I

(Atos legislativos)

REGULAMENTOS

REGULAMENTO (UE) 2022/2554 DO PARLAMENTO EUROPEU E DO CONSELHO

de 14 de dezembro de 2022

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, (UE) n.º 909/2014 e (UE) 2016/1011

(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 ([1]),

Tendo em conta o parecer do Comité Económico e Social Europeu ([2]),

Deliberando de acordo com o processo legislativo ordinário ([3]),

Considerando o seguinte:

(1) Na era digital, as tecnologias da informação e comunicação (TIC) servem de esteio a sistemas complexos utilizados em atividades quotidianas. Mantêm em funcionamento setores fundamentais das nossas economias, nomeadamente o setor financeiro, e melhoram o funcionamento do mercado interno. A intensificação da digitalização e interligação também amplifica o risco associado às 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 utilização generalizada de sistemas de TIC e o elevado nível de digitalização e conectividade serem, atualmente, características centrais das atividades das entidades financeiras da União, a sua resiliência digital tem ainda de ser abordada e integrada de forma mais eficaz nos seus quadros operacionais mais vastos.

(2) A utilização das TIC tem adquirido nas últimas décadas um papel fulcral na prestação de serviços financeiros, de tal forma que se reveste hoje de importância crítica no funcionamento das habituais funções quotidianas de todas as entidades financeiras. Atualmente, a digitalização abrange, por exemplo, os pagamentos, onde se observa uma transição crescente dos métodos com base em numerário e em papel para soluções digitais, bem como a compensação e liquidação de valores mobiliários, a negociação eletrónica e algorítmica, as operações de concessão de empréstimos e de financiamento, o financiamento entre particulares, a notação de risco, a gestão dos sinistros e as operações de processamento administrativo. O setor dos seguros também sofreu transformações devido à

([1]) JO C 343 de 26.8.2021, p. 1.
([2]) JO C 155 de 30.4.2021, p. 38.
([3]) Posição do Parlamento Europeu de 10 de novembro de 2022 (ainda não publicada no Jornal Oficial) e decisão do Conselho de 28 de novembro de 2022.

utilização das TIC que vão desde a emergência de mediadores de seguros que oferecem os seus serviços em linha recorrendo a tecnosseguros, até à subscrição de seguros digitais. O setor financeiro tornou-se em grande medida digital e a digitalização também aprofundou a interligação e as dependências no interior do próprio setor financeiro e em relação a infraestruturas de terceiros e serviços prestados por terceiros.

(3) O Comité Europeu do Risco Sistémico (CERS) reafirmou, num relatório de 2020 sobre o ciber-risco sistémico, 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, poderiam constituir uma vulnerabilidade sistémica, porque os ciberincidentes localizados poderiam rapidamente propagar-se a partir de qualquer uma das aproximadamente 22 mil entidades financeiras da União a todo o sistema financeiro, sem qualquer entrave geográfico. As violações graves no domínio das TIC que ocorrem no setor financeiro não afetam unicamente as entidades financeiras, de forma isolada. Abrem também 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, nomeadamente, crises de liquidez e uma perda de confiança geral nos mercados financeiros.

(4) Mais recentemente, o risco associado às TIC mereceu a atenção de decisores políticos, autoridades de regulamentação e organismos de normalização internacionais, da União e nacionais, numa tentativa de reforçar a resiliência digital, 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, visam proporcionar às autoridades competentes e aos operadores de mercado em diversas jurisdições instrumentos para reforçar a resiliência dos seus sistemas financeiros. Estes trabalhos foram também impulsionados pela necessidade de ter devidamente em conta o risco associado às TIC no contexto de um sistema financeiro mundial altamente interligado, bem como de procurar assegurar uma maior coerência das boas práticas pertinentes.

(5) Não obstante as políticas e iniciativas legislativas específicas da União e nacionais, o risco associado às TIC continua a constituir um desafio para a resiliência operacional, o desempenho e a estabilidade do sistema financeiro da União. As reformas que se seguiram à crise financeira de 2008 reforçaram sobretudo a resiliência financeira do setor financeiro da União e visavam salvaguardar a competitividade e estabilidade da União do ponto de vista económico, prudencial e de conduta no mercado. Embora a segurança e a resiliência digital no domínio das TIC façam parte do risco operacional, têm merecido menor atenção na agenda regulamentar no período pós-crise financeira, tendo sido desenvolvidas apenas em alguns domínios das políticas e do panorama regulamentar da União no domínio dos serviços financeiros ou apenas em alguns Estados-Membros.

(6) Na sua comunicação de 8 de março de 2018 intitulada «Plano de Ação para a Tecnologia Financeira: rumo a um setor financeiro europeu mais competitivo e inovador», a Comissão destacou a extrema importância de tornar o setor financeiro da União mais resiliente, nomeadamente 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, uma prestação eficaz e harmoniosa de serviços financeiros em toda a União, inclusivamente em situações de tensão, preservando simultaneamente a confiança dos consumidores e do mercado.

(7) Em abril de 2019, a Autoridade Europeia de Supervisão (Autoridade Bancária Europeia), (EBA), criada pelo Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho ([4]), a Autoridade Europeia de Supervisão (Autoridade Europeia dos Seguros e Pensões Complementares de Reforma) (EIOPA), criada pelo Regulamento (UE) n.º 1094/2010 do Parlamento Europeu e do Conselho ([5]), e a Autoridade Europeia de Supervisão (Autoridade Europeia dos Valores Mobiliários e dos Mercados) (ESMA), criada pelo Regulamento (UE) n.º 1095/2010 do

([4]) Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Bancária Europeia), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/78/CE da Comissão (JO L 331 de 15.12.2010, p. 12).

([5]) Regulamento (UE) n.º 1094/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Europeia dos Seguros e Pensões Complementares de Reforma), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/79/CE da Comissão (JO L 331 de 15.12.2010, p. 48).

Parlamento Europeu e do Conselho ([6]) (conhecidas coletivamente como «Autoridades Europeias de Supervisão» ou «AES») emitiram conjuntamente pareceres técnicos que instavam a uma abordagem coerente do risco associado às 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 no mercado. Cumpre, pois, desenvolver o conjunto único de regras e o sistema de supervisão, com vista a abranger também a resiliência operacional digital, reforçando os mandatos das autoridades competentes para que possam supervisionar a gestão do risco associado às TIC no setor financeiro, a fim de proteger a integridade e a eficiência do mercado interno e facilitar o seu funcionamento ordenado.

(9) As disparidades legislativas e as assimetrias das abordagens nacionais de regulamentação ou supervisão no que diz respeito ao risco associado às TIC dão origem a obstáculos ao funcionamento do mercado interno dos serviços financeiros, impedindo o exercício harmonioso da liberdade de estabelecimento e a prestação de serviços pelas entidades financeiras que operam a nível transfronteiriço. A concorrência entre os mesmos tipos de entidades financeiras com atividade em diversos Estados-Membros também poderia sofrer distorções. É o caso, em particular, dos domínios em que a harmonização da União tem sido muito limitada, como o da realização de testes de resiliência operacional digital, ou inexistente, como o da monitorização do risco associado às TIC devido a terceiros. As disparidades decorrentes dos desenvolvimentos projetados a nível nacional podem gerar mais obstáculos ao funcionamento do mercado interno, em detrimento dos intervenientes no mercado e da estabilidade financeira.

(10) Até à data, pelo facto de as disposições relacionadas com o risco associado às TIC apenas serem abordadas de modo parcial a nível da União, são patentes lacunas e sobreposições em domínios importantes, como a notificação de incidentes relacionados com as TIC e a realização de testes de resiliência operacional digital, bem como inconsistências decorrentes da emergência de regras nacionais divergentes ou da aplicação ineficaz em termos de custos de regras que se sobrepõem. 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. Atuando isoladamente as entidades financeiras com atividades transfronteiriças ou titulares de diversas autorizações (por exemplo, uma entidade financeira pode ser titular de uma licença bancária, como empresa de investimento e como instituição de pagamento, cada uma delas emitida por autoridades competentes diferentes num ou mais Estados-Membros) enfrentam desafios operacionais para fazer face ao risco associado às TIC e atenuar os impactos negativos dos incidentes relacionados com as TIC de uma forma eficaz em termos de custos

(11) Uma vez que o conjunto único de regras não foi acompanhado de um quadro abrangente para o risco operacional nem para as TIC, é necessária uma maior harmonização dos requisitos essenciais de resiliência operacional digital para todas as entidades financeiras. O desenvolvimento de capacidades e de resiliência geral no domínio das TIC pelas entidades financeiras, com base nos referidos requisitos essenciais, com vista a resistir às indisponibilidades operacionais, ajudaria 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 interno, deverá ter por base as disposições do artigo 114.º do Tratado sobre o Funcionamento da União Europeia (TFUE), interpretado nos termos da jurisprudência constante do Tribunal de Justiça da União Europeia (Tribunal de Justiça).

(12) O presente regulamento visa consolidar e atualizar os requisitos em matéria de risco associado às TIC no âmbito dos requisitos em matéria de risco operacional que, até ao momento, foram abordados separadamente em vários atos jurídicos da União. Apesar de os referidos atos abrangerem as principais categorias de riscos financeiros (ou seja, risco de crédito, risco de mercado, risco de crédito de contraparte, risco de liquidez e risco de conduta no mercado), quando foram adotados não deram uma resposta cabal a todas as componentes da resiliência operacional. As regras em matéria de risco operacional, à medida que foram sendo aprofundadas 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 o risco associado às TIC), em detrimento de regras qualitativas

([6]) Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho, de 24 de novembro de 2010, que cria uma Autoridade Europeia de Supervisão (Autoridade Europeia dos Valores Mobiliários e dos Mercados), altera a Decisão n.º 716/2009/CE e revoga a Decisão 2009/77/CE da Comissão (JO L 331 de 15.12.2010, p. 84).

específicas destinadas a proteger, detetar, conter, recuperar e reparar as capacidades afetadas por incidentes relacionados com as TIC, ou a estabelecer capacidades em matéria de notificação e de testes digitais. Esses atos pretendiam, sobretudo, abranger e atualizar as regras essenciais em matéria de supervisão prudencial, integridade do mercado ou conduta. Ao consolidar e atualizar as diferentes regras em matéria de risco associado às TIC, todas as disposições que abordam o risco digital no setor financeiro deverão ser, pela primeira vez, coligidas de modo coerente num único ato legislativo. Por conseguinte, o presente regulamento colmata as lacunas ou resolve as incoerências em alguns dos anteriores atos jurídicos, nomeadamente em relação à terminologia utilizada, e faz explicitamente referência ao risco associado às TIC por meio de regras específicas relativas às capacidades de gestão desse risco, à notificação de incidentes, aos testes de resiliência operacional, bem como à monitorização do risco associado às TIC devido a terceiros. O presente regulamento deverá, portanto, sensibilizar para o risco associado às TIC e reconhecer que os incidentes relacionados com as TIC e a falta de resiliência operacional podem comprometer a solidez das entidades financeiras.

(13) As entidades financeiras deverão adotar a mesma abordagem e as mesmas regras baseadas em princípios ao abordarem o risco associado às TIC, tendo em conta a sua dimensão e o seu perfil de risco global, bem como a natureza, a escala e a complexidade dos seus serviços, atividades e operações. A coerência contribuirá para reforçar a confiança no sistema financeiro e preservar a sua estabilidade, especialmente quando se verifica uma dependência elevada dos sistemas, plataformas e infraestruturas de TIC, o que implica um aumento do risco digital. A observância de regras básicas de cibersegurança deverá também evitar a imposição de pesados custos para a economia, minimizando o impacto e os custos das perturbações no domínio das TIC.

(14) Um regulamento ajuda a reduzir a complexidade regulamentar, fomenta a convergência da supervisão, aumenta a segurança jurídica e contribui também para limitar os custos de conformidade, em especial para entidades financeiras com atividade a nível transfronteiras, bem como 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 é a forma mais adequada de garantir uma aplicação homogénea e coerente de todas as componentes da gestão do risco associado às TIC pelo setor financeiro da União.

(15) A Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho ([7]) foi o primeiro quadro horizontal para a cibersegurança adotado a nível da União, sendo aplicável também 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 estabeleceu um mecanismo de identificação a nível nacional dos operadores de serviços essenciais, só determinadas instituições de crédito, plataformas de negociação e contrapartes centrais foram identificadas pelos Estados-Membros e passaram a ser abrangidas pelo seu âmbito de aplicação, na prática, sendo, por conseguinte, obrigadas a cumprir os requisitos de notificação de incidentes e de segurança no domínio das TIC estabelecidos na diretiva. A Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho ([8]) estabelece um critério uniforme para determinar as entidades abrangidas pelo seu âmbito de aplicação (regra do limite máximo de dimensão), mantendo simultaneamente os três tipos de entidades financeiras no seu âmbito de aplicação.

(16) No entanto, dado que o presente regulamento aumenta o nível de harmonização das diferentes componentes de resiliência digital, introduzindo requisitos de gestão do risco associado às TIC e de comunicação de incidentes relacionados com as TIC que são mais rigorosos em comparação com os estabelecidos no direito da União vigente em matéria de serviços financeiros da União, este nível mais elevado constitui também um reforço da harmonização em comparação com os requisitos estabelecidos na Diretiva (UE) 2022/2555 Por conseguinte, o presente regulamento constitui *lex specialis* relativamente à Diretiva (UE) 2022/2555 Ao mesmo tempo, é fundamental manter uma ligação forte entre o setor financeiro e o quadro horizontal de cibersegurança da União, tal como consta atualmente da Diretiva (UE) 2022/2555, a fim de assegurar a coerência com as estratégias de cibersegurança adotadas pelos Estados-Membros e de permitir que as autoridades de supervisão financeira tomem conhecimento dos ciberincidentes que afetem outros setores abrangidos por essa diretiva.

([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).

([8]) Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União, que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972, e que revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (ver página 80 do presente Jornal Oficial).

(17) Nos termos do artigo 4.º, n.º 2, do Tratado da União Europeia e sem prejuízo do controlo jurisdicional pelo Tribunal de Justiça, o presente regulamento não deverá afetar a responsabilidade dos Estados-Membros no que respeita às funções essenciais do Estado em matéria de segurança pública, defesa e salvaguarda da segurança nacional, por exemplo no que diz respeito ao fornecimento de informações que sejam contrárias à salvaguarda da segurança nacional.

(18) A fim de possibilitar a aprendizagem intersetorial e retirar efetivamente ensinamentos de outros setores que enfrentam ciberameaças, as entidades financeiras referidas na Diretiva (UE) 2022/2555 deverão continuar a fazer parte do «ecossistema» dessa diretiva [por exemplo, o grupo de cooperação e as equipas de resposta a incidentes de segurança informática (CSIRT)]. As AES e as autoridades nacionais competentes deverão participar nos debates políticos estratégicos e nos trabalhos técnicos do grupo de cooperação ao abrigo dessa diretiva, e trocar informações e reforçar a cooperação com os pontos de contacto únicos designados ou criados nos termos dessa diretiva. As autoridades competentes ao abrigo do presente regulamento deverão igualmente consultar e cooperar com as CSIRT. As autoridades competentes deverão também poder solicitar aconselhamento técnico às autoridades competentes designadas ou criadas nos termos da Diretiva (UE) 2022/2555 e celebrar acordos de cooperação destinados a assegurar mecanismos de coordenação eficazes e de resposta rápida.

(19) Tendo em conta as fortes interligações entre a resiliência digital e a resiliência física das entidades financeiras, é necessário assegurar uma abordagem coerente da resiliência das entidades críticas no presente regulamento e na Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho ([9]). Uma vez que a resiliência física das entidades financeiras é abordada de forma abrangente no quadro das obrigações em matéria de gestão do risco associado às TIC e de notificação abrangidas pelo presente regulamento, as obrigações previstas nos capítulos III e IV da Diretiva (UE) 2022/2557 não deverão aplicar-se às entidades financeiras abrangidas pelo âmbito de aplicação dessa diretiva.

(20) Os prestadores de serviços de computação em nuvem são uma das categorias de infraestruturas digitais abrangidas pela Diretiva (UE) 2022/2555 O quadro de superintendência da União («quadro de superintendência») estabelecido pelo presente regulamento aplica-se a todos os terceiros prestadores de serviços de TIC críticos, incluindo os prestadores de serviços de computação em nuvem que prestam serviços de TIC a entidades financeiras, e deverá ser considerado complementar da supervisão nos termos da Diretiva (UE) 2022/2555 Além disso, o quadro de superintendência estabelecido no presente regulamento deverá abranger os prestadores de serviços de computação em nuvem na ausência de um quadro horizontal da União que estabeleça uma autoridade de supervisão digital.

(21) Para que mantenham pleno controlo do risco associado às TIC, as entidades financeiras deverão dispor de capacidades abrangentes que possibilitem uma gestão robusta e eficaz do risco associado às TIC, bem como de mecanismos e políticas específicas para o tratamento de todos os incidentes relacionados com as TIC e para a notificação dos incidentes de caráter severo relacionados com as TIC. Do mesmo modo, as entidades financeiras deverão dispor de políticas para a realização de testes dos sistemas, controlos e processos de TIC, bem como para gerir o risco associado às TIC devido a terceiros. A base de referência para a resiliência operacional digital das entidades financeiras deverá ser elevada, permitindo simultaneamente uma aplicação proporcionada dos requisitos aplicáveis a certas entidades financeiras, nomeadamente as microempresas, bem como as entidades financeiras sujeitas a um quadro simplificado de gestão do risco associado às TIC. A fim de facilitar uma supervisão eficiente das instituições de realização de planos de pensões profissionais que seja proporcionada e dê resposta à necessidade de reduzir os encargos administrativos para as autoridades competentes, os mecanismos nacionais de supervisão pertinentes aplicáveis a essas entidades financeiras deverão ter em conta a sua dimensão e o seu perfil de risco global, bem como a natureza, a escala e a complexidade dos seus serviços, atividades e operações, mesmo quando os limiares pertinentes estabelecidos no artigo 5.º da Diretiva (UE) 2016/2341 do Parlamento Europeu e do Conselho ([10]) sejam excedidos. Em especial, as atividades de supervisão deverão centrar-se principalmente na necessidade de fazer face a riscos graves relacionados com a gestão do risco associado às TIC por parte de determinada entidade.

([9]) Diretiva (UE) 2022/2557 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa à resiliência das entidades críticas e que revoga a Diretiva 2008/114/CE do Conselho (ver página 164 do presente Jornal Oficial).

([10]) Diretiva (UE) 2016/2341 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2016, relativa às atividades e à supervisão das instituições de realização de planos de pensões profissionais (IRPPP) (JO L 354 de 23.12.2016, p. 37).

As autoridades competentes deverão igualmente manter uma abordagem vigilante mas proporcionada em relação à supervisão das instituições de realização de planos de pensões profissionais que, nos termos do artigo 31.º da Diretiva (UE) 2016/2341, subcontratam a prestadores de serviços uma parte significativa da sua atividade principal, como a gestão de ativos, os cálculos atuariais, a contabilidade e a gestão de dados.

(22) Os limiares e as taxonomias que regem a notificação de incidentes relacionados com as TIC variam significativamente a nível nacional. Embora seja possível chegar a consensos, por meio dos esforços pertinentes envidados pela Agência da União Europeia para a Cibersegurança (ENISA), criada pelo Regulamento (UE) 2019/881 do Parlamento Europeu e do Conselho ([11]) e pelo grupo de cooperação ao abrigo da Diretiva (UE) 2022/2555, ainda existem e podem surgir abordagens divergentes em matéria de fixação de limiares e utilização de taxonomias para as restantes entidades financeiras. Devido a essas divergências, há múltiplos requisitos que as entidades financeiras têm de cumprir, em especial se tiverem atividades em diversos Estados-Membros e integrarem um grupo financeiro. Além disso, tais divergências têm potencial para prejudicar a criação de outros mecanismos uniformes ou centralizados da União que acelerem o processo de notificação e apoiem uma partilha rápida e facilitada de informações entre as autoridades competentes, que é crucial para dar resposta ao risco associado às TIC em caso de ataques em grande escala com consequências potencialmente sistémicas.

(23) A fim de reduzir os encargos administrativos e a potencial duplicação das obrigações de notificação para certas entidades financeiras, o requisito relativo à notificação de incidentes nos termos da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho ([12]) deverá deixar de ser aplicável aos prestadores de serviços de pagamento abrangidos pelo âmbito de aplicação do presente regulamento. Por conseguinte, as instituições de crédito, as instituições de moeda eletrónica, as instituições de pagamento e os prestadores de serviços de informação sobre contas a que se refere o artigo 33.º, n.º 1, dessa diretiva deverão, a partir da data de aplicação do presente regulamento, notificar, nos termos do presente regulamento, todos os incidentes operacionais ou de segurança relacionados com pagamentos que tenham sido previamente notificados nos termos da referida diretiva, independentemente de tais incidentes estarem relacionados com as TIC.

(24) Para permitir que as autoridades competentes cumpram as 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, o presente regulamento deverá estabelecer um regime sólido de notificação dos incidentes relacionados com as TIC, ao abrigo do qual os requisitos pertinentes abordem as atuais lacunas no direito dos serviços financeiros, e eliminem sobreposições e duplicações existentes para reduzir os custos. É essencial harmonizar o regime de notificação 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, conforme estabelecido no presente regulamento. Além disso, as AES deverão estar habilitadas a especificar elementos pertinentes para o quadro de notificação de incidentes relacionados com as TIC, tais como a taxonomia, os prazos, os conjuntos de dados, os modelos e os limiares aplicáveis. A fim de assegurar a plena coerência com a Diretiva (UE) 2022/2555, as entidades financeiras deverão estar autorizadas a notificar, a título voluntário, a autoridade competente pertinente da existência de ciberameaças significativas sempre que considerem as ameaças relevantes para o sistema financeiro, os utilizadores ou os clientes do serviço.

(25) Foram desenvolvidos requisitos em matéria de testes de resiliência operacional digital em certos subsetores financeiros que estabelecem quadros que nem sempre estão totalmente alinhados. Esta situação conduz a uma potencial duplicação dos custos para as entidades financeiras transfronteiriças e torna complexo o reconhecimento mútuo dos resultados dos testes de resiliência operacional digital, o que, por sua vez, pode fragmentar o mercado interno.

([11]) 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).

([12]) Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno, que altera as Diretivas 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE (JO L 337 de 23.12.2015, p. 35).

(26) Além disso, nos casos em que não é obrigatório realizar testes às TIC, existem vulnerabilidades que continuam ocultas e que conduzem à exposição de uma entidade financeira ao risco associado às TIC e, em última análise, aumentam o risco para a estabilidade e a integridade do setor financeiro. Sem a intervenção da União, a realização de testes de resiliência operacional digital continuaria a ser incoerente e careceria de um sistema de reconhecimento mútuo dos resultados dos testes às TIC entre as diversas jurisdições. Além disso, e uma vez que será pouco provável que outros subsetores financeiros adotem regimes de realização de testes a uma escala significativa, não terão acesso aos potenciais benefícios de um quadro para a realização de testes, em termos de identificação de vulnerabilidades e risco associado às TIC, e avaliação das capacidades de defesa e de garantia de continuidade das atividades, que contribuem para aumentar a confiança dos clientes, fornecedores e parceiros comerciais. A fim de resolver essas sobreposições, divergências e lacunas, é necessário estabelecer regras relativas a um regime de realização de testes coordenados, facilitando assim o reconhecimento mútuo de testes avançados para as entidades financeiras que preencham os requisitos previstos no presente regulamento.

(27) A dependência das entidades financeiras da utilização 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 satisfazer a procura dos consumidores. A natureza e a dimensão desta dependência têm evoluído continuamente nos últimos anos e impulsionou uma redução dos custos de intermediação financeira, permitindo a expansão das empresas e economias de escala no desenvolvimento de atividades financeiras e oferecendo simultaneamente uma gama alargada de instrumentos de TIC para gerir processos internos complexos.

(28) 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, mesmo quando estes últimos estão consagrados nos seus acordos contratuais. Acresce que muitos desses acordos contratuais não preveem salvaguardas suficientes para a plena monitorização dos processos de subcontratação, privando assim a entidade financeira dos instrumentos necessários para avaliar os riscos associados. Além disso, uma vez que os terceiros prestadores de serviços de TIC prestam muitas vezes serviços normalizados a diferentes tipos de clientes, tais acordos contratuais nem sempre dão uma resposta cabal às necessidades individuais ou específicas dos intervenientes do setor financeiro.

