasys Jakeliūnas, Philippe Lamberts, Kira Marie Peter-Hansen, Ernest Urtasun

5	-
ID	Gerolf Annemans, Gunnar Beck, France Jamet, Jörg Meuthen
NI	Lefteris Nikolaou-Alavanos

5	0
ID	Valentino Grant, Antonio Maria Rinaldi, Marco Zanni
The Left	José Gusmão, Martin Schirdewan

Legenda dos símbolos utilizados:
+ : votos a favor
- : votos contra
0 : abstenções