(29) Embora o direito da União dos serviços financeiros contenha certas regras gerais em matéria de externalização, a monitorização da dimensão contratual não está plenamente ancorada no direito 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 associado às 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 associado às TIC devido a terceiros, princípios esses que assumem particular importância quando as entidades financeiras recorrem a terceiros prestadores de serviços de TIC para apoiar as suas funções críticas ou importantes. Esses princípios deverão ser acompanhados de um conjunto de direitos contratuais fundamentais relativos a diversos elementos da execução e rescisão de acordos contratuais, com vista a proporcionar determinadas salvaguardas mínimas a fim de reforçar a capacidade das entidades financeiras procederem a uma monitorização efetiva de todo o risco associado às TIC que possa surgir a nível dos terceiros prestadores de serviços. Esses princípios são complementares do direito setorial aplicável à externalização.

(30) Verifica-se atualmente uma certa falta de homogeneidade e convergência no que se refere à monitorização do risco associado às TIC devido a terceiros e à dependência de terceiros no domínio das TIC. Não obstante os esforços no sentido de enquadrar a externalização, tais como as Orientações da EBA relativas à subcontratação, de 2019, e as Orientações da ESMA relativas à subcontratação externa a prestadores de serviços de computação em nuvem, de 2021, a questão mais vasta do combate ao risco sistémico que pode ser desencadeado pela exposição do setor financeiro a um conjunto limitado de terceiros prestadores de serviços de TIC críticos não é suficientemente abordada no direito da União. A insuficiência de regras a nível da União é agravada pela ausência de regras a nível nacional sobre instrumentos e mandatos que permitam às autoridades de supervisão financeira obter um bom conhecimento das dependências de terceiros no domínio das TIC e monitorizar de forma adequada os riscos decorrentes da concentração de dependências de terceiros no domínio das TIC.

(31) Tendo em conta o potencial risco sistémico que o aumento das práticas de externalização e a concentração ao nível das TIC implicam, e estando ciente de que os mecanismos nacionais são insuficientes para dotar as autoridades de supervisão financeira de instrumentos adequados para quantificar, qualificar e remediar as consequências do risco associado às TIC devido a terceiros prestadores de serviços de TIC críticos, há que estabelecer um quadro de superintendência adequado que permita a contínua monitorização das atividades de terceiros prestadores de serviços de TIC que sejam críticos para as entidades financeiras, assegurando simultaneamente a confidencialidade e a segurança dos clientes que não sejam entidades financeiras. Embora a prestação de serviços de TIC intragrupo implique riscos e benefícios específicos, não deverá ser automaticamente considerada menos arriscada do que a prestação de serviços de TIC por prestadores de serviços que não pertençam a um grupo financeiro, devendo, por conseguinte, estar sujeita ao mesmo quadro regulamentar. No entanto, quando os serviços de TIC são prestados no âmbito do mesmo grupo financeiro, as entidades financeiras podem ter um nível mais elevado de controlo sobre os prestadores intragrupo, o que deverá ser tido em conta na avaliação global dos riscos.

(32) Dado que o risco associado às TIC é cada vez mais complexo e sofisticado, a adequação das medidas de deteção e prevenção do risco associado às TIC dependerá, em grande medida, da partilha regular de informações entre as entidades financeiras sobre as ameaças e vulnerabilidades. A partilha de informações contribui para aumentar a sensibilização para as ciberameaças. Por sua vez, tal reforça a capacidade das entidades financeiras para impedirem que as ciberameaças se transformem em incidentes reais relacionados com as TIC e permite que as entidades financeiras contenham de forma mais eficaz o impacto dos incidentes relacionados com as TIC e recuperem dos mesmos mais rapidamente. Na ausência de orientações a nível da União, diversos fatores, em especial a incerteza quanto à sua compatibilidade com as regras em matéria de proteção de dados, anti-trust e de responsabilidade, parecem ter inibido a referida partilha de informações.

(33) Além disso, as dúvidas quanto ao 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) levaram a que informações úteis não fossem partilhadas. Por conseguinte, a dimensão e a qualidade da partilha de informações continuam a ser limitadas e fragmentadas, sendo os intercâmbios pertinentes realizados sobretudo 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 sistema financeiro integrado. Por conseguinte, é importante reforçar esses canais de comunicação.

(34) Importa incentivar as entidades financeiras a partilharem entre si informações específicas e sensíveis relativas a ciberameaças e 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, participando em acordos de partilha de informações. Por conseguinte, é necessário possibilitar o surgimento a nível da União de mecanismos que prevejam acordos de partilha de informações a título voluntário, que, quando realizada em ambientes fiáveis, ajudaria o setor financeiro a prevenir e dar resposta coletivamente às ciberameaças, limitando rapidamente a propagação do risco associado às TIC e impedindo o possível contágio ao longo dos canais financeiros. Esses mecanismos deverão respeitar as regras aplicáveis em matéria de direito da concorrência da União previstas na Comunicação da Comissão, de 14 de janeiro de 2011, intitulada «Orientações sobre a aplicação do artigo 101.º do Tratado sobre o Funcionamento da União Europeia aos acordos de cooperação horizontal», bem como as regras da União em matéria de proteção dos dados, nomeadamente o Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([13]). Deverão funcionar com base em uma ou várias das bases jurídicas estabelecidas no artigo 6.º desse regulamento, 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, bem como no contexto do tratamento de dados pessoais necessário para o cumprimento de uma obrigação jurídica à qual o responsável pelo tratamento de dados está sujeito ou para o exercício de funções de interesse público ou da autoridade pública de que está investido o responsável pelo tratamento dos dados, conforme referido no artigo 6.º, n.º 1, alíneas c) e e), respetivamente, desse regulamento.

([13]) 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).

(35) A fim de manter um elevado nível de resiliência operacional digital para todo o setor financeiro e, ao mesmo tempo, acompanhar a evolução tecnológica, o presente regulamento deverá abordar os riscos decorrentes de todos os tipos de serviços de TIC. Para o efeito, a definição de serviços de TIC no contexto do presente regulamento deverá ser entendida de forma ampla e abranger os serviços digitais e de dados prestados por meio de sistemas de TIC a um ou mais utilizadores internos ou externos de forma contínua. Essa definição deverá incluir, por exemplo, os chamados «serviços over the top» (de distribuição de conteúdos audiovisuais), que se inserem na categoria dos serviços de comunicações eletrónicas. Deverá excluir apenas a categoria limitada de serviços telefónicos analógicos tradicionais considerados serviços da rede telefónica pública comutada (RTPC), serviços da rede fixa, serviços telefónicos convencionais (POTS, do inglês *Plain Old Telephone Service*) ou serviços de comunicações por telefone fixo.

(36) Não obstante a ampla cobertura pretendida com o presente regulamento, a aplicação das regras de resiliência operacional digital deverá ter em conta as diferenças significativas entre as entidades financeiras em termos da sua dimensão e do seu perfil de risco global. Como princípio geral, ao afetarem recursos e capacidades à aplicação do quadro de gestão do risco associado às TIC, as entidades financeiras deverão equacionar cuidadosamente as suas necessidades relacionadas com as TIC em função da sua dimensão e do seu perfil de risco global, bem como da natureza, escala e complexidade dos seus serviços, atividades e operações, enquanto as autoridades competentes deverão avaliar e rever de forma recorrente a abordagem seguida para tal afetação.

(37) Os prestadores de serviços de informação sobre contas, referidos no artigo 33.º, n.º 1, da Diretiva (UE) 2015/2366, estão explicitamente incluídos no âmbito de aplicação do presente regulamento, tendo em conta a natureza específica das suas atividades e os riscos daí decorrentes. Além disso, as instituições de moeda eletrónica e as instituições de pagamento, isentas nos termos do artigo 9.º, n.º 1, da Diretiva 2009/110/CE do Parlamento Europeu e do Conselho ([14]) e do artigo 32.º, n.º 1, da Diretiva (UE) 2015/2366, estão incluídas no âmbito de aplicação do presente regulamento, mesmo que não lhes tenha sido concedida autorização, nos termos da Diretiva 2009/110/CE, para emitir moeda eletrónica, ou que não lhes tenha sido concedida autorização, nos termos da Diretiva (UE) 2015/2366, para prestar e executar serviços de pagamento. No entanto, as instituições de cheques postais referidas no artigo 2.º, n.º 5, ponto 3, da Diretiva 2013/36/UE do Parlamento Europeu e do Conselho ([15]) estão excluídas do âmbito de aplicação do presente regulamento. A autoridade competente para as instituições de pagamento isentas nos termos da Diretiva (UE) 2015/2366, as instituições de moeda eletrónica isentas nos termos da Diretiva 2009/110/CE e os prestadores de serviços de informação sobre contas referidos no artigo 33.º, n.º 1, da Diretiva (UE) 2015/2366, deverá ser a autoridade competente designada nos termos do artigo 22.º da Diretiva (UE) 2015/2366.

(38) Uma vez que as entidades financeiras de maior dimensão dispõem de mais recursos e conseguem 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. Essas entidades estão mais bem equipadas, nomeadamente para criarem funções específicas de gestão destinadas a supervisionar os acordos celebrados com terceiros prestadores de serviços de TIC ou gerir as crises, para organizarem a sua gestão do risco associado às TIC de acordo com o modelo das três linhas de defesa, ou para criarem um modelo interno de controlo e gestão dos riscos e submeterem o seu quadro de gestão do risco associado às TIC a auditorias internas.

(39) Algumas entidades financeiras beneficiam de isenções ou estão sujeitas a um quadro regulamentar muito leve ao abrigo do direito setorial da União pertinente. Entre essas entidades financeiras contam-se os gestores de fundos de investimento alternativos a que se refere o artigo 3.º, n.º 2, da Diretiva 2011/61/UE do Parlamento Europeu e do Conselho ([16]), as empresas de seguros e de resseguros a que se refere o artigo 4.º da Diretiva 2009/138/CE do Parlamento Europeu e do Conselho ([17]), e as instituições de realização de planos de pensões profissionais que gerem

([14]) 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).

([15]) Diretiva 2013/36/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa ao acesso à atividade das instituições de crédito e à supervisão prudencial das instituições de crédito, que altera a Diretiva 2002/87/CE e revoga as Diretivas 2006/48/CE e 2006/49/CE (JO L 176 de 27.6.2013, p. 338).

([16]) Diretiva 2011/61/UE do Parlamento Europeu e do Conselho, de 8 de junho de 2011, relativa aos gestores de fundos de investimento alternativos e que altera as Diretivas 2003/41/CE e 2009/65/CE e os Regulamentos (CE) n.º 1060/2009 e (UE) n.º 1095/2010 (JO L 174 de 1.7.2011, p. 1).

([17]) Diretiva 2009/138/CE do Parlamento Europeu e do Conselho, de 25 de novembro de 2009, relativa ao acesso à atividade de seguros e resseguros e ao seu exercício (Solvência II) (JO L 335 de 17.12.2009, p. 1).

planos de pensões que, no seu conjunto, não têm mais de 15 membros no total. À luz das referidas isenções, não seria proporcionado incluir estas entidades financeiras no âmbito de aplicação do presente regulamento. Além disso, o presente regulamento reconhece as especificidades da estrutura do mercado de mediação de seguros, pelo que os mediadores de seguros, os mediadores de resseguros e os mediadores de seguros a título acessório considerados microempresas ou pequenas ou médias empresas não deverão ser abrangidos pelo presente regulamento.

(40) Uma vez que as entidades a que se refere o artigo 2.º, n.º 5, pontos 4 a 23, da Diretiva 2013/36/UE estão excluídas do âmbito de aplicação dessa diretiva, os Estados-Membros deverão, por conseguinte, poder optar por excluir da aplicação do presente regulamento essas entidades que se situem nos respetivos territórios.

(41) Do mesmo modo, a fim de alinhar o presente regulamento com o âmbito de aplicação da Diretiva 2014/65/UE do Parlamento Europeu e do Conselho ([18]), é igualmente oportuno excluir do âmbito de aplicação do presente regulamento as pessoas singulares e coletivas a que se referem os artigos 2.º e 3.º dessa diretiva e que estão autorizadas a prestar serviços de investimento sem terem de obter autorização ao abrigo da Diretiva 2014/65/UE. No entanto, o artigo 2.º da Diretiva 2014/65/UE também exclui do âmbito de aplicação dessa diretiva as entidades consideradas entidades financeiras para efeitos do presente regulamento, como as centrais de valores mobiliários, os organismos de investimento coletivo ou as empresas de seguros e de resseguros. A exclusão do âmbito de aplicação do presente regulamento das pessoas e entidades a que se referem os artigos 2.º e 3.º da referida diretiva não deverá abranger essas centrais de depósito de valores mobiliários, organismos de investimento coletivo ou empresas de seguros e de resseguros.

(42) Ao abrigo do direito setorial da União, algumas entidades financeiras estão sujeitas a requisitos ou isenções mais leves devido à sua dimensão ou aos serviços que prestam. Essa categoria de entidades financeiras inclui empresas de investimento de pequena dimensão e não interligadas, pequenas instituições de realização de planos de pensões profissionais, que podem ser excluídas do âmbito de aplicação da Diretiva (UE) 2016/2341 pelo Estado-Membro em causa, nas condições estabelecidas no artigo 5.º dessa diretiva, e que gerem planos de pensões que, no seu conjunto, não têm mais de 100 membros no total, bem como as instituições isentas nos termos da Diretiva 2013/36/UE. Por conseguinte, em consonância com o princípio da proporcionalidade e a fim de preservar o espírito do direito setorial da União, é igualmente adequado que, ao abrigo do presente regulamento, essas entidades financeiras sejam abrangidas por um quadro simplificado de gestão do risco associado às TIC. O caráter proporcionado do quadro de gestão do risco associado às TIC que abrange essas entidades financeiras não deverá ser alterado pelas normas técnicas de regulamentação que devem ser desenvolvidas pelas AES. Além disso, de acordo com o princípio da proporcionalidade, é adequado que as instituições de pagamento a que se refere o artigo 32.º, n.º 1, da Diretiva (UE) 2015/2366 e as instituições de moeda eletrónica a que se refere o artigo 9.º da Diretiva 2009/110/CE, isentas nos termos do direito nacional que transpõe esses atos jurídicos da União, também sejam abrangidas por um quadro simplificado de gestão do risco associado às TIC ao abrigo do presente regulamento, ao passo que as instituições de pagamento e as instituições de moeda eletrónica que não estejam isentas nos termos do respetivo direito nacional que transpõe o direito setorial da União deverão cumprir o quadro geral estabelecido no presente regulamento.

(43) Do mesmo modo, as entidades financeiras consideradas microempresas ou abrangidas pelo quadro simplificado de gestão do risco associado às TIC ao abrigo do presente regulamento não deverão ser obrigadas a criar um cargo para monitorizar os acordos celebrados com terceiros prestadores de serviços de TIC relativos à utilização de serviços de TIC; nem a designar um membro da direção de topo responsável pela superintendência da exposição ao risco conexa e pela documentação pertinente; a atribuir a responsabilidade pela gestão e superintendência do risco associado às TIC a uma função de controlo e assegurar um nível adequado de independência e objetividade dessa função de controlo, a fim de evitar conflitos de interesses; a documentar e rever, pelo menos uma vez por ano, o quadro de gestão do risco associado às TIC; a submeter periodicamente a auditoria interna o quadro de gestão do risco associado às TIC; a realizar avaliações em profundidade após a introdução de alterações importantes nas suas infraestruturas e processos do sistema de rede e informação; a realizar análises do risco periódicas de sistemas de TIC legados; a submeter a execução dos planos de resposta e recuperação em matéria de TIC a auditorias internas independentes; a dispor de uma função de gestão de crises, 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; a comunicar às autoridades competentes, a pedido destas,

([18]) Diretiva 2014/65/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativa aos mercados de instrumentos financeiros e que altera a Diretiva 2002/92/CE e a Diretiva 2011/61/UE (JO L 173 de 12.6.2014, p. 349).

uma estimativa dos custos e perdas anuais agregados causados por incidentes de caráter severo relacionados com as TIC; a manter capacidades de TIC redundantes, a comunicar às autoridades nacionais competentes as alterações introduzidas na sequência de avaliações de incidentes relacionados com as TIC; a monitorizar continuamente a evolução tecnológica pertinente, a estabelecer um programa abrangente de realização de testes de resiliência operacional digital para efeitos do quadro de gestão do risco associado às TIC previsto no presente regulamento, ou a adotar e rever periodicamente uma estratégia para o risco associado às TIC devido a terceiros. Além disso, as microempresas deverão ser obrigadas a avaliar a necessidade de manter essas capacidades de TIC redundantes apenas com base no seu perfil de risco. As microempresas deverão beneficiar de um regime mais flexível no que diz respeito aos programas de realização de testes de resiliência operacional digital. Ao considerar o tipo e a frequência dos testes, deverão equacionar, de forma adequada, o objetivo de manter uma elevada resiliência operacional digital com os recursos disponíveis e com o seu perfil de risco global. As microempresas e as entidades financeiras abrangidas pelo quadro simplificado de gestão do risco associado às TIC ao abrigo do presente regulamento deverão estar isentas da obrigação de realizar testes avançados às ferramentas, aos sistemas e aos processos relacionados com as TIC mediante testes de penetração baseados em ameaças (TLPT, do inglês *threat-led penetration testing*), uma vez que apenas as entidades financeiras que preencham os critérios previstos no presente regulamento deverão ser obrigadas a realizar esses testes. Atendendo às suas capacidades limitadas, as microempresas deverão poder acordar com os terceiros prestadores de serviços de TIC críticos a delegação dos direitos de acesso, inspeção e auditoria da entidade financeira a uma entidade terceira independente, a nomear pelo terceiro prestador de serviços de TIC, desde que a entidade financeira possa solicitar, a qualquer momento, todas as informações e garantias pertinentes sobre o desempenho do terceiro prestador de serviços de TIC à respetiva entidade terceira independente.

(44) Uma vez que apenas as entidades financeiras consideradas para efeitos da realização de testes avançados de resiliência digital deverão ser obrigadas a realizar testes de penetração baseados em ameaças, os processos administrativos e os custos financeiros que a realização de tais testes implicam deverão recair sobre uma pequena percentagem das entidades financeiras.

(45) A fim de 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 associado às TIC, os órgãos de administração das entidades financeiras deverão estar obrigados a manter um papel fulcral e ativo na orientação e adaptação do quadro de gestão do risco associado às TIC e da estratégia global de resiliência digital operacional. A abordagem a adotar pelos órgãos de administração deverá centrar-se não só nos meios destinados a assegurar a resiliência dos sistemas de TIC como também abranger as pessoas e os processos por meio de um conjunto de políticas que promovam, em cada nível da empresa e junto de todos os funcionários, uma boa sensibilização para os ciber-riscos e o compromisso de respeitar regras básicas de cibersegurança rigorosas a todos os níveis. A responsabilidade última do órgão de administração pela gestão do risco associado às TIC de uma entidade financeira deverá 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 associado às TIC.

(46) Além disso, o princípio da responsabilidade total e última do órgão de administração pela gestão do risco associado às TIC da entidade financeira está estreitamente ligado à necessidade de garantir um nível de investimento relacionado com as TIC e um orçamento global da entidade financeira que lhe permita alcançar um nível elevado de resiliência operacional digital.

(47) Inspirando-se nas boas práticas, orientações, recomendações e abordagens pertinentes a nível internacional, nacional e setorial em matéria de gestão dos ciber-riscos, o presente regulamento promove um conjunto de princípios que facilitam a estruturação geral da gestão do risco associado às TIC. Por conseguinte, as entidades financeiras deverão ter liberdade para utilizar modelos de gestão do risco associado às TIC enquadrados ou categorizados de diferentes formas, desde que as principais capacidades criadas pelas entidades financeiras respondam às diferentes funções de gestão do risco associado às TIC (identificação, proteção e prevenção, deteção, resposta e recuperação, aprendizagem e evolução e notificação) estabelecidas no presente regulamento.

(48) A fim de acompanhar o ritmo de um cenário de ciberameaças em rápida evolução, as entidades financeiras deverão dispor de sistemas de TIC atualizados que sejam fiáveis e tenham capacidade não só para garantir o tratamento dos dados necessários para os seus serviços, mas também para assegurar uma resiliência tecnológica suficiente que lhes permita dar uma resposta adequada às necessidades adicionais de tratamento decorrentes de condições de tensão no mercado ou outras situações adversas.

(49) 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, em conformidade com as suas políticas de salvaguarda. No entanto, essa retoma não pode, de modo algum, pôr em risco a integridade e segurança dos sistemas de rede e informação nem a disponibilidade, autenticidade, integridade ou confidencialidade, dos dados.

(50) Embora o presente regulamento autorize as entidades financeiras a determinarem de modo flexível os seus objetivos em termos de tempo de recuperação e ponto 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, deverá, contudo, exigir que realizem uma avaliação do potencial impacto global na eficiência do mercado ao determinar os referidos objetivos.

(51) Os disseminadores de ciberataques tendem a procurar obter ganhos financeiros diretamente na fonte, expondo assim as entidades financeiras a consequências significativas. A fim de evitar que os sistemas de TIC percam a integridade ou fiquem indisponíveis e, por conseguinte, evitar a violação de dados e danos para a infraestrutura física de TIC, é necessário melhorar significativamente e simplificar a notificação de incidentes de caráter severo relacionados com as TIC por parte das entidades financeiras. A notificação de incidentes relacionados com as TIC deverá ser harmonizada mediante a introdução de um requisito aplicável a todas as entidades financeiras, exigindo que estas notifiquem diretamente as respetivas autoridades competentes relevantes. Caso uma entidade financeira esteja sujeita a supervisão por mais do que uma autoridade nacional competente, os Estados-Membros deverão designar uma única autoridade competente como destinatária dessa notificação. As instituições de crédito avaliadas como significativas nos termos do artigo 6.º, n.º 4, do Regulamento (UE) n.º 1024/2013 do Conselho ([19]) deverão apresentar essa notificação às autoridades nacionais competentes, que subsequentemente a deverão transmitir ao Banco Central Europeu (BCE).

(52) Essa notificação direta deverá permitir que as autoridades de supervisão financeira tenham acesso imediato a informações sobre incidentes de caráter severo relacionados com as TIC. Por sua vez, as autoridades de supervisão financeira deverão transmitir pormenores de incidentes de caráter severo relacionados com as TIC às autoridades públicas não financeiras (como as autoridades competentes e os pontos de contacto únicos nos termos da Diretiva (UE) 2022/2555, as autoridades nacionais de proteção de dados e as autoridades responsáveis pela aplicação da lei em caso de incidentes de caráter severo relacionados com as TIC de natureza criminosa), a fim de aumentar a sensibilização dessas autoridades para esse tipo de incidentes e, no caso das CSIRT, facilitar a assistência imediata que pode ser prestada às entidades financeiras, se for caso disso. Além disso, os Estados-Membros deverão poder determinar que as próprias entidades financeiras forneçam essas informações a autoridades públicas fora do domínio dos serviços financeiros. Esses fluxos de informação deverão permitir que as entidades financeiras beneficiem rapidamente de qualquer contributo técnico pertinente, aconselhamento sobre medidas corretivas e subsequente acompanhamento por parte dessas autoridades. É necessário canalizar numa base mútua as informações sobre incidentes de caráter severo relacionados com as TIC: as autoridades de supervisão financeira deverão transmitir todas as observações ou orientações necessárias à entidade financeira, ao passo que as AES deverão partilhar dados anonimizados sobre as ciberameaças e vulnerabilidades relacionadas com um evento, a fim de contribuir para uma defesa coletiva mais alargada.

(53) Embora todas as entidades financeiras devam ser obrigadas a proceder à notificação de incidentes, não se prevê que esse requisito as afete todas do mesmo modo. Com efeito, os limiares de materialidade pertinentes, bem como os prazos de notificação, deverão ser devidamente ajustados, no contexto de atos delegados baseados em normas técnicas de regulamentação a desenvolver pelas AES, a fim de abranger apenas os incidentes de caráter severo relacionados com as TIC. Além disso, as especificidades das entidades financeiras deverão ser tidas em conta na fixação dos prazos aplicáveis às obrigações de notificação.

(54) O presente regulamento deverá exigir que as instituições de crédito, as instituições de pagamento, os prestadores de serviços de informação sobre contas e as instituições de moeda eletrónica notifiquem todos os incidentes operacionais ou de segurança relacionados com pagamentos — anteriormente notificados nos termos da Diretiva (UE) 2015/2366 — independentemente da natureza do incidente relacionado com as TIC.

([19]) 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).

(55) As AES deverão ser incumbidas de analisar a viabilidade e as condições de uma eventual centralização da notificação de incidentes relacionados com as TIC a nível da União. Essa centralização poderá consistir numa plataforma única da UE para a notificação de incidentes de caráter severo relacionados com as TIC que receba diretamente as notificações pertinentes e proceda automaticamente à notificação das autoridades competentes ou simplesmente centralize os relatórios pertinentes que lhe sejam transmitidos pelas autoridades competentes nacionais, desempenhando assim uma função de coordenação. As AES deverão ser incumbidas de elaborar, em consulta com o BCE e a ENISA, um relatório conjunto que explore a viabilidade do estabelecimento de uma plataforma única da UE.

(56) A fim de alcançar um nível elevado de resiliência operacional digital, e em consonância quer com as normas internacionais pertinentes (por exemplo, os elementos fundamentais da realização de testes de penetração baseados em ameaças, elaborados pelo G7) quer com os quadros aplicados na União, como o TIBER–EU (do inglês *Threat Intelligence based Ethical Red teaming*), afigura-se oportuno que as entidades financeiras realizem regularmente testes aos seus sistemas de TIC, bem como ao pessoal com responsabilidades relacionadas com as TIC, em termos de eficácia das respetivas capacidades de prevenção, deteção, resposta e recuperação, a fim de detetar e resolver possíveis vulnerabilidades no domínio das TIC. Para atender às diferenças que existem entre os diversos subsetores financeiros e dentro dos próprios subsetores no que respeita ao nível de preparação das entidades financeiras no domínio da cibersegurança, a realização dos testes deverá compreender uma ampla variedade de instrumentos e medidas, desde a avaliação de requisitos básicos (por exemplo, avaliações e rastreamento de vulnerabilidade, análises de fonte aberta, avaliações da segurança das redes, análises das lacunas, análises da segurança física, questionários e programas informáticos de rastreamento, revisões do código fonte, se possível, testes baseados em cenários, testes de compatibilidade, testes de desempenho ou testes de extremo a extremo) a testes mais avançados, por meio de TLPT. Esses testes mais avançados deverão ser exigidos apenas a entidades financeiras com uma maturidade suficiente em termos de TIC para os realizarem de forma razoável. Os testes de resiliência operacional digital exigidos pelo presente regulamento deverão, por conseguinte, ser mais exigentes para essas entidades financeiras que preencham os critérios previstos no presente regulamento (por exemplo, as instituições de crédito grandes, sistémicas e maduras em matéria de TIC, as bolsas de valores, as centrais de valores mobiliários e as contrapartes centrais) do que para as demais entidades financeiras. Simultaneamente, a realização de testes de resiliência operacional digital por meio de TLPT deverá ser mais pertinente para as entidades financeiras que operam em subsetores com serviços financeiros fundamentais e têm uma função sistémica (por exemplo, pagamentos, banca, compensação e liquidação), e menos pertinente para outros subsetores (por exemplo, gestores de ativos e agências de notação de risco).

(57) As entidades financeiras que participem em atividades transfronteiriças e que exerçam a liberdade de estabelecimento ou prestação de serviços na União deverão cumprir um conjunto único de requisitos de realização de testes avançados (por exemplo, TLPT) no respetivo Estado-Membro de origem, o qual deverá abranger as infraestruturas de TIC em todas as jurisdições em que os grupos financeiros transfronteiriços desenvolvam a sua atividade na União, permitindo assim aos referidos grupos suportar os custos dos testes relacionados com as TIC numa única jurisdição.

(58) A fim de tirar partido dos conhecimentos especializados já adquiridos por determinadas autoridades competentes, em especial no que respeita à aplicação do quadro TIBER–EU, o presente regulamento deverá permitir que os Estados-Membros designem uma única autoridade pública como responsável no setor financeiro, a nível nacional, por todas as questões relacionadas com os TLPT, ou que as autoridades competentes deleguem, na ausência dessa designação, o exercício de funções relacionadas com os TLPT noutra autoridade financeira competente nacional.

(59) Uma vez que o presente regulamento não exige que as entidades financeiras abranjam todas as funções críticas ou importantes num único teste de penetração baseado em ameaças, as entidades financeiras deverão ter liberdade para determinar quais e quantas funções críticas ou importantes deverão ser incluídas no âmbito desse teste.

(60) A realização de testes agrupados na aceção do presente regulamento — que envolvam a participação de várias entidades financeiras num TLPT e relativamente aos quais um terceiro prestador de serviços de TIC pode celebrar diretamente acordos contratuais com um testador externo — só deverá ser autorizada nos casos em que haja motivos razoáveis para esperar que a qualidade ou segurança dos serviços prestados pelo terceiro prestador de serviços de TIC a clientes que não sejam abrangidos pelo âmbito de aplicação do presente regulamento, ou a confidencialidade dos dados relacionados com esses serviços, sejam adversamente afetadas; a realização de testes agrupados deverá estar igualmente sujeita a garantias (orientação por uma entidade financeira designada, adaptação do número de entidades financeiras participantes) para assegurar uma realização rigorosa de testes às entidades financeiras envolvidas que cumpram os objetivos do TLPT nos termos do presente regulamento.

(61) A fim de tirar partido dos recursos internos disponíveis a nível da empresa, o presente regulamento deverá permitir o recurso a testadores internos para efeitos da realização de TLPT, sob reserva de aprovação da autoridade de supervisão, da inexistência de conflitos de interesses e de alternação periódica relativamente ao recurso a testadores internos e externos (de três em três testes), exigindo simultaneamente que o fornecedor das informações sobre ameaças no TLPT seja sempre externo à entidade financeira. A responsabilidade pela realização do TLPT deverá continuar a caber plenamente à entidade financeira. Os comprovativos fornecidos pelas autoridades deverão destinar-se exclusivamente a fins de reconhecimento mútuo e não deverão excluir quaisquer medidas de acompanhamento necessárias para dar resposta ao risco associado às TIC a que a entidade financeira está exposta, nem deverão ser considerados uma validação decorrente da supervisão das capacidades de gestão e mitigação do risco associado às TIC de uma entidade financeira.

(62) A fim de assegurar uma robusta monitorização do risco associado às TIC devido a terceiros no setor financeiro, convém estabelecer um conjunto de regras com base em princípios para orientar as entidades financeiras ao monitorizarem os riscos decorrentes da externalização de funções a terceiros prestadores de serviços de TIC, nomeadamente no caso de serviços de TIC de apoio a funções críticas ou importantes, bem como, de modo mais geral, no contexto de todas as dependências de terceiros no domínio das TIC.

(63) A fim de dar resposta à complexidade das diferentes fontes de risco associado às TIC, tendo simultaneamente em conta a multiplicidade e a diversidade dos fornecedores de soluções tecnológicas que permitem uma prestação harmoniosa de serviços financeiros, o presente regulamento deverá abranger uma vasta gama de terceiros prestadores de serviços de TIC, incluindo prestadores de serviços de computação em nuvem, de programas informáticos e de serviços de análise de dados e prestadores de serviços de centros de dados. Do mesmo modo, uma vez que as entidades financeiras deverão identificar e gerir de forma eficaz e coerente todos os tipos de risco, incluindo no contexto dos serviços de TIC adquiridos no âmbito de um grupo financeiro, importa clarificar que as empresas que fazem parte de um grupo financeiro e prestam predominantemente serviços de TIC à sua empresa-mãe, ou a filiais ou sucursais da sua empresa-mãe, bem como as entidades financeiras que prestam serviços de TIC a outras entidades financeiras, também deverão ser consideradas terceiros prestadores de serviços de TIC nos termos do presente regulamento. Por último, à luz da evolução do mercado dos serviços de pagamento, que depende cada vez mais de soluções técnicas complexas, e tendo em conta os novos tipos de serviços de pagamento e soluções relacionadas com pagamentos, os participantes no ecossistema de serviços de pagamento que prestem atividades de processamento de pagamentos ou operem infraestruturas de pagamento deverão também ser considerados terceiros prestadores de serviços de TIC nos termos do presente regulamento, com exceção dos bancos centrais, ao gerirem sistemas de pagamento ou de liquidação de valores mobiliários, e das autoridades públicas, ao prestarem serviços relacionados com as TIC no contexto do cumprimento de funções do Estado.

(64) As entidades financeiras deverão manter sempre a plena responsabilidade pelo cumprimento das suas obrigações estabelecidas no presente regulamento. As entidades financeiras deverão adotar uma abordagem proporcionada da monitorização dos riscos ao nível dos terceiros prestadores de serviços de TIC, tendo em devida conta a natureza, escala, complexidade e importância das suas dependências relacionadas com as TIC e a criticalidade ou importância dos serviços, dos processos ou das funções objeto de acordos contratuais, bem como, em última análise, tendo por base uma cuidadosa avaliação do possível impacto na continuidade e qualidade dos serviços financeiros a nível individual e a nível do grupo, se for caso disso.

(65) A realização de tal monitorização deverá seguir uma abordagem estratégica do risco associado às TIC devido a terceiros formalizada por meio da adoção, pelo órgão de administração da entidade financeira, de uma estratégia específica para o risco associado às TIC devido a terceiros, radicada na análise contínua de todas as dependências de terceiros no domínio das TIC. A fim de que as autoridades de supervisão tenham melhor conhecimento das dependências de terceiros no domínio das TIC, e com vista a prestar maior apoio aos trabalhos no contexto do quadro de superintendência estabelecido no presente regulamento, todas as entidades financeiras deverão ser obrigadas a manter um registo de informações com todos os acordos contratuais relativos à utilização de serviços de TIC prestados por terceiros prestadores de serviços de TIC. As autoridades de supervisão financeira deverão poder solicitar o registo de informações completo, ou solicitar secções específicas do mesmo, obtendo assim informações essenciais que lhes permitam ter uma compreensão mais ampla das dependências das entidades financeiras no domínio das TIC.

(66) A celebração formal dos acordos contratuais deverá estar subjacente e deverá preceder uma análise exaustiva na fase pré-contratual, centrando-se, em especial, em elementos como a criticalidade ou importância dos serviços apoiados pelo contrato de TIC previsto, as necessárias aprovações da autoridade de supervisão ou outras condições, o eventual risco de concentração inerente, bem como aplicando a devida diligência no processo de seleção e avaliação de terceiros prestadores de serviços de TIC e avaliando potenciais conflitos de interesses. No que se refere aos acordos contratuais relativos a funções críticas ou importantes, as entidades financeiras deverão ter em conta a utilização, por terceiros prestadores de serviços de TIC, das normas mais atualizadas e mais rigorosas em matéria de segurança da informação. A rescisão de acordos contratuais poderá ser desencadeada por, pelo menos, uma série de

circunstâncias que revelem insuficiências a nível do terceiro prestador de serviços de TIC, em especial violações significativas da legislação ou das condições contratuais, circunstâncias que revelem uma potencial alteração do desempenho das funções previstas nos acordos contratuais, provas de debilidades por parte do terceiro prestador de serviços de TIC na sua gestão global do risco associado às TIC, ou circunstâncias que demonstrem a incapacidade da autoridade competente relevante para supervisionar eficazmente a entidade financeira.

(67) A fim de fazer face ao impacto sistémico do risco de concentração de terceiros no domínio das TIC, o presente regulamento promove uma solução equilibrada, adotando uma abordagem flexível e gradual desse risco de concentração, uma vez que a imposição de limites máximos rígidos ou restrições rigorosas pode prejudicar o exercício da atividade e restringir a liberdade contratual. As entidades financeiras deverão avaliar exaustivamente os acordos contratuais que preveem celebrar a fim de identificar a probabilidade do surgimento desse risco, incluindo por meio de análises em profundidade de acordos de subcontratação, em especial nos casos em que sejam celebrados com terceiros prestadores de serviços de TIC estabelecidos em países terceiros. Nesta fase, com vista a encontrar a um equilíbrio justo entre o imperativo que dita a preservação da liberdade contratual e o que dita a salvaguarda da estabilidade financeira, não se afigura adequado estabelecer regras relativas a limites máximos rigorosos e limites de exposição a terceiros no domínio das TIC. No contexto do quadro de superintendência, a autoridade fiscalizadora principal designada nos termos do presente regulamento deverá, no que diz respeito aos terceiros prestadores de serviços de TIC críticos, prestar especial atenção a fim de compreender plenamente o grau das interdependências, 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 e manter um diálogo com terceiros prestadores de serviços de TIC críticos, sempre que esse risco específico seja identificado.

(68) A fim de avaliar e monitorizar regularmente a capacidade de um terceiro prestador de serviços de TIC de prestar, de modo seguro, serviços a uma entidade financeira sem afetar negativamente a resiliência operacional digital dessa entidade financeira, importa proceder à harmonização de vários elementos contratuais fundamentais acordados com os terceiros prestadores de serviços de TIC. Essa harmonização deverá abranger domínios mínimos que sejam cruciais para permitir que a entidade financeira monitorize plenamente os riscos que poderão advir do terceiro prestador de serviços de TIC, na perspetiva da necessidade de uma entidade financeira garantir a sua resiliência digital, uma vez que está profundamente dependente da estabilidade, funcionalidade, disponibilidade e segurança dos serviços de TIC que lhe são prestados.

(69) Aquando da renegociação de acordos contratuais a fim de os alinhar com os requisitos do presente regulamento, as entidades financeiras e os terceiros prestadores de serviços de TIC deverão assegurar a cobertura das principais disposições contratuais previstas no presente regulamento.

(70) A definição de «função crítica ou importante» prevista no presente regulamento abrange as «funções críticas» previstas no artigo 2.º, n.º 1, ponto 35, da Diretiva 2014/59/UE do Parlamento Europeu e do Conselho ([20]). Assim, as funções consideradas críticas nos termos da Diretiva 2014/59/UE estão incluídas na definição de «funções críticas» na aceção do presente regulamento.

(71) Independentemente da criticalidade ou importância da função apoiada pelos serviços de TIC, os acordos contratuais deverão, 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 deverão ser tratados os dados, assim como uma indicação das descrições do nível de serviço. Outros elementos essenciais para que uma entidade financeira possa monitorizar o risco associado às TIC devido a terceiros são: disposições contratuais que especificam a forma como a acessibilidade, a disponibilidade, a integridade, a segurança e a proteção de dados pessoais são asseguradas pelo terceiro prestador de serviços de TIC. Igualmente essenciais são as disposições que estabelecem garantias pertinentes para permitir o acesso, a recuperação e a devolução de dados em caso de insolvência, resolução ou cessação da atividade do terceiro prestador de serviços de TIC, bem como as disposições que exigem que o terceiro prestador de serviços de TIC preste assistência em caso de incidentes relacionados com as TIC decorrentes dos serviços prestados, sem custos adicionais ou com um custo previamente determinado; as disposições relativas à obrigação de o terceiro

([20]) 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).

prestador de serviços de TIC cooperar plenamente com as autoridades competentes e as autoridades de resolução da entidade financeira; e as disposições relativas aos direitos de rescisão e períodos mínimos de pré-aviso relacionados com a rescisão dos acordos contratuais, em conformidade com as expectativas das autoridades competentes e das autoridades de resolução.

(72) Para além das disposições contratuais referidas anteriormente, e a fim de assegurar que as entidades financeiras continuam a ter pleno controlo de todos os acontecimentos a nível de terceiros suscetíveis de comprometer a respetiva segurança no domínio das TIC, os contratos relativos à prestação de serviços de TIC de apoio a funções críticas ou importantes deverão prever igualmente os seguintes elementos: a especificação das descrições completas do nível de serviço, com metas de desempenho quantitativas e qualitativas precisas, a fim de permitir a adoção, sem demora injustificada, de medidas corretivas adequadas, quando os níveis de serviço acordados não forem cumpridos; os períodos de pré-aviso e obrigações de notificação pertinentes do terceiro prestador de serviços de TIC em caso de acontecimentos com um potencial impacto importante na capacidade de o terceiro prestador de serviços de TIC prestar eficazmente os respetivos serviços de TIC; a obrigação de o terceiro prestador de serviços de TIC executar e testar planos de contingência para as suas atividades e dispor de medidas, ferramentas e políticas de segurança no domínio das TIC que garantam uma prestação segura de serviços, bem como de participar e cooperar plenamente no TLPT realizado pela entidade financeira.

(73) Os contratos relativos à prestação de serviços de TIC de apoio a funções críticas ou importantes deverão conter igualmente disposições que prevejam os direitos de acesso, inspeção ou auditoria por parte da entidade financeira ou de um terceiro designado para o efeito, bem como o direito a fazer cópias, enquanto instrumentos cruciais da monitorização contínua realizada pelas entidades financeiras do desempenho do terceiro prestador de serviços de TIC, a par da plena cooperação do prestador de serviços durante as inspeções. De igual modo, também a autoridade competente da entidade financeira deverá ter o direito, mediante notificação, de inspecionar e auditar o terceiro prestador de serviços de TIC, sob reserva da proteção de informações confidenciais.

(74) Esses acordos contratuais deverão prever igualmente estratégias de saída específicas que permitam, em especial, períodos obrigatórios de transição durante os quais os terceiros prestadores de serviços de TIC deverão continuar a prestar os serviços pertinentes com vista a reduzir o risco de perturbações a nível da entidade financeira, ou a permitir que esta última passe a recorrer efetivamente a outro terceiro prestador de serviços de TIC ou, em alternativa, mudar para soluções internas, em função da complexidade do serviço de TIC prestado. Além disso, as entidades financeiras abrangidas pelo âmbito de aplicação da Diretiva 2014/59/UE deverão assegurar que os contratos pertinentes relativos a serviços de TIC sejam sólidos e plenamente aplicáveis em caso de resolução dessas entidades financeiras. Por conseguinte, em consonância com as expectativas das autoridades de resolução, essas entidades financeiras deverão assegurar que os contratos pertinentes relativos a serviços de TIC sejam resilientes à resolução. Enquanto continuarem a cumprir as suas obrigações de pagamento, essas entidades financeiras deverão assegurar, entre outros requisitos, que os contratos pertinentes relativos a serviços de TIC contenham cláusulas de não rescisão, de não suspensão e de não alteração por motivos de reestruturação ou resolução.

(75) Além disso, a utilização a título voluntário de cláusulas contratuais normalizadas desenvolvidas pelas autoridades públicas ou pelas instituições da União, em especial, a utilização de cláusulas contratuais desenvolvidas pela Comissão para os serviços de computação em nuvem podem, igualmente, oferecer garantias suplementares às entidades financeiras e aos terceiros prestadores de serviços de TIC, reforçando o nível de segurança jurídica quanto à utilização de serviços de computação em nuvem pelo setor financeiro, em total consonância com os requisitos e as expectativas estabelecidas pelo direito da União dos serviços financeiros. O desenvolvimento de cláusulas contratuais normalizadas assenta 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 em serviços de computação em nuvem a nível intersetorial já facilitados pela Comissão, com o apoio da participação do setor financeiro.

(76) A fim de promover a convergência e eficiência no que respeita às abordagens de supervisão para fazer face ao risco associado às TIC devido a terceiros no setor financeiro, bem como reforçar a resiliência operacional digital das entidades financeiras que dependem de terceiros prestadores de serviços de TIC críticos para a prestação de serviços de TIC que apoiam a prestação de serviços financeiros e, assim, contribuir para preservar a estabilidade do sistema financeiro da União e a integridade do mercado interno de serviços financeiros, os terceiros prestadores de serviços de TIC críticos deverão estar sujeitos a um quadro de superintendência da União. Embora a criação do quadro de superintendência se justifique pelo valor acrescentado de tomar medidas a nível da União e em virtude do papel inerente e das especificidades da utilização dos serviços de TIC na prestação de serviços financeiros, importa

recordar, ao mesmo tempo, que esta solução se afigura adequada apenas no contexto do presente regulamento, que trata especificamente da resiliência operacional digital do setor financeiro. No entanto, este quadro de superintendência não deverá ser considerado um novo modelo para a supervisão da União em outros domínios dos serviços e atividades financeiros.

(77) O quadro de superintendência deverá aplicar-se apenas aos terceiros prestadores de serviços de TIC críticos. Por conseguinte, deverá existir um mecanismo de designação que tenha em conta a dimensão e natureza da dependência do setor financeiro de tais terceiros prestadores de serviços de TIC. Esse mecanismo deverá consistir num conjunto de critérios quantitativos e qualitativos para definir os parâmetros de criticalidade como base para a inclusão no quadro de superintendência. A fim de assegurar a exatidão dessa avaliação, e independentemente da estrutura empresarial do terceiro prestador de serviços de TIC, esses critérios deverão, no caso de um terceiro prestador de serviços de TIC que faça parte de um grupo mais vasto, ter em conta toda a estrutura do grupo de terceiros prestadores de serviços de TIC. Por outro lado, será conveniente conceder uma opção de inclusão a título voluntário no quadro de superintendência aos terceiros prestadores de serviços de TIC que não sejam automaticamente designados em virtude da aplicação desses critérios, ao passo que os terceiros prestadores de serviços de TIC que já estejam sujeitos a quadros de regime de superintendência que apoiam o desempenho das atribuições do Sistema Europeu de Bancos Centrais a que se refere o artigo 127.º, n.º 2, do TFUE deverão estar isentos.

(78) Do mesmo modo, as entidades financeiras que prestam serviços de TIC a outras entidades financeiras, embora pertençam à categoria de terceiros prestadores de serviços de TIC nos termos do presente regulamento, deverão também estar isentas do quadro de superintendência, uma vez que já estão sujeitas aos mecanismos de supervisão estabelecidos pelo direito da União dos serviços financeiros aplicável. Se for caso disso, as autoridades competentes deverão ter em conta, no contexto das suas atividades de superintendência, o risco associado às TIC para as entidades financeiras por entidades financeiras que prestam serviços de TIC. Do mesmo modo, devido aos mecanismos de monitorização dos riscos existentes a nível do grupo, deverá ser introduzida a mesma isenção para os terceiros prestadores de serviços de TIC que prestam serviços predominantemente às entidades do seu próprio grupo. Os terceiros prestadores de serviços de TIC que prestam serviços de TIC apenas num Estado-Membro a entidades financeiras que operam apenas nesse Estado-Membro deverão também estar isentos do mecanismo de designação devido à limitação das suas atividades e à ausência de impacto transfronteiriço.

(79) A transformação digital no domínio dos serviços financeiros acarretou um nível sem precedentes de utilização e dependência dos serviços de TIC. Uma vez que se tornou inconcebível prestar serviços financeiros sem recorrer a serviços de computação em nuvem, programas informáticos e serviços relacionados com dados, o ecossistema financeiro da União tornou-se intrinsecamente codependente de determinados serviços de TIC prestados por fornecedores de serviços de TIC. Alguns desses fornecedores, inovadores no desenvolvimento e aplicação de tecnologias baseadas nas TIC, desempenham um papel significativo na prestação de serviços financeiros ou passaram a integrar a cadeia de valor dos serviços financeiros. Tornaram-se, assim, críticos para a estabilidade e integridade do sistema financeiro da União. Esta dependência generalizada dos serviços prestados por terceiros prestadores de serviços de TIC críticos, combinada com a interdependência dos sistemas de informação de vários operadores de mercado, cria um risco direto, potencialmente grave, para o sistema de serviços financeiros da União e para a continuidade da prestação de serviços financeiros, caso os terceiros prestadores de serviços de TIC críticos sejam afetados por perturbações operacionais ou ciberincidentes de caráter severo. Os ciberincidentes distinguem-se pela capacidade de se multiplicarem e propagarem em todo o sistema financeiro a um ritmo consideravelmente mais rápido do que outros tipos de risco monitorizados no setor financeiro e podem alastrar a vários setores e para além das fronteiras geográficas. Podem redundar numa crise sistémica, traduzida num enfraquecimento da confiança no sistema financeiro devido à perturbação das funções de apoio à economia real, ou em perdas financeiras substanciais, a um ponto que o sistema financeiro seja incapaz de suportar, ou que exija a aplicação de medidas para absorver choques graves. A fim de evitar estes cenários, pondo assim em perigo a estabilidade financeira e a integridade da União, é essencial assegurar a convergência das práticas de supervisão relativas ao risco associado às TIC devido a terceiros no setor financeiro, em especial através de novas regras que permitam a superintendência pela União de terceiros prestadores de serviços de TIC críticos.

(80) O quadro de superintendência depende, em grande medida, do grau de colaboração entre a autoridade fiscalizadora principal e o terceiro prestador de serviços de TIC crítico que presta serviços a entidades financeiras que afetam a prestação de serviços financeiros. O êxito da superintendência depende, nomeadamente, da capacidade da autoridade fiscalizadora principal para realizar eficazmente missões de monitorização e inspeções para avaliar as regras, os controlos e os processos utilizados pelos terceiros prestadores de serviços de TIC críticos, bem como para avaliar o potencial impacto cumulativo das suas atividades na estabilidade financeira e na integridade do sistema financeiro. Ao mesmo tempo, é crucial que os terceiros prestadores de serviços de TIC críticos acatem as recomendações da autoridade fiscalizadora principal e deem resposta às suas preocupações. Uma vez que a falta de cooperação de um terceiro prestador de serviços de TIC crítico que presta serviços que afetam o fornecimento de serviços financeiros, como a recusa de conceder acesso às suas instalações ou de apresentar informações, privaria, em última análise, a autoridade fiscalizadora principal das suas ferramentas essenciais para avaliar o risco associado às TIC devido a terceiros e poderia afetar negativamente a estabilidade financeira e a integridade do sistema financeiro, é igualmente necessário prever um regime de sanções proporcionado.

(81) Neste contexto, a necessidade de a autoridade fiscalizadora principal impor sanções pecuniárias para obrigar os terceiros prestadores de serviços de TIC críticos a cumprir as obrigações em matéria de transparência e de acesso estabelecidas no presente regulamento não deverá ser posta em causa pelas dificuldades devidas à aplicação dessas sanções em relação a terceiros prestadores de serviços de TIC críticos estabelecidos em países terceiros. A fim de assegurar a aplicabilidade dessas sanções e permitir uma rápida implementação de procedimentos que respeitem os direitos de defesa dos terceiros prestadores de serviços de TIC críticos no contexto do mecanismo de designação e da emissão de recomendações, os referidos terceiros prestadores de serviços de TIC críticos que prestem serviços a entidades financeiras que afetem a prestação de serviços financeiros deverão ser obrigados a assegurar uma presença comercial adequada na União. Devido à natureza da supervisão e à ausência de disposições comparáveis noutras jurisdições, não existem mecanismos alternativos adequados que garantam este objetivo através de uma cooperação eficaz com as autoridades de supervisão financeira de países terceiros no que diz respeito à monitorização do impacto dos riscos operacionais digitais colocados por terceiros prestadores de serviços de TIC sistémicos, considerados terceiros prestadores de serviços de TIC críticos estabelecidos em países terceiros. Por conseguinte, a fim de continuar a prestar serviços de TIC a entidades financeiras na União, um terceiro prestador de serviços de TIC estabelecido num país terceiro designado como crítico nos termos do presente regulamento deverá, no prazo de 12 meses a contar dessa designação, tomar todas as medidas necessárias para assegurar a sua incorporação na União, através do estabelecimento de uma filial, na aceção da globalidade do acervo da União, nomeadamente a Diretiva 2013/34/UE do Parlamento Europeu e do Conselho ([21]).

(82) O requisito de criar uma filial na União não deverá impedir o terceiro prestador de serviços de TIC crítico de prestar serviços de TIC e apoio técnico conexo a partir de instalações e infraestruturas situadas fora da União. O presente regulamento não impõe uma obrigação de localização de dados, uma vez que não exige o armazenamento ou o tratamento de dados na União.

(83) Os terceiros prestadores de serviços de TIC críticos deverão poder prestar serviços de TIC a partir de qualquer parte do mundo, não necessariamente ou não apenas em instalações situadas na União. As atividades de superintendência deverão ser realizadas, em primeiro lugar, em instalações situadas na União e através da interação com entidades localizadas na União, incluindo as filiais estabelecidas por terceiros prestadores de serviços de TIC críticos nos termos do presente regulamento. No entanto, essas ações no interior da União podem não ser suficientes para que a autoridade fiscalizadora principal possa desempenhar plena e eficazmente as suas funções nos termos do presente regulamento. Por conseguinte, a autoridade fiscalizadora principal deverá também poder exercer os seus poderes de superintendência pertinentes em países terceiros. O exercício desses poderes em países terceiros deverá permitir à autoridade fiscalizadora principal examinar as instalações a partir das quais os serviços de TIC ou os serviços de apoio técnico são efetivamente prestados ou geridos pelo terceiro prestador de serviços de TIC crítico e deverá proporcionar à autoridade fiscalizadora principal uma compreensão abrangente e operacional da gestão do risco associado às TIC por parte do terceiro prestador de serviços de TIC crítico. A possibilidade de a autoridade fiscalizadora principal, enquanto agência da União, exercer poderes fora do território da União deverá ser devidamente enquadrada pelas condições pertinentes, em especial o consentimento do terceiro prestador de serviços de TIC crítico em causa. Analogamente, as autoridades competentes do país terceiro deverão ser informadas do exercício, no seu próprio território, das atividades da autoridade fiscalizadora principal, e não terem levantado objeções a esse exercício. No entanto, a fim de assegurar uma execução eficiente, e sem prejuízo das

([21]) Diretiva 2013/34/UE do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativa às demonstrações financeiras anuais, às demonstrações financeiras consolidadas e aos relatórios conexos de certas formas de empresas, que altera a Diretiva 2006/43/CE do Parlamento Europeu e do Conselho e revoga as Diretivas 78/660/CEE e 83/349/CEE do Conselho (JO L 182 de 29.6.2013, p. 19).

competências respetivas das instituições da União e dos Estados-Membros, esses poderes deverão também ser plenamente consagrados quando são celebrados acordos de cooperação administrativa com as autoridades competentes relevantes do país terceiro em causa. O presente regulamento deverá, por conseguinte, permitir que as AES celebrem acordos de cooperação administrativa com as autoridades relevantes de países terceiros, que, aliás, não deverão criar obrigações jurídicas para a União e os seus Estados-Membros.

(84) A fim de facilitar a comunicação com a autoridade fiscalizadora principal e assegurar uma representação adequada, os terceiros prestadores de serviços de TIC críticos que façam parte de um grupo deverão designar uma pessoa coletiva como ponto de coordenação.

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

(86) A fim de tirar melhor partido da arquitetura institucional multifacetada no domínio dos serviços financeiros, o Comité Conjunto das AES deverá continuar a assegurar a coordenação intersetorial global quanto a todas as matérias relativas ao risco associado às TIC, em consonância com as suas atribuições em matéria de cibersegurança. Deverá ter o apoio de um novo subcomité (o «fórum de superintendência»), que leva a cabo os trabalhos preparatórios quer para as decisões individuais dirigidas a terceiros prestadores de serviços de TIC críticos quer para a emissão de recomendações coletivas, em especial no que se refere à avaliação comparativa dos programas de superintendência de terceiros prestadores de serviços de TIC críticos e à identificação de boas práticas para dar resposta às questões relativas ao risco de concentração no domínio das TIC.

(87) A fim de assegurar que os terceiros prestadores de serviços de TIC críticos são supervisionados de forma adequada e eficaz a nível da União, o presente regulamento prevê que qualquer das três AES possa ser designada como autoridade fiscalizadora principal. A atribuição individual de um terceiro prestador de serviços de TIC crítico a uma das três AES deverá resultar de uma avaliação que determine as entidades financeiras que operam predominantemente nos setores financeiros da responsabilidade dessa AES. Esta abordagem deverá assegurar uma repartição equilibrada de tarefas e responsabilidades entre as três AES, no contexto do exercício das funções de supervisão, e deverá utilizar da melhor forma os recursos humanos e as competências técnicas disponíveis em cada uma das três AES.

(88) A autoridade de superintendência principal deverá ser dotada dos poderes necessários para realizar investigações e inspeções no local e à distância às instalações e locais pertinentes dos terceiros prestadores de serviços de TIC críticos e para obter informações completas e atualizadas. Esses poderes deverão permitir à autoridade fiscalizadora principal obter um efetivo conhecimento do tipo, da dimensão e do impacto do risco associado às TIC devido a terceiros que as entidades financeiras e, em última análise, o sistema financeiro da União enfrentam. Confiar às AES o papel de liderança da superintendência constitui uma condição prévia para compreender e fazer face à dimensão sistémica do risco associado às TIC no setor financeiro. O impacto dos terceiros prestadores de serviços de TIC críticos no setor dos serviços financeiros da União e os potenciais problemas provocados pelo risco de concentração no domínio das TIC exigem a adoção de uma abordagem coletiva a nível da União. A realização simultânea e em separado de múltiplas auditorias e os direitos de acesso por numerosas autoridades competentes, com pouca ou nenhuma coordenação, obstaria a que os supervisores financeiros obtivessem uma visão global completa e abrangente do risco associado às TIC devido a terceiros na União, criando também redundância, encargos e complexidade para os terceiros prestadores de serviços de TIC críticos se fossem sujeitos a numerosos pedidos de monitorização e inspeção.

(89) Devido às importantes repercussões que a designação como crítico implica, o presente regulamento deverá assegurar que os direitos dos terceiros prestadores de serviços de TIC críticos são respeitados ao longo da aplicação do quadro de superintendência. Antes de serem designados como críticos, esses prestadores deverão, por exemplo, ter o direito de apresentar à autoridade fiscalizadora uma declaração fundamentada que contenha todas as informações relevantes para efeitos da avaliação relacionada com a sua designação. Uma vez que a autoridade de superintendência principal deverá estar habilitada a apresentar recomendações sobre questões relativas ao risco associado às TIC e respetivas medidas corretivas, que incluem os poderes de se opor a determinados acordos contratuais que, em última análise, afetam a estabilidade da entidade financeira ou do sistema financeiro, os terceiros prestadores de serviços de TIC críticos deverão também ter a oportunidade de fornecer, antes da finalização dessas recomendações, explicações sobre o impacto esperado das soluções previstas nas recomendações sobre os clientes que sejam entidades não abrangidas pelo âmbito de aplicação do presente regulamento e de

formular soluções para atenuar os riscos. Os terceiros prestadores de serviços de TIC críticos que discordem das recomendações deverão apresentar uma explicação fundamentada da sua intenção de não acatar a recomendação. Se essa explicação fundamentada não for apresentada ou for considerada insuficiente, a autoridade fiscalizadora principal deverá emitir um anúncio público que descreva resumidamente a questão do incumprimento.

(90) Nas suas funções de supervisão prudencial das entidades financeiras, as autoridades competentes deverão incluir devidamente a tarefa de verificar o cumprimento substantivo das recomendações emitidas pela autoridade fiscalizadora principal. As autoridades competentes deverão poder exigir que as entidades financeiras tomem medidas adicionais para fazer face aos riscos identificados nas recomendações da autoridade fiscalizadora principal e deverão, em devido tempo, emitir notificações para esse efeito. Caso a autoridade fiscalizadora principal dirija recomendações a terceiros prestadores de serviços de TIC críticos que sejam supervisionadas nos termos da Diretiva (UE) 2022/2555, as autoridades competentes deverão poder, numa base voluntária e antes de adotar medidas adicionais, consultar as autoridades competentes nos termos dessa diretiva, a fim de promover uma abordagem coordenada em relação aos terceiros prestadores de serviços de TIC críticos em causa.

(91) O exercício da supervisão deverá pautar-se por três princípios operacionais destinados a assegurar: a) a estreita coordenação entre as AES nas suas funções de autoridades fiscalizadoras principais, através de uma rede de superintendência conjunta, b) a coerência com o quadro estabelecido pela Diretiva (UE) 2022/2555 (através da consulta voluntária dos organismos ao abrigo dessa diretiva para evitar a duplicação de medidas dirigidas a terceiros prestadores de serviços de TIC críticos), e c) a diligência para minimizar o potencial risco de perturbação dos serviços prestados pelos terceiros prestadores de serviços de TIC críticos aos clientes que são entidades não abrangidas pelo âmbito de aplicação do presente regulamento.

(92) O quadro de superintendência não deverá substituir, de forma alguma ou em parte alguma, o requisito de que as entidades financeiras se encarreguem elas próprias da gestão dos riscos decorrentes do recurso a terceiros prestadores de serviços de TIC, nomeadamente, a sua obrigação de assegurar a monitorização contínua dos acordos contratuais celebrados com terceiros prestadores de serviços de TIC críticos. De igual forma, o quadro de superintendência não deverá afetar a plena responsabilidade das entidades financeiras pelo cumprimento de todas as obrigações jurídicas estabelecidas no presente regulamento e no direito dos serviços financeiros aplicável.

(93) A fim de evitar duplicações e sobreposições, as autoridades competentes deverão evitar adotar medidas de modo individual que visem a monitorização dos riscos do terceiro prestador de serviços de TIC crítico e deverão, a esse respeito, confiar na avaliação pertinente da autoridade fiscalizadora principal. Quaisquer medidas deverão, em todo o caso, ser coordenadas e acordadas de antemão com a autoridade de superintendência principal no contexto do exercício das atribuições no âmbito do quadro de superintendência.

(94) A fim de promover a convergência a nível internacional no que diz respeito às boas práticas a aplicar no exame e na monitorização da gestão do risco digital por parte 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.

(95) Para tirar melhor partido das competências específicas, das competências técnicas e dos conhecimentos especializados do pessoal especializado em riscos operacionais e associados às TIC das autoridades competentes, as três AES e, a título voluntário, as autoridades competentes nos termos da Diretiva (UE) 2022/2555, a autoridade de superintendência principal deverão aproveitar as capacidades e o conhecimento da supervisão nacional e estabelecer equipas de avaliação para cada terceiro prestador de serviços de TIC crítico, reunindo equipas multidisciplinares para apoiar a preparação e execução de atividades de superintendência, nomeadamente investigações de natureza geral e inspeções no local a terceiros prestadores de serviços de TIC críticos, bem como qualquer acompanhamento posterior que seja necessário.

(96) Embora os custos resultantes das tarefas de superintendência sejam integralmente financiados pelas taxas cobradas aos terceiros prestadores de serviços de TIC críticos, é provável que as AES incorram, antes do início do quadro de superintendência, em custos com a implementação de sistemas de TIC específicos de apoio à futura superintendência, uma vez que os sistemas de TIC específicos terão de ser desenvolvidos e implantados previamente. Por conseguinte, o presente regulamento prevê um modelo de financiamento híbrido, segundo o qual o quadro de superintendência será, enquanto tal, integralmente financiado por taxas, enquanto o desenvolvimento dos sistemas de TIC das AES será financiado a partir das contribuições da União e das autoridades nacionais competentes.

(97) As autoridades competentes deverão estar investidas de todos os poderes de supervisão, investigação e sancionatórios necessários para assegurar o exercício adequado das suas obrigações nos termos do presente regulamento. Deverão, em princípio, publicar os avisos das sanções administrativas que aplicam. 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 competentes, a aplicação do presente regulamento deverá ser facilitada, por um lado, pela 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, e, por outro, pela consulta com as AES, através do intercâmbio de informações e da prestação de assistência no contexto das atividades pertinentes de supervisão.

(98) A fim de quantificar e qualificar mais aprofundadamente os critérios para designar os terceiros prestadores de serviços de TIC como críticos e harmonizar as taxas de superintendência, o poder de adotar atos nos termos do artigo 290.º do TFUE deverá ser delegado na Comissão para completar o presente regulamento especificando mais detalhadamente o impacto sistémico que uma falha ou indisponibilidade operacional de um terceiro prestador de serviços de TIC pode ter nas entidades financeiras às quais presta serviços, o número de instituições de importância sistémica global (G-SII) ou outras instituições de importância sistémica (O-SII) que dependem do terceiro prestador de serviços de TIC em causa, o número de terceiros prestadores de serviços de TIC ativos num dado mercado, os custos de migração dos dados e dos volumes de trabalho de TIC para outro terceiro prestador de serviços de TIC, bem como o montante de taxas de superintendência e as respetivas modalidades de pagamento. É particularmente importante que a Comissão proceda às consultas adequadas durante os trabalhos preparatórios, inclusive a 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 ([22]). 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.

(99) É conveniente que se assegure a harmonização dos requisitos estabelecidos no presente regulamento por meio de normas técnicas de regulamentação. Nos seus papéis de organismos dotados de conhecimentos muito especializados, as AES deverão elaborar projetos de normas técnicas de regulamentação que não impliquem escolhas políticas, a apresentar à Comissão. Deverão ser desenvolvidas normas técnicas de regulamentação em matéria de gestão do risco associado às TIC, notificação de incidentes de caráter severo relacionados com as TIC, realização de testes, bem como em relação aos requisitos essenciais para uma robusta monitorização do risco associado às TIC devido a terceiros. A Comissão e as AES deverão assegurar que essas normas e requisitos podem ser aplicados por todas as entidades financeiras de uma forma que seja proporcionada à sua dimensão e perfil de risco global, e à natureza, escala e complexidade dos seus serviços, atividades e operações. A Comissão deverá ser ainda habilitada a adotar as referidas normas técnicas de regulamentação por meio de atos delegados nos termos do artigo 290.º do TFUE e nos termos dos artigos 10.º a 14.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010, (UE) n.º 1095/2010.

(100) Para facilitar a comparabilidade dos relatórios de incidentes de caráter severo relacionados com as TIC e incidentes de caráter severo operacionais ou de segurança relacionados com pagamentos, bem como assegurar a transparência respeitante aos acordos contratuais a utilizar no âmbito dos serviços de TIC prestados por terceiros prestadores de serviços de TIC, as AES deverão elaborar projetos de normas técnicas de execução que criem procedimentos, formulários e modelos normalizados para que as entidades financeiras possam notificar incidentes de caráter severo relacionados com as TIC e incidentes de caráter severo operacionais ou de segurança relacionados com pagamentos, bem como modelos normalizados para o registo de informações. Ao elaborarem essas normas, as AES deverão ter em conta a dimensão e o perfil de risco global da entidade financeira, bem como a natureza, a escala e a complexidade dos seus serviços, atividades e operações. A Comissão deverá ainda ficar habilitada a adotar as referidas normas técnicas de execução por meio de atos de execução nos termos do artigo 291.º do TFUE e nos termos do artigo 15.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010, (UE) n.º 1095/2010.

([22]) JO L 123 de 12.5.2016, p. 1.

(101) 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 ([23]), (UE) n.º 648/2012 ([24]), (UE) n.º 600/2014 ([25]) e (UE) n.º 909/2014 do Parlamento Europeu e do Conselho ([26]), 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 associado às TIC.

(102) Uma vez que o presente regulamento, juntamente com a Diretiva (UE) 2022/2556 do Parlamento Europeu e do Conselho ([27]), implica uma consolidação das disposições em matéria de gestão do risco associado às TIC em diversos regulamentos e diretivas do acervo da União em matéria de serviços financeiros, nomeadamente os Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014 e (UE) n.º 909/2014 e o Regulamento (UE) 2016/1011 do Parlamento Europeu e do Conselho ([28]), a fim de assegurar a plena coerência, os referidos regulamentos deverão ser alterados para clarificar que as disposições aplicáveis relacionadas com o risco associado às TIC são estabelecidas no presente regulamento.

(103) Por conseguinte, o âmbito de aplicação dos artigos pertinentes relacionados com o risco operacional, sobre os quais os poderes conferidos nos Regulamentos (CE) n.º 1060/2009, (UE) n.º 648/2012, (UE) n.º 600/2014, (UE) n.º 909/2014 e (UE) 2016/1011 preveem a adoção de atos delegados e de execução, deverá ser restringido, com vista a transpor para o presente regulamento todas as disposições que abrangem os aspetos da resiliência operacional digital que atualmente fazem parte desses regulamentos.

(104) O potencial ciber-risco sistémico associado à utilização de infraestruturas de TIC que permitem o funcionamento dos sistemas de pagamento e a realização de atividades de processamento de pagamentos deverão ser devidamente abordados a nível da União através de regras harmonizadas em matéria de resiliência digital. Para o efeito, a Comissão deverá avaliar rapidamente a necessidade de rever o âmbito de aplicação do presente regulamento, alinhando simultaneamente essa revisão com o resultado da revisão global prevista na Diretiva (UE) 2015/2366. Numerosos ataques em grande escala ao longo da última década têm demonstrado como os sistemas de pagamento ficaram expostos a ciberameaças. No centro da cadeia de serviços de pagamento e com fortes interligações com o sistema financeiro global, os sistemas de pagamento e as atividades de processamento de pagamentos assumiram uma importância crítica para o funcionamento dos mercados financeiros da União. Os ciberataques a esses sistemas podem causar graves perturbações operacionais às empresas, com repercussões diretas nas principais funções económicas, como a facilitação dos pagamentos, e com efeitos indiretos nos processos económicos conexos. Até que sejam instituídos, a nível da União, um regime harmonizado e a supervisão dos operadores de sistemas de pagamento e das entidades de processamento, os Estados-Membros podem, com vista à aplicação de práticas de mercado semelhantes, inspirar-se nos requisitos de resiliência operacional digital estabelecidos no presente regulamento, ao aplicarem regras aos operadores de sistemas de pagamento e às entidades de processamento supervisionadas nas suas próprias jurisdições.

([23]) Regulamento (CE) n.º 1060/2009 do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, relativo às agências de notação de risco (JO L 302 de 17.11.2009, p. 1).

([24]) Regulamento (UE) n.º 648/2012 do Parlamento Europeu e do Conselho, de 4 de julho de 2012, relativo aos derivados do mercado de balcão, às contrapartes centrais e aos repositórios de transações (JO L 201 de 27.7.2012, p. 1).

([25]) Regulamento (UE) n.º 600/2014 do Parlamento Europeu e do Conselho, de 15 de maio de 2014, relativo aos mercados de instrumentos financeiros e que altera o Regulamento (UE) n.º 648/2012 (JO L 173 de 12.6.2014, p. 84).

([26]) Regulamento (UE) n.º 909/2014 do Parlamento Europeu e do Conselho, de 23 de julho de 2014, relativo à melhoria da liquidação de valores mobiliários na União Europeia e às Centrais de Valores Mobiliários (CSDs) e que altera as Diretivas 98/26/CE e 2014/65/UE e o Regulamento (UE) n.º 236/2012 (JO L 257 de 28.8.2014, p. 1).

([27]) Diretiva (UE) 2022/2556 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, que altera as Diretivas 2009/65/CE, 2009/138/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE, 2014/65/UE, (UE) 2015/2366 e (UE) 2016/2341 no que diz respeito à resiliência operacional digital do setor financeiro (ver página 153 do presente Jornal Oficial).

([28]) 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).

(105) Atendendo a que o objetivo do presente regulamento, a saber, alcançar um elevado nível de resiliência operacional digital em relação a todas as entidades reguladas do setor financeiro, não pode ser suficientemente alcançado pelos Estados-Membros por requerer a harmonização de várias regras diferentes no direito da União e nacional, 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 esse objetivo.

(106) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([29]) e emitiu parecer em 10 de maio de 2021 ([30]),

ADOTARAM O PRESENTE REGULAMENTO:

CAPÍTULO I

Disposições gerais

Artigo 1.º

Objeto

1. A fim de alcançar um elevado nível de resiliência operacional digital, o presente regulamento estabelece requisitos uniformes no que respeita à segurança dos sistemas de rede e informação que apoiam os processos operacionais das entidades financeiras, como se segue:

a) Requisitos aplicáveis às entidades financeiras em matéria de:

   i) gestão do risco no domínio das tecnologias da informação e comunicação (TIC),

   ii) notificação de incidentes de caráter severo relacionados com as TIC e notificação, numa base voluntária, de ciberameaças significativas às autoridades competentes,

   iii) notificação de incidentes de caráter severo operacionais ou de segurança, relacionados com pagamentos, às autoridades competentes pelas entidades financeiras a que se refere o artigo 2.º, n.º 1, alíneas a) a d),

   iv) realização de testes de resiliência operacional digital,

   v) partilha de dados e informações sobre as ciberameaças e as vulnerabilidades,

   vi) medidas para a boa gestão do risco associado às TIC devido a terceiros;

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

c) Regras para o estabelecimento e execução do quadro de superintendência dos terceiros prestadores de serviços de TIC críticos na prestação desses serviços a entidades financeiras;

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

2. Quanto às entidades financeiras identificadas como entidades essenciais ou importantes nos termos das regras nacionais que transpõem o artigo 3.º da Diretiva (UE) 2022/2555, considera-se que o presente regulamento constitui um ato jurídico setorial da União para efeitos do artigo 4.º da referida diretiva.

3. O presente regulamento não prejudica a responsabilidade dos Estados-Membros no que diz respeito às funções essenciais do Estado respeitantes à segurança pública, à defesa e à segurança nacional, em conformidade com o direito da União.

([29]) Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho, de 23 de outubro de 2018, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas instituições e pelos órgãos e organismos da União e à livre circulação desses dados, e que revoga o Regulamento (CE) n.º 45/2001 e a Decisão n.º 1247/2002/CE (JO L 295 de 21.11.2018, p. 39).

([30]) JO C 229 de 15.6.2021, p. 16.

Artigo 2.º

Âmbito

1. Sem prejuízo no disposto nos n.os 3 e 4, o presente regulamento é aplicável às seguintes entidades:

a) Instituições de crédito;

b) Instituições de pagamento, incluindo instituições de pagamento isentas nos termos da Diretiva (UE) 2015/2366;

c) Prestadores de serviços de informação sobre contas;

d) Instituições de moeda eletrónica, incluindo instituições de moeda eletrónica isentas nos termos da Diretiva 2009/110/CE;

e) Empresas de investimento;

f) Prestadores de serviços de criptoativos, autorizados nos termos de um regulamento do Parlamento Europeu e do Conselho relativo aos mercados de criptoativos, e que altera os Regulamentos (UE) n.º 1093/2010 e (UE) n.º 1095/2010 e as Diretivas 2013/36/UE e (UE) 2019/1937 (o «regulamento relativo aos mercados de criptoativos») e emitentes de criptofichas (tokens) referenciadas a ativos;

g) Centrais de valores mobiliários;

h) Contrapartes centrais;

i) Plataformas de negociação;

j) Repositórios de transações;

k) Gestores de fundos de investimento alternativos;

l) Sociedades gestoras;

m) Prestadores de serviços de comunicação de dados;

n) Empresas de seguros e de resseguros;

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

p) Instituições de realização de planos de pensões profissionais;

q) Agências de notação de risco;

r) Administradores de índices de referência críticos;

s) Prestadores de serviços de financiamento colaborativo;

t) Repositórios de titularizações;

u) Terceiros prestadores de serviços de TIC.

2. Para efeitos do presente regulamento, as entidades a que se refere o n.º 1, alíneas a) a t), são coletivamente referidas como «entidades financeiras».

3. O presente regulamento não se aplica a:

a) Gestores de fundos de investimento alternativos, a que se refere o artigo 3.º, n.º 2, da Diretiva 2011/61/UE;

b) Empresas de seguros e de resseguros, a que se refere o artigo 4.º, da Diretiva 2009/138/CE;

c) Instituições de realização de planos de pensões profissionais que gerem planos de pensões que, no seu conjunto, não tenham mais de 15 membros;

d) Pessoas singulares ou coletivas isentas nos termos dos artigos 2.º e 3.º da Diretiva 2014/65/UE;

e) Mediadores de seguros, mediadores de resseguros e mediadores de seguros a título acessório que sejam microempresas ou pequenas ou médias empresas;

f) Instituições de cheques postais a que se refere o artigo 2.º, n.º 5, ponto 3, da Diretiva 2013/36/UE.

4. Os Estados-Membros podem excluir do âmbito de aplicação do presente regulamento as entidades a que se refere o artigo 2.º, n.º 5, pontos 4 a 23, da Diretiva 2013/36/UE que estejam situadas nos respetivos territórios. Sempre que um Estado-Membro recorrer a essa opção, informa do facto a Comissão, bem como de quaisquer alterações subsequentes. A Comissão disponibiliza essas informações ao público no seu sítio Web ou noutros meios facilmente acessíveis.

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 e fiabilidade operacionais, assegurando direta ou indiretamente, com recurso a serviços fornecidos por terceiros prestadores de serviços de TIC, toda a gama de capacidades relacionadas com as TIC necessárias para salvaguardar a segurança dos sistemas de rede e informação que a entidade financeira utiliza e que permitem a contínua prestação de serviços financeiros e a qualidade dos mesmos, inclusive em alturas de perturbações;

2) «Sistema de rede e informação», um sistema de rede e informação na aceção do artigo 6.º, ponto 1, da Diretiva (UE) 2022/2555;

3) «Sistema de TIC legado», um sistema de TIC que atingiu o fim do seu ciclo de vida (fim de vida), que não é passível de atualizações ou correções, por razões tecnológicas ou comerciais, ou que deixou de ser apoiado pelo seu fornecedor ou por um terceiro prestador de serviços de TIC, mas que ainda está a ser utilizado e apoia as funções da entidade financeira;

4) «Segurança dos sistemas de rede e informação», a segurança dos sistemas de rede e informação na aceção do artigo 6.º, ponto 2, da Diretiva (UE) 2022/2555;

5) «Risco associado às TIC», qualquer circunstância razoavelmente identificável relacionada com a utilização de sistemas de rede e informação que, caso se materialize, pode comprometer a segurança dos sistemas de rede e informação, de qualquer instrumento ou processo dependente de tecnologia, do funcionamento e da execução de processos ou da prestação de serviços, causando efeitos adversos no ambiente digital ou físico;

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

7) «Ativo de TIC», um ativo de programas informáticos ou de equipamentos informáticos nos sistemas de rede e informação utilizados pela entidade financeira;

8) «Incidente relacionado com as TIC», uma ocorrência ou uma série de ocorrências conexas não previstas pelas entidades financeiras que comprometem a segurança dos sistemas de rede e informação e têm um impacto adverso na disponibilidade, autenticidade, integridade ou confidencialidade dos dados ou nos serviços prestados pela entidade financeira;

9) «Incidente operacional ou de segurança relacionado com pagamentos», uma ocorrência ou uma série de ocorrências conexas não previstas pelas entidades financeiras, a que se refere o artigo, 2.º, n.º 1, alíneas a) a d), quer sejam ou não relacionados com as TIC, que têm um impacto adverso na disponibilidade, autenticidade, integridade ou confidencialidade dos dados relacionados com pagamentos ou nos serviços prestados pela entidade financeira relacionados com pagamentos;

10) «Incidente de caráter severo relacionado com as TIC», um incidente relacionado com as TIC que tem um elevado impacto negativo nos sistemas de rede e informação que apoiam funções críticas ou importantes da entidade financeira;

11) «Incidente de caráter severo operacional ou de segurança relacionado com pagamentos», um incidente operacional ou de segurança relacionado com pagamentos que tem um elevado impacto negativo nos serviços prestados relacionados com pagamentos;

12) «Ciberameaça», uma ciberameaça na aceção do artigo 2.º, ponto 8, do Regulamento (UE) 2019/881;

13) «Ciberameaça significativa», uma ciberameaça cujas características técnicas indicam que tem o potencial de resultar num incidente de caráter severo relacionado com as TIC ou num incidente de caráter severo operacional ou de segurança relacionado com pagamentos;

14) «Ciberataque», um incidente doloso relacionado com as TIC provocado por uma tentativa perpetrada pelo autor de ameaças de destruir, revelar, alterar, incapacitar, furtar, obter acesso não autorizado ou utilizar sem autorização um ativo;

15) «Informações sobre ameaças», as informações que foram agregadas, transformadas, analisadas, interpretadas ou suplementadas para dar o contexto necessário à tomada de decisão e permitir 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;

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

17) «Testes de penetração baseados em ameaças (TLPT)», 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 de produção críticos «ao vivo» da entidade financeira;

18) «Risco associado às TIC devido a terceiros», um risco no domínio das TIC a que uma entidade financeira pode estar sujeita no âmbito da sua utilização de serviços de TIC prestados por terceiros prestadores de serviços de TIC ou por subcontratantes desses terceiros, inclusive mediante acordos de subcontratação;

19) «Terceiro prestador de serviços de TIC», uma empresa que presta serviços de TIC;

20) «Prestador de serviços de TIC intragrupo», uma empresa que faz parte de um grupo financeiro e presta predominantemente serviços de TIC a entidades financeiras do mesmo grupo ou a entidades financeiras pertencentes ao mesmo sistema de proteção institucional, inclusive às respetivas empresas-mãe, filiais, sucursais ou outras entidades detidas ou controladas pela mesma entidade;

21) «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 incluindo equipamentos informáticos enquanto serviço e serviços de equipamento informático, o que inclui a prestação de apoio técnico através de atualizações de programas informáticos ou microprogramas pelo fornecedor de equipamentos informáticos, com exclusão dos serviços telefónicos analógicos tradicionais;

22) «Função crítica ou importante», uma função cuja perturbação comprometeria significativamente o desempenho financeiro de uma entidade financeira ou a solidez ou continuidade dos seus serviços e das suas atividades, ou a interrupção, anomalia ou falha dessa função comprometeria significativamente o contínuo cumprimento das condições e obrigações decorrentes da autorização da entidade financeira, ou das suas restantes obrigações ao abrigo do direito dos serviços financeiros aplicável;

23) «Terceiro prestador de serviços de TIC crítico», um terceiro prestador de serviços de TIC designado como crítico nos termos do artigo 31.º;

24) «Terceiro prestador de serviços de TIC estabelecido num país terceiro», um terceiro prestador de serviços de TIC que é uma pessoa coletiva estabelecida num país terceiro que celebrou um acordo contratual com uma entidade financeira para a prestação de serviços de TIC;

25) «Filial», uma empresa filial na aceção do artigo 2.º, ponto 10, e do artigo 22.º da Diretiva 2013/34/UE;

26) «Grupo», um grupo na aceção do artigo 2.º, ponto 11, da Diretiva 2013/34/UE;

27) «Empresa-mãe», uma empresa-mãe na aceção do artigo 2.º, ponto 9, e do artigo 22.º da Diretiva 2013/34/UE;

28) «Subcontratante de TIC estabelecido num país terceiro», um subcontratante de TIC que é uma pessoa coletiva estabelecida num país terceiro, e que celebrou um acordo contratual ou com um terceiro prestador de serviços de TIC, ou com um terceiro prestador de serviços de TIC estabelecido num país terceiro;

29) «Risco de concentração no domínio das TIC», a exposição a um ou mais terceiros prestadores de serviços de TIC críticos que cria um nível de dependência desses prestadores de tal modo que a indisponibilidade, uma avaria ou outro tipo de insuficiência destes últimos pode pôr em perigo a capacidade de uma entidade financeira para desempenhar funções críticas ou importantes, ou provocar outros tipos de efeitos negativos para essa entidade, incluindo perdas consideráveis, ou ainda pôr em perigo a estabilidade financeira da União no seu todo;

30) «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 Parlamento Europeu e do Conselho ([31]), 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 e das disposições pertinentes do regulamento relativo aos mercados de criptoativos ou as pessoas equiparadas que administram efetivamente a entidade ou desempenham funções fundamentais em conformidade com o direito nacional ou da União pertinente;

31) «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 ([32]);

32) «Instituição isenta nos termos da Diretiva 2013/36/UE», uma entidade referida no artigo 2.º, n.º 5, pontos 4 a 23, da Diretiva 2013/36/UE;

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

34) «Empresa de investimento de 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 do Parlamento Europeu e do Conselho ([33]);

35) «Instituição de pagamento», uma instituição de pagamento na aceção do artigo 4.º, ponto 4, da Diretiva (UE) 2015/2366;

36) «Instituição de pagamento isenta nos termos da Diretiva (UE) 2015/2366», uma instituição de pagamento isenta nos termos do artigo 32.º, n.º 1, da Diretiva (UE) 2015/2366;

37) «Prestador de serviços de informação sobre contas», um prestador de serviços de informação sobre contas na aceção do artigo 33.º, n.º 1, da Diretiva (UE) 2015/2366;

38) «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;

39) «Instituição de moeda eletrónica isenta nos termos da Diretiva 2009/110/CE», uma instituição de moeda eletrónica que beneficia de uma isenção nos termos do artigo 9.º, n.º 1, da Diretiva 2009/110/CE;

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

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

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

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

44) «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;

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

46) «Prestador de serviços de comunicação de dados», um prestador de serviços de comunicação de dados na aceção do Regulamento (UE) n.º 600/2014, tal como referido no artigo 2.º, n.º 1, pontos 34 a 36;

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

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

([31]) Diretiva 2009/65/CE do Parlamento Europeu e do Conselho, de 13 de julho de 2009, que coordena as disposições legislativas, regulamentares e administrativas respeitantes a alguns organismos de investimento coletivo em valores mobiliários (OICVM) (JO L 302 de 17.11.2009, p. 32).

([32]) 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 que altera o Regulamento (UE) n.º 648/2012 (JO L 176 de 27.6.2013, p. 1).

([33]) Regulamento (UE) 2019/2033 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, relativo aos requisitos prudenciais aplicáveis às empresas de investimento e que altera os Regulamentos (UE) n.º 1093/2010, (UE) n.º 575/2013, (UE) n.º 600/2014 e (UE) n.º 806/2014 (JO L 314 de 5.12.2019, p. 1).

49) «Mediador de seguros», um mediador de seguros na aceção do artigo 2.º, n.º 1, ponto 3, da Diretiva (UE) 2016/97 do Parlamento Europeu e do Conselho ([34]);

50) «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;

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

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

53) «Pequena instituição de realização de planos de pensões profissionais», uma instituição de realização de planos de pensões profissionais que gere planos de pensões que, no seu conjunto, têm menos de 100 membros;

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

55) «Prestador de serviços de criptoativos», um prestador de serviços de criptoativos na aceção das disposições pertinentes do regulamento relativo aos mercados de criptoativos;

56) «Emitente de criptofichas (tokens) referenciadas a ativos», um emitente de criptofichas (tokens) referenciadas a ativos na aceção das disposições pertinentes do regulamento relativo aos mercados de criptoativos;

57) «Administrador de índices de referência críticos», um administrador de «índices de referência críticos» na aceção do artigo 3, n.º 1, ponto 25, do Regulamento (UE) 2016/1011;

58) «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 do Parlamento Europeu e do Conselho ([35]);

59) «Repositório de titularizações», um repositório de titularizações na aceção do artigo 2.º, ponto 23, do Regulamento (UE) 2017/2402 do Parlamento Europeu e do Conselho ([36]);

60) «Microempresa», uma entidade financeira que não é uma plataforma de negociação, uma contraparte central, um repositório de transações ou uma central de valores mobiliários que emprega menos de 10 pessoas e cujo volume de negócios anual e/ou balanço total anual não excede 2 milhões de EUR;

61) «Autoridade fiscalizadora principal», a Autoridade Europeia de Supervisão nomeada nos termos do artigo 31.º, n.º 1, alínea b), do presente regulamento;

62) «Comité Conjunto», o comité a que se refere o artigo 54.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010;

63) «Pequena empresa», uma entidade financeira que emprega 10 ou mais pessoas, mas menos de 50 pessoas e cujo volume de negócios anual e/ou balanço total anual excede 2 milhões de EUR, mas não excede 10 milhões de EUR;

64) «Média empresa», uma entidade financeira que não é uma pequena empresa e que emprega menos de 250 pessoas e cujo volume de negócios anual não excede 50 milhões de EUR e/ou o balanço anual não excede 43 milhões de EUR;

65) «Autoridade pública», qualquer entidade pública ou da administração pública, incluindo os bancos centrais nacionais.

([34]) Diretiva (UE) 2016/97 do Parlamento Europeu e do Conselho, de 20 de janeiro de 2016, sobre a distribuição de seguros (JO L 26 de 2.2.2016, p. 19).

([35]) Regulamento (UE) 2020/1503 do Parlamento Europeu e do Conselho, de 7 de outubro de 2020, relativo aos prestadores europeus de serviços de financiamento colaborativo às entidades, e que altera o Regulamento (UE) 2017/1129 e a Diretiva (UE) 2019/1937 (JO L 347 de 20.10.2020, p. 1).

([36]) Regulamento (UE) 2017/2402 do Parlamento Europeu e do Conselho, de 12 de dezembro de 2017, que estabelece um regime geral para a titularização e cria um regime específico para a titularização simples, transparente e padronizada, e que altera as Diretivas 2009/65/CE, 2009/138/CE e 2011/61/UE e os Regulamentos (CE) n.º 1060/2009 e (UE) n.º 648/2012 (JO L 347 de 28.12.2017, p. 35).

Artigo 4.º

Princípio da proporcionalidade

1. As entidades financeiras aplicam as regras estabelecidas no capítulo II em conformidade com o princípio da proporcionalidade, tendo em conta a respetiva dimensão e o seu perfil de risco global, a natureza, a escala e a complexidade dos seus serviços, atividades e operações.

2. Além disso, a aplicação pelas entidades financeiras dos capítulos III, IV e V, secção I, é proporcional à sua dimensão e perfil de risco global, bem como à natureza, escala e complexidade dos seus serviços, atividades e operações, tal como especificamente previsto nas regras pertinentes desses capítulos.

3. As autoridades competentes têm em conta a aplicação do princípio da proporcionalidade pelas entidades financeiras ao analisarem a coerência do quadro de gestão do risco associado às TIC com base nos relatórios apresentados a pedido das autoridades competentes nos termos do artigo 6.º, n.º 5, e do artigo 16.º, n.º 2.

CAPÍTULO II

Gestão do risco associado às TIC

Secção I

Artigo 5.º

Governação e organização

1. As entidades financeiras implantam um quadro de governação interna e de controlo que garanta uma gestão eficaz e prudente do risco associado às TIC, em consonância com o artigo 6.º, n.º 4, a fim de 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 associado às TIC a que se refere o artigo 6.º, n.º 1.

Para efeitos do primeiro parágrafo, o órgão de administração:

a) Assume a responsabilidade final pela gestão do risco associado às TIC da entidade financeira;

b) Aplica políticas que visem a manutenção de elevados níveis de disponibilidade, autenticidade, integridade e confidencialidade dos dados;

c) Determina competências e responsabilidades claras para todas as funções relacionadas com as TIC e estabelece mecanismos adequados de governação para assegurar que essas funções comuniquem, cooperem e se coordenem de forma eficaz e atempada entre essas funções;

d) Assume a responsabilidade global pela definição e aprovação da estratégia de resiliência operacional digital a que se refere o artigo 6.º, n.º 8, incluindo a determinação do nível adequado de tolerância ao risco associado às TIC da entidade financeira, a que se refere o artigo 6.º, n.º 8, alínea b);

e) Aprova, fiscaliza e reavalia periodicamente a aplicação da política de continuidade das atividades no domínio das TIC da entidade financeira e dos planos de resposta e recuperação em matéria de TIC, referidos, respetivamente, no artigo 11.º, n.ºs 1, e 3, que podem ser adotados como uma política dedicada específica que faz parte integrante da política global de continuidade das atividades e do plano de resposta e recuperação da entidade financeira;

f) Aprova e reavalia periodicamente os planos de auditoria interna das TIC da entidade financeira, as auditorias das TIC e as alterações significativas aos mesmos;

g) Atribui e reavalia periodicamente o orçamento adequado para suprir as necessidades da entidade financeira em matéria de resiliência operacional digital a respeito de todos os tipos de recursos, incluindo programas pertinentes de sensibilização para a segurança das TIC e a formação em matéria de resiliência operacional digital, a que se refere o artigo 13.º, n.º 6, e competências no domínio das TIC para todos os funcionários;

h) Aprova e reavalia periodicamente a política da entidade financeira em matéria de acordos relativos à utilização de serviços de TIC prestados por terceiros;

i) Cria canais de comunicação a nível institucional que lhe permitam ser devidamente informado do seguinte:

   i) acordos celebrados para a utilização de serviços de TIC prestados por terceiros,

   ii) quaisquer alterações significativas previstas relativas aos terceiros prestadores de serviços de TIC,

   iii) potencial impacto de tais alterações em funções críticas ou importantes objeto dos referidos acordos, incluindo um resumo da análise de risco para avaliar o impacto dessas alterações, e, pelo menos dos incidentes de caráter severo relacionados com as TIC e do respetivo impacto, bem como das medidas de resposta, de recuperação e corretivas.

3. As entidades financeiras, salvo as microempresas, criam um cargo para monitorizar os acordos celebrados com terceiros prestadores de serviços de TIC relativos à utilização de serviços de TIC ou designam um membro da direção de topo incumbido de fiscalizar a exposição ao risco conexo e a documentação pertinente.

4. Os membros do órgão de administração da entidade financeira atualizam ativamente os seus conhecimentos e competências para poderem compreender e avaliar o risco associado às TIC e o respetivo impacto no funcionamento da entidade financeira, inclusive frequentando regularmente formações específicas, adequadas ao risco associado às TIC que são chamados a gerir.

Secção II

Artigo 6.º

Quadro de gestão do risco associado às TIC

1. As entidades financeiras dispõem de um quadro de gestão do risco associado às TIC sólido, abrangente e bem documentado, que faz parte do seu sistema global de gestão do risco, e que lhes permite 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 inclui, pelo menos, as estratégias, políticas, procedimentos, protocolos e ferramentas de TIC que sejam necessários para proteger devida e adequadamente todos os ativos de informação e de TIC, designadamente programas informáticos, equipamentos informáticos e servidores, bem como todos os componentes físicos e infraestruturas pertinentes, como instalações físicas, centros de dados e áreas consideradas sensíveis, por forma a assegurar que todos os ativos de informação ou de TIC estão devidamente protegidos contra riscos, nomeadamente no que diz respeito a danos e ao acesso ou utilização não autorizados.

3. Em consonância com o respetivo quadro de gestão do risco associado às TIC, as entidades financeiras minimizam o impacto do risco associado às TIC implementando as estratégias, políticas, procedimentos, protocolos e ferramentas adequados. Fornecem igualmente às autoridades competentes, a pedido destes, informações completas e atualizadas sobre o risco associado às TIC e sobre o respetivo quadro de gestão do risco associado às TIC.

4. As entidades financeiras que não sejam microempresas atribuem a responsabilidade pela gestão e supervisão do risco associado às TIC a uma função de controlo e asseguram um nível adequado de independência dessa função de controlo, a fim de evitar conflitos de interesses. As entidades financeiras asseguram a segregação e independência adequadas entre as funções de gestão, de controlo e de auditoria interna do risco associado às TIC, de acordo com o modelo das três linhas de defesa ou com um modelo interno de controlo e gestão do risco.

5. O quadro de gestão do risco associado às TIC a que se refere o n.º 1 é documentado e revisto pelo menos uma vez por ano, ou periodicamente, no caso das microempresas, bem como quando ocorrerem incidentes de caráter severo 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 é continuamente aperfeiçoado com base nas lições retiradas da implementação e monitorização. É apresentado à autoridade competente, a pedido desta, um relatório de análise do quadro de gestão do risco associado às TIC.

6. O quadro de gestão do risco associado às TIC das entidades financeiras, que não sejam microempresas, é periodicamente sujeito a auditorias internas efetuadas por auditores em conformidade com o plano de auditoria das entidades financeiras. Estes auditores dispõem de conhecimentos gerais, competências e conhecimentos especializados suficientes sobre o risco associado às TIC, bem como de independência adequada. A frequência e a ênfase das auditorias às TIC são proporcionais ao risco associado às TIC da entidade financeira.

7. Com base nas conclusões da análise da auditoria interna, as entidades financeiras estabelecem um processo formal de acompanhamento, incluindo regras para a verificação e correção atempadas dos resultados críticos das auditorias às TIC.

8. O quadro de gestão do risco associado às TIC inclui uma estratégia de resiliência operacional digital que defina as modalidades da sua implementação. Para esse fim, a estratégia de resiliência operacional digital inclui os métodos para dar resposta ao risco associado às TIC e alcançar os objetivos específicos em matéria de TIC, devendo para tal:

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

b) Estabelecer o nível de tolerância ao risco 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, incluindo principais indicadores de desempenho e principais métricas de risco;

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

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

f) Atestar a atual situação de resiliência operacional digital com base no número de incidentes de caráter severo relacionados com as TIC comunicados e a eficácia das medidas preventivas;

g) Realizar testes à resiliência operacional digital, nos termos do capítulo IV do presente regulamento;

h) Delinear uma estratégia de notificação em caso de incidentes relacionados com as TIC, cuja divulgação seja obrigatória nos termos do artigo 14.º.

9. As entidades financeiras podem, no contexto da estratégia de resiliência operacional digital a que se refere o n.º 8, definir uma estratégia holística com múltiplos fornecedores no domínio das TIC, ao nível do grupo ou da entidade, mostrando as principais dependências de terceiros prestadores de serviços de TIC e explicando a lógica subjacente à contratação de vários terceiros prestadores de serviços de TIC.

10. As entidades financeiras podem, nos termos do direito setorial da União e nacional, subcontratar as tarefas de verificação do cumprimento dos requisitos de gestão do risco associado às TIC a empresas pertencentes ao grupo ou a empresas externas. Nesse caso, a entidade financeira continua a ser plenamente responsável pela verificação do cumprimento dos requisitos de gestão do risco associado às TIC.

Artigo 7.º

Sistemas, protocolos e ferramentas de TIC

A fim de abordar e gerir o risco associado às TIC, as entidades financeiras utilizam e mantêm atualizados sistemas, protocolos e ferramentas de TIC que sejam:

a) Adequados à dimensão das operações que apoiam o desenvolvimento das suas atividades, em conformidade com o princípio da proporcionalidade a que se refere o artigo 4.º;

b) Fiáveis;

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

d) Resilientes do ponto de vista tecnológico para responder adequadamente a necessidades adicionais de tratamento de informações em situações de grande tensão no mercado ou noutras circunstâncias adversas.

Artigo 8.º

Identificação

1. Para efeitos do quadro de gestão do risco associado às TIC referido no artigo 6.º, n.º 1, as entidades financeiras identificam, classificam e documentam adequadamente todas as funções operacionais apoiadas pelas TIC, os papéis e as responsabilidades, os ativos de informação e os ativos de TIC que apoiam essas funções, bem como os respetivos papéis e dependências em relação com o risco associado às TIC. As entidades financeiras reveem na medida do necessário, e pelo menos uma vez por ano, a adequação desta classificação e de toda a documentação pertinente.

2. As entidades financeiras identificam de forma contínua todas as fontes de risco associado às TIC, em especial a exposição ao risco face a outras entidades financeiras e decorrente de outras entidades financeiras, e avaliam as ciberameaças e as vulnerabilidades das TIC pertinentes para as suas funções operacionais apoiadas pelas TIC, os seus ativos de informação e ativos de TIC. As entidades financeiras reveem periodicamente e pelo menos uma vez por ano os cenários de risco suscetíveis de as afetar.

3. As entidades financeiras, que não sejam microempresas, efetuam uma avaliação do risco aquando de qualquer grande alteração na infraestrutura dos sistemas de rede e informação, nos processos ou nos procedimentos que afetem as suas funções operacionais apoiadas pelas TIC, nos ativos de informação ou nos ativos de TIC.

4. As entidades financeiras identificam todos os ativos de informação e os ativos de TIC, nomeadamente os localizados à distância, os recursos de rede e os equipamentos informáticos, e fazem um levantamento dos considerados críticos. Descrevem igualmente a configuração dos ativos de informação e dos ativos de TIC e das ligações e interdependências entre os diferentes ativos de informação e ativos de TIC.

5. As entidades financeiras identificam e documentam todos os processos que dependem de terceiros prestadores de serviços de TIC e identificam as interconexões com os terceiros prestadores de serviços de TIC que prestam serviços de apoio a funções críticas ou importantes.

6. Para efeitos dos n.os 1, 4 e 5, as entidades financeiras elaboram os inventários relevantes e atualizam-nos periodicamente e sempre que ocorra qualquer alteração importante a que se refere o n.º 3.

7. As entidades financeiras que não sejam microempresas realizam periodicamente e pelo menos uma vez por ano uma avaliação do risco associado às TIC específica em todos os sistemas de TIC legados, e, em todo o caso, antes e depois de conectarem tecnologias, aplicações ou sistemas.

Artigo 9.º

Proteção e prevenção

1. No intuito de proteger adequadamente os sistemas TIC e de organizar medidas de resposta, as entidades financeiras monitorizam e controlam continuamente a segurança e o funcionamento dos sistemas e das ferramentas de TIC e minimizam o impacto de risco associado às TIC nos sistemas de TIC através da implementação de ferramentas, políticas e procedimentos de segurança adequados no domínio das TIC.

2. As entidades financeiras concebem, adquirem e executam políticas, procedimentos, protocolos e ferramentas de segurança no domínio das TIC que visem assegurar a resiliência, a continuidade e a disponibilidade dos sistemas de TIC, em especial os sistemas que apoiem funções críticas ou importantes e manter elevados níveis de disponibilidade, autenticidade, integridade e confidencialidade dos dados conservados, em uso ou em trânsito.

3. A fim de alcançar os objetivos referidos no n.º 2, as entidades financeiras recorrem a soluções e processos de TIC adequados nos termos do artigo 4.º. Essas soluções e processos de TIC:

a) Asseguram a segurança dos meios de transferência de dados;

b) Minimizam o risco de corrupção ou a perda de dados, o acesso não autorizado e falhas técnicas suscetíveis de prejudicar a atividade operacional;

c) Evitam a falta de disponibilidade, as violações da autenticidade e da integridade, a quebra da confidencialidade e a perda de dados;

d) Asseguram que os dados estejam protegidos contra riscos decorrentes da gestão de dados, incluindo má administração, riscos relacionados com o tratamento e erros humanos.

4. Para efeitos do quadro de gestão do risco associado às TIC referido no artigo 6.º, n.º 1, as entidades financeiras:

a) Desenvolvem e documentam uma política de segurança das informações que defina regras para proteger a disponibilidade, autenticidade, integridade e confidencialidade dos dados, dos ativos de informação, e dos ativos de TIC, incluindo os dos seus clientes, se for caso disso;

b) De acordo com uma abordagem baseada no risco, estabelecem uma estrutura de gestão sólida das redes e infraestruturas utilizando técnicas, métodos e protocolos adequados, que podem incluir a implementação de mecanismos automatizados para isolar os ativos de informação afetados em caso de ciberataque;

c) Executam políticas que limitem o acesso físico ou lógico aos ativos de informação e aos ativos de TIC àquilo que é estritamente necessário para funções e atividades legítimas e aprovadas e, para o efeito, estabelecem um conjunto de políticas, procedimentos e controlos centrado nos direitos de acesso e que asseguram a boa administração dos mesmos;

d) Executam políticas e protocolos que garantam mecanismos de autenticação robustos, com base nas normas pertinentes e em sistemas de controlo dedicados e medidas de proteção das chaves criptográficas por meio das quais os dados são encriptados em função dos resultados de processos aprovados de classificação dos dados e de avaliação do risco associado às TIC;

e) Executam políticas, procedimentos e controlos documentados relativos à gestão das alterações das TIC, nomeadamente mudanças de programas informáticos, equipamentos informáticos, componentes de microprogramas, sistemas ou parâmetros de segurança, assentes 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) Dispõem de estratégias documentadas adequadas e abrangentes para correções e atualizações.

Para efeitos do primeiro parágrafo, alínea b), as entidades financeiras configuram a infraestrutura de conexão das redes por forma a que essas conexões possam ser instantaneamente cortadas ou segmentadas, com vista a minimizar e evitar o contágio, em especial em processos financeiros interligados.

Para efeitos do primeiro parágrafo, alínea e), o processo de gestão de alteração das TIC é aprovado pelas linhas hierárquicas adequadas e dispõe de protocolos específicos.

Artigo 10.º

Deteção

1. As entidades financeiras dispõem de mecanismos que detetem rapidamente atividades anómalas nos termos do artigo 17.º, nomeadamente questões relacionadas com o desempenho das redes e incidentes relacionados com as TIC, identificando as potenciais falhas pontuais significativas.

Todos os mecanismos de deteção referidos no primeiro parágrafo são periodicamente testados nos termos do artigo 25.º.

2. Os mecanismos de deteção referidos no n.º 1 permitem que o controlo se faça em etapas múltiplas, definem limiares de alerta e critérios que desencadeiem e iniciem processos de resposta a incidentes relacionados com as TIC, incluindo mecanismos automáticos de alerta do pessoal competente responsável pela resposta aos incidentes relacionados com as TIC.

3. As entidades financeiras canalizam recursos e capacidades suficientes para monitorizar a atividade dos utilizadores, a ocorrência de anomalias e incidentes relacionados com as TIC, em especial ciberataques.

4. Os prestadores de serviços de comunicação de dados dispõem também de sistemas que permitam verificar de forma eficaz as comunicações de transações, identificar as omissões e os erros manifestos e solicitar a retransmissão dessas comunicações.

Artigo 11.º

Resposta e recuperação

1. Para efeitos do quadro de gestão do risco associado às TIC referido no artigo 6.º, n.º 1, e com base nos requisitos de identificação definidos no artigo 8.º, as entidades financeiras implementam uma política abrangente para assegurar a continuidade das atividades, que pode ser aprovada enquanto política distinta específica e ser parte integrante da política global de continuidade das atividades da entidade financeira.

2. As entidades financeiras aplicam a política de continuidade das atividades no domínio das TIC através de medidas, planos, procedimentos e mecanismos dedicados, adequados e documentados que visem:

a) Assegurar a continuidade das funções críticas ou importantes da entidade financeira;

b) Dar uma resposta rápida, adequada e eficaz e solucionar todos os incidentes relacionados com as TIC, por forma a limitar os danos e a dar prioridade ao relançamento das atividades e às ações de recuperação;

c) 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 relacionado com as TIC, evitando assim outros danos, bem como uma resposta adequada e os procedimentos de recuperação estabelecidos nos termos do artigo 12.º;

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

e) 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 nos termos do artigo 14.º, bem como a sua comunicação às autoridades competentes nos termos do artigo 19.º.

3. Para efeitos do quadro de gestão do risco associado às TIC referido no artigo 6.º, n.º 1, as entidades financeiras executam planos de resposta e recuperação em matéria de TIC que, no caso das entidades financeiras que não sejam microempresas, são sujeitos a auditorias internas independentes.

4. As entidades financeiras dispõem, mantêm e testam periodicamente planos de continuidade das atividades no domínio das TIC adequados, designadamente em relação a funções críticas ou importantes externalizadas ou subcontratadas através de acordos com terceiros prestadores de serviços de TIC.

5. No âmbito da política global de continuidade das atividades, as entidades financeiras realizam uma análise do impacto na atividade (BIA, do inglês *business impact analysis*) das suas exposições a perturbações graves. No âmbito da BIA, as entidades financeiras avaliam o impacto potencial de perturbações graves das atividades em função de critérios quantitativos e qualitativos, utilizando dados internos e externos e análises de cenários, conforme adequado. A BIA atende à importância crítica das funções operacionais identificadas e mapeadas, dos processos de apoio, das dependências de terceiros e dos ativos de informação, bem como às suas interdependências. As entidades financeiras asseguram que os ativos e serviços de TIC são concebidos e utilizados em plena articulação com a BIA, em especial no que diz respeito a assegurar adequadamente a redundância de todos os componentes críticos.

6. Para efeitos da gestão abrangente do risco associado às TIC, as entidades financeiras:

a) Testam os planos de continuidade das atividades no domínio das TIC e os planos de resposta e recuperação em matéria de TIC em relação a sistemas de TIC que apoiem todas as funções, pelo menos uma vez por ano, bem como no caso de alterações substanciais de sistemas de TIC que apoiem funções críticas ou importantes;

b) Testam os planos de comunicação de crises estabelecidos nos termos do artigo 14.º.

Para efeitos do primeiro parágrafo, alínea a), as entidades financeiras que não sejam microempresas incluem nos planos de testagem cenários de ciberataques e de passagem entre a infraestrutura primária de TIC e a capacidade redundante, cópias de segurança e equipamentos redundantes necessários ao cumprimento das obrigações definidas no artigo 12.º.

As entidades financeiras reveem periodicamente a sua política de continuidade das atividades no domínio das TIC e os planos de resposta e recuperação em matéria de TIC tendo em conta os resultados dos testes realizados nos termos do primeiro parágrafo e as recomendações decorrentes das auditorias ou das avaliações de supervisão.

7. As entidades financeiras que não sejam microempresas têm uma função de gestão de crises que, em caso de ativação dos seus planos de continuidade das atividades no domínio das TIC ou dos seus planos de resposta e recuperação em matéria de TIC, preveja, nomeadamente, procedimentos claros para gerir as comunicações internas e externas em caso de crise nos termos do artigo 14.º.

8. As entidades financeiras mantêm registos prontamente acessíveis das atividades antes e durante a ocorrência de perturbações aquando da ativação dos seus planos de continuidade das atividades no domínio das TIC ou dos seus planos de resposta e recuperação em matéria de TIC.

9. As centrais de valores mobiliários fornecem às autoridades competentes cópias dos resultados dos testes de continuidade das atividades no domínio das TIC ou de exercícios semelhantes.

10. As entidades financeiras que não sejam microempresas comunicam às autoridades competentes, a pedido destas, uma estimativa dos custos e perdas anuais agregados causados por incidentes de caráter severo relacionados com as TIC.

11. Nos termos do artigo 16.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, as AES, através do Comité Conjunto, elaboram, até 17 de julho de 2024, orientações comuns para a estimativa dos custos e perdas anuais agregados a que se refere o n.º 10.

Artigo 12.º

Políticas e procedimentos de salvaguarda e procedimentos e métodos de restauração e recuperação

1. A fim de assegurar a restauração dos sistemas de TIC e de dados limitando ao mínimo o tempo de indisponibilidade, as perturbações e as perdas, as entidades financeiras desenvolvem e documentam, para efeitos do seu quadro de gestão do risco associado às TIC:

a) Políticas e procedimentos de salvaguarda que especifiquem o âmbito dos dados abrangidos e a frequência mínima com que são geradas as cópias de segurança, em função da natureza crítica das informações ou do nível de confidencialidade dos dados;

b) Procedimentos e métodos de restauração e recuperação.

2. As entidades financeiras criam sistemas de salvaguarda que possam ser ativados de acordo com as políticas e procedimentos de salvaguarda, bem como procedimentos e métodos de restauração e recuperação. A ativação dos sistemas de salvaguarda não pode pôr em perigo a segurança dos sistemas de rede e informação nem a disponibilidade, autenticidade, integridade ou confidencialidade dos dados. São realizados periodicamente testes dos procedimentos de salvaguarda e dos procedimentos e métodos de restauração e recuperação.

3. Quando restauram dados das cópias de segurança utilizando sistemas próprios, as entidades financeiras utilizam sistemas de TIC que estejam física e logicamente separados do sistema de TIC de origem. Os sistemas de TIC estão devidamente protegidos contra todo o acesso não autorizado ou corrupção ao nível das TIC e permitem a restauração atempada dos serviços utilizando dados e cópias de salvaguarda do sistema, conforme necessário.

Em relação às contrapartes centrais, os planos de recuperação permitem 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.

Os prestadores de serviços de comunicação de dados mantêm além disso recursos adequados e dispõem de equipamentos de salvaguarda e de restauração, a fim de poderem oferecer e manter os seus serviços em qualquer momento.

4. As entidades financeiras que não sejam microempresas mantêm capacidades de TIC redundantes equipadas com recursos, capacidade e funções suficientes e adequados para acautelar as necessidades operacionais. As microempresas avaliam a necessidade de manter essas capacidades de TIC redundantes com base no seu perfil de risco.

5. As Centrais de valores mobiliários mantêm pelo menos um local de tratamento de dados secundário, dotado de recursos, capacidades, funções e efetivos adequados para acautelar as necessidades operacionais.

O local de tratamento de dados secundário deve:

a) Estar localizado a uma distância geográfica do local de tratamento de dados principal que lhe garanta um perfil de risco distinto e evita que seja afetado pela ocorrência que afetou o local principal;

b) Poder assegurar a continuidade das funções críticas ou importantes de forma idêntica ao local principal ou fornecer o nível de serviços necessário para assegurar que a entidade financeira realiza as suas operações críticas no âmbito dos objetivos de recuperação;

c) Estar imediatamente 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 tenha ficado indisponível.

6. Ao determinar o tempo de recuperação e os objetivos concretos de recuperação para cada função, as entidades financeiras têm em conta se a função é crítica ou importante, bem como o potencial impacto global na eficiência do mercado. Os referidos objetivos temporais garantem 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 realizam as verificações necessárias, incluindo verificações múltiplas, e reconciliações de dados, por forma a assegurar a manutenção do mais alto nível de integridade dos dados. Estas verificações também são realizadas aquando da reconstrução de dados de partes interessadas externas, por forma a assegurar a coerência de todos os dados nos diferentes sistemas.

Artigo 13.º

Aprendizagem e evolução

1. As entidades financeiras dispõem de capacidades e de pessoal para recolherem informações sobre as vulnerabilidades e as ciberameaças, os incidentes relacionados com as TIC, em especial ciberataques, e analisarem os potenciais impactos dos mesmos na sua resiliência operacional digital.

2. As entidades financeiras realizam avaliações pós-incidentes relacionados com as TIC após a ocorrência de um incidente de caráter severo relacionado com as TIC que perturbe as suas atividades principais, analisando as causas das perturbações e identificando as melhorias necessárias a nível do funcionamento das TIC ou da política de continuidade das atividades no domínio das TIC a que se refere o artigo 11.º.

As entidades financeiras que não sejam microempresas comunicam, a pedido, às autoridades competentes as alterações introduzidas na sequência de avaliações pós-incidentes relacionados com as TIC a que se refere o primeiro parágrafo.

As avaliações pós-incidentes relacionados com as TIC a que se refere o primeiro parágrafo averiguam 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, quando tal for considerado adequado;

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 de resiliência operacional digital realizados nos termos dos artigos 26.º e 27.º e a partir de incidentes reais relacionados com as TIC, em especial de ciberataques, a par dos desafios enfrentados aquando da ativação dos planos de continuidade das atividades no domínio das TIC e dos planos de resposta e recuperação em matéria de TIC, juntamente com as informações relevantes trocadas com as contrapartes e avaliadas durante as avaliações de supervisão, são devidamente incorporados de forma contínua no processo de avaliação do risco associado às TIC. Esses resultados constituem a base para exames adequados dos componentes relevantes do quadro de gestão do risco associado às TIC a que se refere o artigo 6.º, n.º 1.

4. As entidades financeiras monitorizam a eficácia da execução da sua estratégia de resiliência operacional digital definida no artigo 6.º, n.º 8. Fazem também um levantamento da evolução do risco associado às TIC ao longo do tempo, analisam 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, em particular no que diz respeito às funções críticas ou importantes, e melhoram a cibercomunidade e o grau de preparação da entidade financeira.

5. Os quadros superiores responsáveis pelas TIC comunicam, pelo menos uma vez por ano, informações ao órgão de gestão sobre os resultados a que se refere o n.º 3 e fazem recomendações.

6. As entidades financeiras desenvolvem programas de sensibilização para a segurança das TIC e a formação em matéria de resiliência operacional digital como módulos obrigatórios nos planos de formação do seu pessoal. Esses programas e formação são aplicáveis a todos os trabalhadores e aos membros da direção de topo e têm um nível de complexidade proporcional às suas funções. Se for caso disso, as entidades financeiras incluem também terceiros prestadores de serviços de TIC nos seus programas de formação pertinentes, nos termos do artigo 30.º, n.º 2, alínea i).

7. As entidades financeiras que não sejam microempresas monitorizam continuamente os desenvolvimentos tecnológicos mais importantes, também com vista a compreender o possível impacto da implantação dessas novas tecnologias nos requisitos de segurança no domínio das TIC e na resiliência operacional digital. Mantêm-se a par dos mais recentes processos de gestão do risco associado às TIC, a fim de combater eficazmente os ciberataques nas suas formas atuais ou futuras.

Artigo 14.º

Comunicação

1. Para efeitos do quadro de gestão do risco associado às TIC a que se refere o artigo 6.º, n.º 1, as entidades financeiras dispõem de planos de comunicação de crises que permitam divulgar de forma responsável, pelo menos, os incidentes de caráter severo relacionados com as TIC ou as vulnerabilidades aos clientes e às contrapartes, bem como ao público, se for caso disso.

2. Para efeitos do quadro de gestão do risco associado às TIC, as entidades financeiras aplicam políticas de comunicação destinadas ao seu pessoal interno e às partes interessadas externas. As políticas de comunicação destinadas ao pessoal têm em conta a necessidade de diferenciar entre o pessoal envolvido na gestão do risco associado às TIC, em especial, o pessoal responsável pela resposta e recuperação, e o pessoal que precisa de ser informado.

3. Pelo menos uma pessoa na entidade financeira é responsável pela execução da estratégia de comunicação em caso de incidentes relacionados com as TIC e desempenha essa função perante o público e os média para o efeito.

Artigo 15.º

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

As AES desenvolvem, através do Comité Conjunto, em consulta com a Agência da União Europeia para a Cibersegurança (ENISA), projetos de normas técnicas de regulamentação comuns a fim de:

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 9.º, n.º 2, com vista a acautelar a segurança das redes, prever salvaguardas adequadas contra as intrusões e a utilização abusiva dos dados, preservar a disponibilidade, autenticidade, integridade e confidencialidade dos dados, nomeadamente por via de técnicas criptográficas, e garantir uma transmissão fiável e rápida dos dados sem grandes interrupções, e sem demoras injustificadas;

b) Desenvolver mais pormenorizadamente os componentes de controlo da gestão dos direitos de acesso a que se refere o artigo 9.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 ao risco associado às TIC através dos indicadores adequados, nomeadamente os padrões de utilização das redes, as horas de acesso, a atividade informática e os dispositivos desconhecidos;

c) Desenvolver mais pormenorizadamente os mecanismos especificados no artigo 10.º, n.º 1, que permitem a deteção rápida de atividades anómalas, bem como os critérios estabelecidos no artigo 10.º, n.º 2, que desencadeiam processos de deteção e resposta a incidentes relacionados com as TIC;

d) Especificar mais pormenorizadamente os componentes da política de continuidade das atividades no domínio das TIC a que se refere o artigo 11.º, n.º 1;

e) Especificar mais pormenorizadamente os testes dos planos de continuidade das atividades no domínio das TIC a que se refere o artigo 11.º, n.º 6, por forma a assegurar que os testes têm devidamente em conta cenários em que a qualidade do desempenho de uma função crítica ou importante atinge níveis inaceitáveis ou falha, e considerar devidamente o potencial impacto de uma insolvência, ou de outras falhas, de qualquer terceiro prestador de serviços de TIC relevante e, quando pertinente, os riscos políticos nas respetivas jurisdições desses prestadores;

f) Especificar mais pormenorizadamente os componentes dos planos de resposta e recuperação em matéria de TIC a que se refere o artigo 11.º, n.º 3;

g) Especificar mais pormenorizadamente o conteúdo e o formato do relatório de análise do quadro de gestão do risco associado às TIC a que se refere o artigo 6.º, n.º 5;

Ao elaborar esses projetos de normas técnicas de regulamentação, as AES têm em conta a dimensão e o perfil de risco global da entidade financeira, bem como a natureza, a escala e a complexidade dos seus serviços, atividades e operações, tendo devidamente em conta qualquer característica específica decorrente da natureza distinta das atividades nos diferentes setores dos serviços financeiros.

As AES apresentam esses projetos de normas técnicas de regulamentação à Comissão até 17 de janeiro de 2024.

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 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 16.º

Quadro simplificado de gestão do risco associado às TIC

1. Os artigos 5.º a 15.° do presente regulamento não se aplicam às empresas de investimento de pequena dimensão e não interligadas, nem às instituições de pagamento isentas nos termos da Diretiva (UE) 2015/2366; às instituições isentas nos termos da Diretiva 2013/36/UE relativamente às quais os Estados-Membros tenham decidido não aplicar a opção a que se refere o artigo 2.º, n.º 4, do presente regulamento; às instituições de moeda eletrónica isentas nos termos da Diretiva 2009/110/CE; nem às pequenas instituições de realização de planos de pensões profissionais.

Sem prejuízo do disposto no primeiro parágrafo, as entidades enumeradas no primeiro parágrafo:

a) Estabelecem e mantêm um quadro sólido e documentado de gestão do risco associado às TIC que especifique os mecanismos e as medidas destinados a uma gestão rápida, eficiente e abrangente do risco associado às TIC, inclusive para a proteção de componentes e infraestruturas físicas pertinentes;

b) Controlam permanentemente a segurança e o funcionamento de todos os sistemas de TIC;

c) Minimizam o impacto do risco associado 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, bem como proteger adequadamente a disponibilidade, autenticidade, integridade e confidencialidade dos dados nos sistemas de rede e informação;

d) Permitem identificar e detetar rapidamente as fontes de risco associado às TIC, bem como as anomalias nos sistemas de rede e informação e tratar prontamente os incidentes relacionados com as TIC;

e) Identificam as principais dependências em relação aos terceiros prestadores de serviços de TIC;

f) Asseguram a continuidade das funções críticas ou importantes, através de planos de continuidade das atividades e de medidas de resposta e recuperação, que incluam, pelo menos, medidas de salvaguarda e de restauração;

g) Testam regularmente os planos e medidas a que se refere a alínea f), bem como a eficácia dos controlos levados a cabo nos termos das alíneas a) e c);

h) Aplicam, se for caso disso, as conclusões operacionais pertinentes resultantes dos testes a que se refere a alínea g) e da análise pós-incidente no processo de avaliação do risco associado às TIC e desenvolvem, de acordo com as necessidades e o perfil de risco associado às TIC, programas de sensibilização para a segurança das TIC e a formação em matéria de resiliência digital operacional ao pessoal e à administração.

2. O quadro de gestão do risco associado às TIC a que se refere o n.º 1, segundo parágrafo, alínea a), é documentado e revisto periodicamente e aquando da ocorrência de incidentes de caráter severo relacionados com as TIC, em conformidade com as instruções de supervisão. O quadro é continuamente aperfeiçoado com base nas lições retiradas da implementação e monitorização. Deve ser apresentado anualmente à autoridade competente, a seu pedido, um relatório de análise do quadro de gestão do risco associado às TIC.

3. As AES desenvolvem, através do Comité Conjunto, em consulta com a ENISA, projetos de normas técnicas de regulamentação comuns a fim de:

a) Especificar mais pormenorizadamente os elementos a incluir no quadro de gestão do risco associado às TIC a que se refere o n.º 1, segundo parágrafo, alínea a);

b) Especificar mais pormenorizadamente os elementos relativos aos sistemas, protocolos e ferramentas para minimizar o impacto do risco associado às TIC a que se refere o n.º 1, segundo parágrafo, alínea c), com vista a assegurar a segurança das redes, possibilitando salvaguardas adequadas contra intrusões e a utilização abusiva de dados e preservando a disponibilidade, autenticidade, integridade e confidencialidade dos dados;

c) Especificar mais pormenorizadamente os componentes dos planos de continuidade das atividades no domínio das TIC a que se refere o n.º 1, segundo parágrafo, alínea f);

d) Especificar mais pormenorizadamente as regras relativas aos testes dos planos de continuidade das atividades e assegurar a eficácia dos controlos a que se refere o n.º 1, segundo parágrafo, alínea g), e assegurar que esses testes têm devidamente em conta cenários em que a qualidade do desempenho de uma função crítica ou importante atinge níveis inaceitáveis ou falha;

e) Especificar mais pormenorizadamente o conteúdo e o formato do relatório de análise do quadro de gestão do risco associado às TIC a que se refere o n.º 2.

Ao elaborarem esses projetos de normas técnicas de regulamentação, as AES têm em conta a dimensão e o perfil de risco global da entidade financeira, bem como a natureza, a escala e a complexidade dos seus serviços, atividades e operações.

As AES apresentam esses projetos de normas técnicas de regulamentação à Comissão até 17 de janeiro de 2024.

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 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.

CAPITULO III

Gestão, classificação e comunicação de informações sobre incidentes relacionados com as TIC

Artigo 17.º

Processo de gestão de incidentes relacionados com as TIC

1. As entidades financeiras definem, estabelecem e aplicam um processo de gestão de incidentes relacionados com as TIC para detetar, gerir e notificar esses incidentes.

2. As entidades financeiras registam todos os incidentes relacionados com as TIC, bem como as ciberameaças significativas. As entidades financeiras estabelecem procedimentos e processos adequados para assegurar a monitorização, o tratamento e acompanhamento coerente e integrado dos incidentes relacionados com as TIC, por forma a assegurar que as causas profundas são identificadas, documentadas e resolvidas a fim de evitar a ocorrência desses incidentes.

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

a) Estabelece indicadores de alerta precoce;

b) Estabelece procedimentos para identificar, rastrear, registar, categorizar e classificar os incidentes relacionados com as TIC de acordo com a sua prioridade e de acordo com a gravidade e importância dos serviços afetados, em conformidade com os critérios estabelecidos no artigo 18.º, n.º 1;

c) Atribui as funções e responsabilidades que devem ser ativadas para os diferentes cenários e tipos de incidentes relacionados com as TIC;

d) Define planos de comunicação ao pessoal, às partes interessadas externas e aos média nos termos do artigo 14.º, planos de notificação aos clientes, para procedimentos de ativação dos níveis sucessivos internos, nomeadamente para tratar 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;

e) Assegura que, pelo menos, os incidentes de caráter severo relacionados com as TIC são comunicados aos membros da direção de topo pertinentes e informa o órgão de gestão de, pelo menos, os incidentes de caráter severo relacionados com as TIC, explicando o impacto, a resposta e os controlos adicionais que devem ser estabelecidos em resultado desses incidentes relacionados com as TIC;

f) Estabelece procedimentos de resposta a incidentes relacionados com as TIC para atenuar os respetivos impactos e assegura o restabelecimento dos serviços em tempo útil e de forma segura.

Artigo 18.º

Classificação dos incidentes relacionados com as TIC e das ciberameaças

1. As entidades financeiras classificam os incidentes relacionados com as TIC e determinam o respetivo impacto com base nos seguintes critérios:

a) O número e/ou a relevância dos clientes, ou contrapartes financeiras, afetados e, sempre que aplicável, a quantidade ou o número de transações afetadas pelo incidente relacionado com as TIC e se o incidente relacionado com as TIC teve algum impacto em termos de reputação;

b) A duração do incidente relacionado com as TIC, nomeadamente o tempo de indisponibilidade 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, no que diz respeito à disponibilidade, autenticidade, integridade ou confidencialidade dos dados;

e) A criticalidade dos serviços afetados, nomeadamente as transações e operações da entidade financeira;

f) O impacto económico, em especial, os custos e as perdas diretos e indiretos do incidente relacionado com as TIC, tanto em termos absolutos como em termos relativos.

2. As entidades financeiras classificam as ciberameaças como significativas com base na criticalidade dos serviços em risco, incluindo as transações e operações da entidade financeira, o número e/ou relevância dos clientes ou contrapartes financeiras visados e a distribuição geográfica das áreas em risco.

3. As AES desenvolvem, através do Comité Conjunto, e em consulta com o BCE e a ENISA, projetos de normas técnicas de regulamentação comuns a fim de especificar mais pormenorizadamente:

a) Os critérios definidos no n.º 1, nomeadamente os limiares de materialidade para determinar os incidentes de caráter severo relacionados com as TIC, ou, consoante aplicável, os incidentes de caráter severo operacionais ou de segurança relacionados com pagamentos, que estão sujeitos à notificação obrigatória de informações prevista no artigo 19.º, n.º 1;

b) Os critérios a aplicar pelas autoridades competentes com o objetivo de avaliar a relevância dos incidentes de caráter severo relacionados com as TIC, ou, consoante aplicável, os incidentes de caráter severo operacionais ou de segurança relacionados com pagamentos, às autoridades competentes pertinentes de outros Estados-Membros, bem como os pormenores dos relatórios dos incidentes de caráter severo relacionados com as TIC, ou, consoante aplicável, os incidentes de caráter severo operacionais ou de segurança relacionados com pagamentos que devem ser partilhados com outras autoridades competentes nos termos do artigo 19.º, n.ºs 6 e 7;

c) Os critérios estabelecidos no n.º 2 do presente artigo, incluindo limiares de materialidade elevados para determinar as ciberameaças significativas.

4. Aquando da elaboração dos projetos de normas técnicas de regulamentação comuns a que se refere o n.º 3 do presente artigo, as AES têm em conta os critérios estabelecidos no artigo 4.º, n.º 2, as normas internacionais, bem como as orientações e as especificações elaboradas e publicadas pela ENISA, incluindo, quando adequado, especificações para outros setores económicos. Para efeitos da aplicação dos critérios estabelecidos no artigo 4.º, n.º 2, as AES têm devidamente em conta a necessidade de as microempresas e as pequenas e médias empresas mobilizarem recursos e capacidades suficientes para assegurar uma gestão rápida dos incidentes relacionados com as TIC.

As AES apresentam esses projetos comuns de normas técnicas de regulamentação à Comissão até 17 de janeiro de 2024.

A Comissão fica habilitada a completar o presente regulamento através da adoção das normas técnicas de regulamentação a que se refere o n.º 3, 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 19.º

Comunicação dos incidentes de caráter severo relacionados com as TIC e notificação voluntária de ciberameaças significativas

1. As entidades financeiras comunicam os incidentes de caráter severo relacionados com as TIC à autoridade competente pertinente, tal como referido no artigo 46.º, nos termos do n.º 4 do presente artigo.

Caso uma entidade financeira esteja sujeita à supervisão de mais do que uma autoridade nacional competente a que se refere o artigo 46.º, os Estados-Membros designam uma única autoridade competente como entidade competente pertinente responsável pelo desempenho das funções e deveres previstos no presente artigo.

As instituições de crédito classificadas como significativas, de acordo com o artigo 6.º, n.º 4, do Regulamento (UE) n.º 1024/2013, comunicam incidentes de caráter severo relacionados com as TIC à autoridade nacional competente designada nos termos do artigo 4.º da Diretiva 2013/36/UE, que transmite imediatamente esse relatório ao BCE.

Para efeitos do primeiro parágrafo, as entidades financeiras elaboram, após recolha e análise de todas as informações relevantes, a notificação inicial e os relatórios a que se refere o n.º 4 do presente artigo, por meio dos modelos a que se refere o artigo 20.º, e apresentam-nos à autoridade competente. Caso uma impossibilidade técnica impeça a apresentação da notificação inicial por meio do modelo, as entidades financeiras notificam do facto a autoridade competente por meios alternativos.

A notificação inicial e os relatórios a que se refere o n.º 4 incluem todas as informações necessárias que permitam à autoridade competente determinar o grau de importância do incidente de caráter severo relacionado com as TIC e avaliar os possíveis impactos transfronteiriços.

Sem prejuízo da comunicação de informações nos termos do primeiro parágrafo pela entidade financeira à autoridade competente relevante, os Estados-Membros podem ainda determinar que algumas ou todas as entidades financeiras devem também transmitir a notificação inicial e cada relatório a que se refere o n.º 4 do presente artigo, por meio dos modelos a que se refere o artigo 20.º, às autoridades competentes ou às equipas de resposta a incidentes de segurança informática (CSIRT) designadas ou criadas nos termos da Diretiva (UE) 2022/2555.

2. As entidades financeiras podem, a título voluntário, notificar ciberameaças significativas à autoridade competente pertinente sempre que considerem essas ameaças relevantes para o sistema financeiro, os utilizadores ou os clientes do serviço. A autoridade competente pertinente pode transmitir essas informações a outras autoridades pertinentes a que se refere o n.º 6.

As instituições de crédito avaliadas como significativas, nos termos do artigo 6.º, n.º 4, do Regulamento (UE) n.º 1024/2013, podem, a título voluntário, notificar ciberameaças significativas à autoridade nacional competente designada nos termos do artigo 4.º da Diretiva 2013/36/UE, que transmite imediatamente essa notificação ao BCE.

Os Estados-Membros podem determinar que as entidades financeiras que, a título voluntário, apresentem uma notificação nos termos do primeiro parágrafo possam também transmitir essa notificação às CSIRT designadas ou criadas nos termos da Diretiva (UE) 2022/2555.

3. Em caso de incidente de caráter severo relacionado com as TIC que tenha impacto nos interesses financeiros dos clientes, as entidades financeiras informam, sem demora indevida e logo que tenham tomado conhecimento do incidente, os seus clientes acerca do incidente de caráter severo relacionado com as TIC e das medidas que foram tomadas para atenuar os efeitos adversos desse incidente.

Em caso de ciberameaça significativa, as entidades financeiras informam, se for caso disso, os seus clientes potencialmente afetados de todas as medidas de proteção adequadas que estes possam ponderar tomar.

4. As entidades financeiras apresentam à autoridade competente pertinente, nos prazos a fixar nos termos do artigo 20.º, primeiro parágrafo, alínea a), subalínea ii), os seguintes elementos:

a) A notificação inicial;

b) Um relatório intercalar após a notificação inicial a que se refere a alínea a), logo que o estado do incidente inicial tenha mudado significativamente ou o tratamento do incidente de caráter severo relacionado com as TIC tenha mudado com base em novas informações disponíveis, seguido, se for caso disso, de notificações atualizadas sempre que fique disponível uma atualização relevante do estado, 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 mitigação, e quando os valores reais do impacto estejam disponíveis para substituir as estimativas.

5. As entidades financeiras podem subcontratar, em conformidade com o direito setorial nacional e da União, as obrigações de notificação previstas no presente artigo a um terceiro prestador de serviços. Em caso de subcontratação, a entidade financeira continua a ser plenamente responsável pelo cumprimento dos requisitos de notificação de incidentes.

6. Aquando da receção da notificação inicial e de cada relatório a que se refere o n.º 4, a autoridade competente comunica, em tempo útil, pormenores sobre o incidente de caráter severo relacionado com as TIC aos seguintes destinatários, com base, se for caso disso, nas respetivas competências:

a) À EBA, à ESMA ou à EIOPA;

b) Ao BCE, no caso das entidades financeiras a que se refere o artigo 2.º, n.º 1, alíneas a), b) e d);

c) Às autoridades competentes, aos pontos de contacto únicos ou CSIRT designados ou criados nos termos da Diretiva (UE) 2022/2555;

d) Às autoridades de resolução, referidas no artigo 3.º da Diretiva 2014/59/UE, e ao Conselho Único de Resolução (CUR), no que respeita às entidades a que se refere o artigo 7.º, n.º 2, do Regulamento (UE) n.º 806/2014 do Parlamento Europeu e do Conselho ([37]), e no que respeita às entidades e grupos a que se refere o artigo 7.º, n.º 4, alínea b), e n.º 5, do Regulamento (UE) n.º 806/2014, se esses pormenores disserem respeito a incidentes que constituam um risco para assegurar funções críticas na aceção do artigo 2.º, n.º 1, ponto 35, da Diretiva 2014/59/UE; e

e) A outras autoridades públicas relevantes ao abrigo do direito nacional.

7. Após a receção de informações nos termos do n.º 6, a EBA, a ESMA ou a EIOPA e o BCE, em consulta com a ENISA e em cooperação com a autoridade competente relevante, avaliam a relevância do incidente de caráter severo relacionado com as TIC para as autoridades competentes de outros Estados-Membros. Na sequência dessa avaliação, a EBA, a ESMA ou a EIOPA notificam, o mais rapidamente possível, as autoridades competentes relevantes de outros Estados-Membros em conformidade. O BCE notifica os membros do Sistema Europeu de Bancos Centrais das questões relevantes para o sistema de pagamentos. Com base nessa notificação as autoridades competentes tomam, se for caso disso, todas as medidas necessárias para proteger a estabilidade imediata do sistema financeiro.

([37]) 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).

8. A notificação a efetuar pela ESMA nos termos do n.º 7 do presente artigo não prejudica a responsabilidade da autoridade competente de transmitir com urgência os pormenores do incidente de caráter severo relacionado com as TIC à autoridade relevante do Estado-Membro de acolhimento, caso uma central de valores mobiliários tenha atividades transfronteiriças significativas no Estado-Membro de acolhimento, o incidente de caráter severo relacionado com as TIC seja suscetível de ter consequências graves para os mercados financeiros do Estado-Membro de acolhimento e caso existam acordos de cooperação entre as autoridades competentes relacionados com a supervisão das entidades financeiras.

Artigo 20.º

Harmonização dos modelos e conteúdos da notificação

As AES, através do Comité Conjunto e em consulta com a ENISA e o BCE, elaboram:

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

   i) estabelecer o conteúdo das notificações de incidentes de caráter severo relacionados com as TIC, a fim de refletir os critérios estabelecidos no artigo 18.º, n.º 1, e incorporar outros elementos, tais como pormenores para determinar a relevância da notificação para outros Estados-Membros e se constitui ou não um incidente de caráter severo operacional ou de segurança relacionado com pagamentos,

   ii) determinar os prazos para a notificação inicial e para cada relatório a que se refere o artigo 19.º, n.º 4,

   iii) determinar o conteúdo da notificação de ciberameaças significativas.

   Ao elaborarem esses projetos de normas técnicas de regulamentação, as AES têm em conta a dimensão e o perfil de risco global da entidade financeira, bem como a natureza, a escala e a complexidade dos seus serviços, atividades e operações, nomeadamente com vista a assegurar que, para efeitos do presente parágrafo, alínea a), subalínea ii), diferentes prazos possam refletir, conforme adequado, as especificidades dos setores financeiros, sem prejuízo da manutenção da coerência no que diz respeito à notificação de incidentes relacionados com as TIC nos termos do presente regulamento e da Diretiva (UE) 2022/2555. As AES apresentam, se for caso disso, uma justificação quando se afastarem das abordagens adotadas no contexto dessa diretiva.

b) Projetos de normas técnicas de execução comuns com vista a estabelecer os formulários, os modelos e os procedimentos normalizados para as entidades financeiras notificarem um incidente de carácter severo relacionado com as TIC e uma ciberameaça significativa.

As AES apresentam os projetos de normas técnicas de regulamentação comuns a que se refere o primeiro parágrafo, alínea a), e os projetos de normas técnicas de execução comuns a que se refere o primeiro parágrafo, alínea b), à Comissão até 17 de julho de 2024.

A Comissão fica habilitada a completar 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 1094/2010 e (UE) n.º 1095/2010.

É conferido à Comissão o poder de 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 1094/2010 e (UE) n.º 1095/2010.

Artigo 21.º

Centralização da notificação de incidentes de caráter severo relacionados com as TIC

1. As AES preparam, através do Comité Conjunto e em consulta com o BCE e a ENISA, um relatório conjunto que avalie a viabilidade de reforçar a centralização da notificação de incidentes através da criação de uma plataforma única na UE para a notificação de incidentes de caráter severo relacionados com as TIC pelas entidades financeiras. O relatório conjunto explora formas de facilitar o fluxo de notificações de incidentes relacionados com as TIC, reduz os custos associados e sustenta análises temáticas com vista a melhorar a convergência em termos de supervisão.

2. O relatório conjunto referido no n.º 1 inclui, pelo menos, os seguintes elementos:

a) Pré-requisitos para a criação de uma plataforma única da UE;

b) Benefícios, limitações e riscos, incluindo o risco associado à elevada concentração de informações sensíveis;

c) A capacidade necessária para assegurar a interoperabilidade no que diz respeito a outros sistemas pertinentes de notificação;

d) Elementos de gestão operacional;

e) Condições de participação;

f) Disposições técnicas de acesso à plataforma única da UE pelas entidades financeiras e pelas autoridades nacionais competentes;

g) Uma avaliação preliminar dos custos financeiros decorrentes da criação da estrutura operacional que servirá de base à plataforma única da UE, incluindo os conhecimentos especializados necessários.

3. As AES apresentam o relatório referido no n.º 1 ao Parlamento Europeu, ao Conselho e à Comissão até 17 de janeiro de 2025.

Artigo 22.º

Observações das autoridades de supervisão

1. Sem prejuízo dos contributos técnicos, do aconselhamento ou das medidas corretivas e do seguimento subsequente que podem ser prestados, se for caso disso, em conformidade com o direito nacional, pelas CSIRTs ao abrigo da Diretiva (UE) 2022/2555, a autoridade competente, acusa a receção da notificação inicial e de cada relatório a que se refere o artigo 19.º, n.º 4, e pode, sempre que exequível, fornecer em tempo útil observações ou orientações de alto nível pertinentes e proporcionadas à entidade financeira, em especial para disponibilizar quaisquer informações anonimizadas sobre ameaças semelhantes, e pode debater as correções aplicadas ao nível da entidade financeira e formas de minimizar e atenuar os impactos adversos no setor financeiro. Sem prejuízo das observações recebidas das autoridades de supervisão, as entidades financeiras continuam a ser plenamente responsáveis pelo tratamento e pelas consequências dos incidentes relacionados com as TIC notificados nos termos do artigo 19.º, n.º 1.

2. As AES, através do Comité Conjunto, comunicam anualmente informações, numa base anónima e agregada, sobre os incidentes de caráter severo relacionados com as TIC, cujos pormenores são fornecidos pelas autoridades competentes, nos termos do artigo 19.º, n.º 6, indicando no mínimo o número de incidentes de caráter severo relacionados com as TIC, a sua natureza, o impacto nas operações das entidades financeiras ou nos clientes, as medidas corretivas adotadas e os custos suportados.

As AES emitem alertas e elaboram estatísticas de alto nível para apoiar as avaliações das ameaças e das vulnerabilidades no domínio das TIC.

Artigo 23.º

Incidentes operacionais ou de segurança relacionados com pagamentos que envolvam instituições de crédito, instituições de pagamento, prestadores de serviços de informação sobre contas e instituições de moeda eletrónica

Os requisitos estabelecidos no presente capítulo são igualmente aplicáveis aos incidentes operacionais ou de segurança relacionados com pagamentos e aos incidentes de caráter severo operacionais ou de segurança relacionados com pagamentos que envolvam instituições de crédito, instituições de pagamento, prestadores de serviços de informação sobre contas e instituições de moeda eletrónica.

CAPITULO IV

Testes de resiliência operacional digital

Artigo 24.º

Requisitos gerais para a realização de testes de resiliência operacional digital

1. Com o intuito de avaliar a preparação para o tratamento de incidentes relacionados com as TIC, identificar pontos fracos, deficiências ou lacunas na resiliência operacional digital e adotar rapidamente medidas corretivas, as entidades financeiras que não sejam microempresas e tendo em consideração os critérios estabelecidos no artigo 4.º, n.º 2, estabelecem, mantêm e revêm um programa sólido e abrangente de testes de resiliência operacional digital para efeitos do quadro de gestão do risco associado às TIC a que se refere o artigo 6.º.

2. O programa de testes de resiliência operacional digital inclui um leque de avaliações, testes, metodologias, práticas e ferramentas a aplicar nos termos dos artigos 25.º e 26.º.

3. Aquando da execução do programa de testes de resiliência operacional digital a que se refere o n.º 1 do presente artigo, as entidades financeiras, que não sejam microempresas, adotam uma abordagem baseada no risco, tendo em conta os critérios estabelecidos no artigo 4.º, n.º 2, atendendo devidamente ao contexto evolutivo do risco associado às TIC, a quaisquer riscos específicos a que a entidade financeira em causa esteja ou possa vir a estar exposta, à criticalidade dos ativos de informação e dos serviços prestados, bem como a qualquer outro fator que a entidade financeira considere adequado.

4. As entidades financeiras que não sejam microempresas asseguram que os testes são realizados por partes independentes, sejam elas internas ou externas. Se os testes forem realizados por um testador interno, as entidades financeiras afetam recursos suficientes e garantem que são evitados conflitos de interesses ao longo das fases de conceção e execução dos testes.

5. As entidades financeiras, que não sejam microempresas, estabelecem procedimentos e políticas para priorizar, classificar e corrigir todas as questões reveladas aquando da realização dos testes e estabelecem metodologias internas de validação para confirmar que é dada uma resposta cabal a todos os pontos fracos, deficiências ou lacunas.

6. As entidades financeiras, que não sejam microempresas, asseguram que são realizados testes adequados, pelo menos uma vez por ano, a todos os sistemas e aplicações que apoiem funções importantes ou críticas no domínio das TIC.

Artigo 25.º

Teste dos sistemas e ferramentas no domínio das TIC

1. O programa de testes de resiliência operacional digital a que se refere o artigo 24.º prevê, em conformidade com os critérios estabelecidos no artigo 4.º, n.º 2, a execução de testes apropriados, como avaliações e rastreamento de vulnerabilidades, análises de fonte aberta, avaliações da segurança das redes, análises das lacunas, análises da segurança física, questionários e soluções de rastreamento com 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 e testes de penetração.

2. As centrais de valores mobiliários e as contrapartes centrais realizam avaliações das vulnerabilidades antes de lançarem ou relançarem serviços novos ou existentes de aplicações e componentes da infraestrutura, e de serviços TIC de apoio às funções críticas ou importantes da entidade financeira.

3. As microempresas realizam os testes a que se refere o n.º 1 combinando uma abordagem baseada no risco com um planeamento estratégico dos testes de TIC, tendo devidamente em conta a necessidade de assegurar o equilíbrio entre a escala dos recursos e o tempo a dedicar aos testes de TIC previstos no presente artigo, por um lado, e a urgência, o tipo de risco, a criticalidade dos ativos de informação e dos serviços prestados, bem como qualquer outro fator relevante, incluindo a capacidade da entidade financeira para assumir riscos calculados, por outro.

Artigo 26.º

Testes avançados às ferramentas, sistemas e processos com base nos TLPT

1. As entidades financeiras que não sejam as entidades a que se refere o artigo 16.º, n.º 1, primeiro parágrafo, nem microempresas, identificadas nos termos do n.º 8, terceiro parágrafo, do presente artigo, realizam, pelo menos de três em três anos, testes avançados através da realização de TLPT. Em função do perfil de risco da entidade financeira e tendo em conta as circunstâncias operacionais, a autoridade competente pode, se necessário, obrigar a entidade financeira a reduzir ou aumentar essa frequência.

2. Cada teste de penetração baseado em ameaças abrange várias ou todas as funções críticas ou importantes de uma entidade financeira e é realizado em sistemas de produção «ao vivo» que apoiem essas funções.

As entidades financeiras identificam todos os sistemas, processos e tecnologias pertinentes de TIC subjacentes de apoio às funções e aos serviços de TIC relevantes que sejam críticos ou importantes, incluindo os que apoiam funções e serviços críticos ou importantes externalizados ou subcontratados a terceiros prestadores de serviços de TIC.

As entidades financeiras avaliam quais as funções críticas ou importantes que devem ser abrangidas pelo TLPT. O resultado desta avaliação determina o âmbito exato do TLPT e é validado pelas autoridades competentes.

3. Quando terceiros prestadores de serviços de TIC estiverem incluídos no âmbito dos TLPT, a entidade financeira toma as medidas e salvaguardas necessárias para assegurar a participação desses terceiros prestadores de serviços de TIC nos TLPT e continua a ser plenamente responsável pelo cumprimento do presente regulamento em qualquer momento.

4. Sem prejuízo do disposto no n.º 2, primeiro e segundo parágrafos, caso seja razoável esperar que a participação de um terceiro prestador de serviços de TIC no TLPT referido no n.º 3, tenha um impacto adverso na qualidade ou na segurança dos serviços fornecidos pelo terceiro prestador de serviços de TIC a clientes que sejam entidades não abrangidas pelo âmbito de aplicação do presente regulamento, ou na confidencialidade dos dados relacionados com esses serviços, a entidade financeira e o terceiro prestador de serviços de TIC podem acordar por escrito que o terceiro prestador de serviços de TIC celebra diretamente acordos contratuais com um testador externo, com o objetivo de realizar, sob a direção de uma entidade financeira designada, um TLPT agrupado que envolva várias entidades financeiras (testes agrupados) às quais o terceiro prestador de serviços de TIC presta serviços de TIC.

Estes testes agrupados abrangem a gama relevante de serviços de TIC que apoiam as funções críticas ou importantes contratadas ao respetivo terceiro prestador de serviços de TIC pelas entidades financeiras. Os testes agrupados são considerados TLPT realizados pelas entidades financeiras que neles participam.

O número de entidades financeiras que participam nos testes agrupados deve ser devidamente ajustado em função da complexidade e dos tipos de serviços envolvidos.

5. As entidades financeiras aplicam, com a cooperação de terceiros prestadores de serviços de TIC e outras partes envolvidas, incluindo os testadores mas excluindo as autoridades competentes, controlos eficazes de gestão do risco para atenuar os riscos de quaisquer potenciais impactos nos dados, danos nos ativos e perturbações nos serviços, operações ou funções críticas ou importantes da própria entidade financeira, das suas contrapartes ou do setor financeiro.

6. No final dos testes, depois de chegarem a acordo sobre os relatórios e os planos corretivos, a entidade financeira e, se for caso disso, os testadores externos fornecem à autoridade designada nos termos dos n.ºs 9 ou 10, um resumo dos resultados relevantes, dos planos corretivos e da documentação que comprova que os TLPT foram realizados em conformidade com os requisitos.

7. As autoridades fornecem às entidades financeiras um comprovativo que certifique que o teste foi realizado em conformidade com os requisitos tal como comprovados na documentação, a fim de permitir o reconhecimento mútuo, por parte das autoridades competentes, dos testes de penetração baseados em ameaças. A entidade financeira notifica a autoridade competente relevante do comprovativo, do resumo das constatações relevantes e dos planos corretivos.

Sem prejuízo deste comprovativo, as entidades financeiras continuam a ser plenamente responsáveis pelo impacto dos testes a que se refere o n.º 4.

8. As entidades financeiras contratam testadores externos nos termos do artigo 27.º para efeitos da realização dos TLPT. Quando as entidades financeiras recorrem a testadores internos para efeitos da realização dos TLPT, contratam um testador externo de três em três testes.

As instituições de crédito que estejam avaliadas como significativas nos termos do artigo 6.º, n.º 4, do Regulamento (UE) n.º 1024/2013, só podem recorrer a testadores externos nos termos do artigo 27.º, n.º 1, alíneas a) a e).

As autoridades competentes identificam as entidades financeiras que devem realizar TLPT tendo em conta os critérios estabelecidos no artigo 4.º, n.º 2, com base numa avaliação dos seguintes elementos:

a) Fatores relacionados com o impacto, em especial a medida em que os serviços prestados e as atividades desenvolvidas pela entidade financeira afetam o setor financeiro;

b) Possíveis preocupações com a estabilidade financeira, nomeadamente o caráter sistémico da entidade financeira a nível da União ou nacional, conforme aplicável;

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

9. Os Estados-Membros podem designar uma única autoridade pública do setor financeiro responsável pelas questões relacionadas com os TLPT no setor financeiro a nível nacional e atribuir-lhe todas as competências e tarefas para o efeito.

10. Na ausência de uma designação nos termos do n.º 9 do presente artigo, e sem prejuízo do poder de identificar as entidades financeiras que devem realizar TLPT, as autoridades competentes podem delegar o exercício de algumas ou de todas as funções a que se referem o presente artigo e o artigo 27.º noutra autoridade nacional do setor financeiro.

11. As AES desenvolvem, em concertação com o BCE, projetos de normas técnicas de regulamentação, em conformidade com o quadro TIBER–EU, a fim de especificar mais pormenorizadamente:

a) Os critérios utilizados para fins de aplicação do n.º 8, segundo parágrafo;

b) Os requisitos e as normas que regem o recurso a testadores internos;

c) Os requisitos relativos:

   i) ao âmbito dos TLPT a que se refere o n.º 2,

   ii) à metodologia 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 dos testes;

d) O tipo de cooperação em matéria de supervisão e outra cooperação relevante e necessária para realizar os TLPT e para facilitar o reconhecimento mútuo desses testes no contexto das entidades financeiras que operam em mais do que um Estado-Membro, para permitir um nível de envolvimento adequado das entidades de supervisão e uma execução flexível, a fim de atender às especificidades dos subsetores financeiros ou dos mercados financeiros locais.

Ao elaborar estes projetos de normas técnicas de regulamentação, as AES têm devidamente em conta todas as características específicas decorrentes da natureza distinta das atividades nos diferentes setores dos serviços financeiros.

As AES apresentam estes projetos de normas técnicas de regulamentação à Comissão até 17 de julho de 2024.

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 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 27.º

Requisitos aplicáveis aos testadores para a realização dos TLPT

1. As entidades financeiras só recorrem à realização dos TLPT a testadores que:

a) Sejam os mais adequados e os mais idóneos;

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

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

d) Forneçam uma garantia independente ou um relatório de auditoria em relação à boa gestão dos riscos associada à realização de TLPT, nomeadamente a devida proteção das informações confidenciais da entidade financeira e a cobertura dos riscos operacionais da entidade financeira;

e) Estejam devida e totalmente cobertos por seguros de indemnização profissional pertinentes, nomeadamente contra riscos de conduta irregular e negligência.

2. Ao usarem testadores internos, as entidades financeiras devem garantir que, além das condições referidas no n.º 1, são preenchidas as seguintes condições:

a) A sua utilização foi aprovada pela autoridade competente pertinente ou pela autoridade pública única designada nos termos do artigo 26.º, n.ºs 9 e 10;

b) A autoridade competente relevante verificou que a entidade financeira afetou recursos suficientes e assegurou que são evitados conflitos de interesses ao longo das fases de conceção e execução do teste; e

c) O prestador de informações sobre ameaças é externo à entidade financeira.

3. As entidades financeiras asseguram que os contratos celebrados com testadores externos exijam uma boa gestão dos resultados dos TLPT e que qualquer tratamento de dados, nomeadamente qualquer produção, conservação, agregação, projeto, relatório, comunicação ou destruição de dados, não acarrete riscos para a entidade financeira.

CAPÍTULO V

Gestão do risco associado às TIC devido a terceiros

Secção I

Princípios fundamentais para a boa gestão do risco associado às TIC devido a terceiros

Artigo 28.º

Princípios gerais

1. As entidades financeiras gerem o risco associado às TIC devido a terceiros como componente integrante do risco associado às TIC no âmbito do seu quadro de gestão do risco associado às TIC, tal como referido no artigo 6.º, n.º 1, e de acordo com os seguintes princípios:

a) As entidades financeiras que celebraram acordos contratuais relativos à utilização de serviços de TIC para gerir as suas operações comerciais mantêm sempre a responsabilidade pelo cumprimento e observância de todas as obrigações previstas no presente regulamento e no direito dos serviços financeiros aplicável;

b) A gestão do risco associado às TIC devido a terceiros por parte das entidades financeiras é efetuada em consonância com o princípio da proporcionalidade, tendo em conta:

i) a natureza, a dimensão, a complexidade e a importância das dependências relacionadas com as TIC,

ii) os riscos decorrentes dos acordos contratuais relativos à utilização de serviços de TIC celebrados com terceiros prestadores de serviços de TIC, tendo em conta a criticalidade ou a importância do respetivo serviço, processo ou função, bem como o impacto potencial na continuidade e na disponibilidade dos serviços e atividades financeiros, a nível individual e de grupo.

2. Para efeitos do seu quadro de gestão do risco associado às TIC, as entidades financeiras que não sejam as entidades a que se refere o artigo 16.º, n.º 1, primeiro parágrafo, nem microempresas adotam e revêm periodicamente uma estratégia em matéria de risco associado às TIC devido a terceiros, tendo em conta a estratégia com múltiplos fornecedores a que se refere o artigo 6.º, n.º 9, se for caso disso. A estratégia relativa ao risco associado às TIC devido a terceiros inclui uma política de utilização dos serviços de TIC, que apoiem funções críticas ou importantes, prestados por terceiros prestadores de serviços de TIC, e é aplicada numa base individual e, quando necessário, numa base subconsolidada e consolidada. O órgão de administração revê, com base numa avaliação do perfil de risco global da entidade financeira e da escala e complexidade dos serviços operacionais, periodicamente os riscos identificados no que diz respeito aos acordos contratuais relativas à utilização de serviços de TIC que apoiem funções críticas ou importantes.

3. Para efeitos do seu quadro de gestão do risco associado às TIC, as entidades financeiras mantêm e atualizam, ao nível da entidade e aos níveis subconsolidado e consolidado, um registo de informações em relação a todos os acordos contratuais relativos à utilização dos serviços TIC prestados por terceiros prestadores de serviços de TIC.

Os acordos contratuais referidos no primeiro parágrafo são devidamente documentados, estabelecendo uma distinção entre os que abrangem serviços TIC que apoiem funções críticas ou importantes e os que não abrangem esses tipos de funções.

As entidades financeiras comunicam pelo menos uma vez por ano às autoridades competentes o número de novos acordos contratuais relativos à utilização de serviços de TIC, as categorias de terceiros prestadores de serviços de TIC, o tipo de acordos contratuais, assim como os serviços de TIC que estão a ser prestados e as funções que estão a ser realizadas.

As entidades financeiras disponibilizam à autoridade competente, a pedido desta, 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 informam atempadamente a autoridade competente sobre qualquer acordo contratual planeado para a utilização de serviços de TIC que apoiem funções críticas ou importantes, bem como quando uma determinada função passar a ser crítica ou importante.

4. Antes de celebrar um acordo contratual relativo à utilização de serviços de TIC, as entidades financeiras:

a) Avaliam se o acordo contratual abrange a utilização de serviços de TIC que apoiem uma função crítica ou importante;

b) Avaliam se as condições de supervisão relativamente à subcontratação estão satisfeitas;

c) Identificam e avaliam todos os riscos relevantes em relação ao acordo contratual, nomeadamente a possibilidade de esse acordo poder contribuir para reforçar o risco de concentração no domínio das TIC, a que se refere o artigo 29.º;

d) Efetuam todas as diligências devidas quanto aos potenciais terceiros prestadores de serviços de TIC e asseguram que, ao longo dos processos de seleção e avaliação, o terceiro prestador de serviços de TIC é adequado;

e) Identificam e avaliam os conflitos de interesses que possam decorrer do acordo contratual.

5. As entidades financeiras só podem celebrar acordos contratuais com terceiros prestadores de serviços de TIC que cumpram normas de segurança da informação adequadas. Quando os acordos contratuais dizem respeito a funções críticas ou importantes, as entidades financeiras atendem, antes da celebração dos acordos, devidamente ao respeito, pelos terceiros prestadores de serviços de TIC, das normas mais atualizadas e mais rigorosas em matéria de segurança da informação.

6. Ao exercer direitos de acesso, inspeção e auditoria sobre o terceiro prestador de serviços de TIC, as entidades financeiras predeterminam, em função de uma 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.

Quando os acordos contratuais celebrados com terceiros prestadores de serviços de TIC para a utilização de serviços de TIC impliquem um nível elevado de complexidade técnica, a entidade financeira verifica se os auditores, sejam eles internos ou externos, ou um grupo de auditores, possuem as aptidões e os conhecimentos adequados para realizar eficazmente as auditorias e as avaliações pertinentes.

7. As entidades financeiras asseguram que os acordos contratuais relativos à utilização de serviços de TIC possam ser rescindidos em qualquer uma das seguintes circunstâncias:

a) Violação significativa pelo terceiro prestador de serviços de TIC da legislação, regulamentação ou das condições contratuais aplicáveis;

b) Circunstâncias identificadas aquando da monitorização do risco associado às TIC devido a terceiros que sejam consideradas como passíveis de alterar o desempenho das funções realizadas através do acordo contratual, nomeadamente alterações materiais que afetem o acordo contratual ou a situação do terceiro prestador de serviços de TIC;

c) Debilidades comprovadas do terceiro prestador de serviços de TIC que se prendem com a sua gestão global do risco associado às TIC e, em particular, qualquer deficiência na forma como garante a disponibilidade, autenticidade, integridade e confidencialidade dos dados, pessoais ou sensíveis ou dos dados não pessoais;

d) Quando a autoridade competente deixar de poder supervisionar eficazmente a entidade financeira em resultado das condições ou das circunstâncias relacionadas com o acordo contratual respetivo.

8. No que respeita aos serviços de TIC que apoiem funções críticas ou importantes, as entidades financeiras preveem estratégias de saída. As estratégias de saída têm em conta riscos que possam surgir a nível dos terceiros prestadores de serviços de TIC, em especial uma possível falha destes, uma deterioração da qualidade dos serviços de TIC prestados, qualquer perturbação das atividades devido a falha ou desadequação da prestação dos serviços de TIC ou qualquer risco material relacionado com o desempenho adequado e contínuo do respetivo serviço de TIC, ou em caso de rescisão dos acordos contratuais com os terceiros prestadores de serviços de TIC em qualquer das circunstâncias enumeradas no n.º 7.

As entidades financeiras asseguram poder rescindir acordos contratuais sem:

a) Perturbação das suas atividades operacionais;

b) Limitação da observância dos requisitos regulamentares;

c) Prejuízo para a continuidade e a qualidade dos serviços prestados aos clientes.

Os planos de saída devem ser abrangentes, documentados e, em conformidade com os critérios estabelecidos no artigo 4.º, n.º 2, devem ser suficientemente testados e regularmente revistos.

As entidades financeiras identificam soluções alternativas e desenvolvem planos de transição que lhes permitam eliminar os serviços de TIC subcontratados e os dados pertinentes junto do terceiro prestador de serviços de TIC e transferi-los em segurança e na íntegra para prestadores de serviços alternativos ou reincorporá-los internamente.

As entidades financeiras preveem medidas de contingência adequadas para manter a continuidade do negócio caso ocorram as circunstâncias a que se refere o primeiro parágrafo.

9. As AES desenvolvem, através do Comité Conjunto, projetos de normas técnicas de execução por forma a criar modelos normalizados para fins do registo de informações a que se refere o n.º 3, incluindo informações que sejam comuns a todos os acordos contratuais relativos à utilização de serviços de TIC. As AES apresentam esses projetos de normas técnicas de execução à Comissão até 17 de janeiro de 2024.

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 1094/2010 e (UE) n.º 1095/2010.

10. As AES elaboram, através do Comité Conjunto, projetos de normas técnicas de regulamentação para especificar mais pormenorizadamente o conteúdo detalhado da política a que se refere o n.º 2 em relação aos acordos contratuais relativos à utilização de serviços de TIC que apoiem funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC.

Ao elaborarem esses projetos de normas técnicas de regulamentação, as AES têm em conta a dimensão e o perfil de risco global da entidade financeira, bem como a natureza, a escala e a complexidade dos seus serviços, atividades e operações. As AES apresentam esses projetos de normas técnicas de regulamentação à Comissão até 17 de janeiro de 2024.

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 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 29.º

Avaliação preliminar do risco de concentração no domínio das TIC ao nível da entidade

1. Quando procedem à identificação e avaliação do risco de concentração no domínio das TIC a que se refere o artigo 28.º, n.º 4, alínea c), as entidades financeiras têm também em conta se a celebração prevista de um acordo contratual em relação a serviços de TIC que apoiem funções críticas ou importantes pode conduzir a qualquer uma das situações seguintes:

a) Celebração de um contrato com um terceiro prestador de serviços de TIC que não seja facilmente substituível; ou

b) Celebração de vários acordos contratuais em relação à prestação de serviços de TIC que apoiem funções críticas ou importantes com o mesmo terceiro prestador de serviços de TIC ou com terceiros prestadores de serviços de TIC com ligações estreitas entre si.

As entidades financeiras ponderam os benefícios e os custos de soluções alternativas como a utilização de terceiros prestadores de serviços de TIC diferentes, tendo em conta se e como as soluções previstas satisfazem as necessidades operacionais e os objetivos definidos na sua estratégia de resiliência digital.

2. Quando os acordos contratuais relativos à utilização de serviços de TIC que apoiem funções críticas ou importantes incluem a possibilidade de um terceiro prestador de serviços de TIC subcontratar serviços TIC que apoiem uma função crítica ou importante a outro terceiro prestador de serviços de TIC, as entidades financeiras ponderam os benefícios e os riscos que podem surgir associados a essa possível subcontratação, em especial no caso de um subcontratante de TIC estabelecido num país terceiro.

Quando os contratos dizem respeito a serviços de TIC que apoiem funções críticas ou importantes, as entidades financeiras consideram devidamente as disposições jurídicas relativas à insolvência aplicáveis em caso de falência do terceiro prestador de serviços de TIC, bem como quaisquer constrangimentos que possam surgir em relação à recuperação urgente dos dados da entidade financeira.

Quando os acordos contratuais relativos à utilização de serviços de TIC que apoiem funções críticas ou importantes são celebrados com um terceiro prestador de serviços de TIC estabelecido num país terceiro, as entidades financeiras têm igualmente em conta, para além das considerações referidas no segundo parágrafo, o cumprimento das regras da União em matéria de proteção de dados e a aplicação efetiva da lei nesse país terceiro.

Quando os acordos contratuais para a utilização de serviços de TIC que apoiem funções críticas ou importantes preveem a subcontratação; as entidades financeiras avaliam se e de que forma as cadeias de subcontratação potencialmente longas e complexas podem afetar a sua capacidade de monitorizar cabalmente as funções subcontratadas e a capacidade da autoridade competente para supervisionar eficazmente a entidade financeira nesse aspeto.

Artigo 30.º

Principais disposições contratuais

1. Os direitos e obrigações da entidade financeira e do terceiro prestador de serviços de TIC são claramente identificados e especificados por escrito. O contrato na sua totalidade inclui os acordos de nível de serviço e consta de um documento escrito disponível para as partes em papel ou num documento com outro formato descarregável, duradouro e acessível.

2. Os acordos contratuais relativos à utilização de serviços de TIC incluem, pelo menos, os seguintes elementos:

a) A descrição clara e completa de todas as funções e serviços de TIC a prestar pelo terceiro prestador de serviços de TIC, indicando se a subcontratação de serviços TIC que apoiem uma função crítica ou importante, ou de partes materiais da mesma, é permitida e, se for esse o caso, as condições aplicáveis a essa subcontratação;

b) Os locais, nomeadamente as regiões ou os países, onde as funções e os serviços de TIC objeto de contratação ou subcontratação devem ser prestados e onde devem ser tratados os dados, nomeadamente o local de conservação dos dados, bem como o requisito, aplicável ao terceiro prestador de serviços de TIC, de notificar antecipadamente a entidade financeira se planear mudar de locais;

c) Disposições sobre a disponibilidade, autenticidade, integridade e confidencialidade em relação à proteção de dados, incluindo dados pessoais;

d) 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 do terceiro prestador de serviços de TIC, ou em caso de rescisão dos acordos contratuais;

e) Descrições do nível de serviço, incluindo as respetivas atualizações e revisões;

f) A obrigação de o terceiro prestador de serviços de TIC prestar assistência à entidade financeira sem custos adicionais, ou a um custo previamente determinado, caso ocorra um incidente relacionado com as TIC que envolve o serviço de TIC prestado à entidade financeira;

g) A obrigação de o terceiro prestador de serviços de TIC cooperar plenamente com as autoridades competentes e as autoridades de resolução da entidade financeira, e, nomeadamente, com pessoas designadas por essas autoridades;

h) Direitos de rescisão e períodos mínimos de pré-aviso relacionado com a rescisão dos acordos contratuais, que correspondam às expectativas das autoridades competentes e das autoridades de resolução;

i) As condições aplicáveis à participação de terceiros prestadores de serviços de TIC nos programas de sensibilização para a segurança das TIC e na formação em matéria de resiliência operacional digital das entidades financeiras, nos termos do artigo 13.º, n.º 6.

3. Os acordos contratuais relativos à utilização de serviços de TIC de apoio a funções críticas ou importantes incluem, para além dos elementos referidos no n.º 2, pelo menos, o seguinte:

a) Descrições completas do nível de serviço, incluindo as respetivas atualizações e revisões, com metas de desempenho quantitativas e qualitativas rigorosas para os níveis de serviço acordados, por forma a permitir uma monitorização eficaz, por parte da entidade financeira, dos serviços TIC, e a adoção, sem demora injustificada, de medidas corretivas, quando os níveis de serviço acordados não forem cumpridos;

b) Períodos de notificação e obrigações de notificação do terceiro prestador de serviços de TIC à entidade financeira, nomeadamente quanto a quaisquer desenvolvimentos que possam ter impacto material na capacidade de o terceiro prestador de serviços de TIC prestar eficazmente serviços de TIC que apoiem funções críticas ou importantes em consonância com os níveis de serviço acordados;

c) Requisitos que obrigam o terceiro prestador de serviços de TIC a executar e testar planos de contingência operacional e a dispor de medidas, ferramentas e políticas de segurança no domínio das TIC que garantam um nível adequado de segurança na prestação de serviços pela entidade financeira em consonância com o seu quadro regulamentar;

d) A obrigação de o terceiro prestador de serviços de TIC participar e cooperar plenamente nos TLPT realizados pela entidade financeira, conforme referido nos artigos 26.º e 27.º;

e) O direito de monitorizar numa base contínua o desempenho do terceiro prestador de serviços de TIC, o que implica o seguinte:

i) direitos ilimitados de acesso, inspeção e auditoria pela entidade financeira, ou por um terceiro designado, e pela autoridade competente, bem como o direito a fazer cópias da documentação importante no local, caso essa documentação seja crítica para as operações do terceiro prestador de serviços de TIC, cujo exercício efetivo não seja impedido nem limitado por outros acordos contratuais ou políticas de execução,

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

iii) a obrigação de plena cooperação por parte do terceiro prestador de serviços de 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

iv) a obrigação de fornecer pormenores sobre o âmbito, os procedimentos a seguir e a frequência das referidas inspeções e auditorias;

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

i) durante o qual o terceiro prestador de serviços de TIC continuará a desempenhar as respetivas funções ou a prestar serviços de TIC 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 migrar para outro terceiro prestador de serviços de TIC ou passar a utilizar soluções internas em função da complexidade do serviço prestado.

Em derrogação da alínea e), o terceiro prestador de serviços de TIC e a entidade financeira, que seja uma microempresa, podem decidir que os direitos de acesso, inspeção e auditoria da entidade financeira possam ser delegados numa entidade terceira independente, nomeada pelo terceiro prestador de serviços de TIC, e que a entidade financeira possa requerer, a qualquer momento, informações e garantias sobre o desempenho do terceiro prestador de serviços de TIC.

4. Aquando da negociação dos acordos contratuais, as entidades financeiras e os terceiros prestadores de serviços de TIC preveem a utilização de cláusulas contratuais normalizadas desenvolvidas pelas autoridades públicas para serviços específicos.

5. As AES desenvolvem, através do Comité Conjunto, projetos de normas técnicas de regulamentação que especifiquem mais pormenorizadamente os elementos a que se refere o n.º 2, alínea a), que permitam à entidade financeira determinar e avaliar quando proceder à subcontratação de serviços de TIC de apoio a funções críticas ou importantes.

Ao elaborarem esses projetos de normas técnicas de regulamentação, as AES têm em conta a dimensão e o perfil de risco global da entidade financeira, bem como a natureza, a escala e a complexidade dos seus serviços, atividades e operações.

As AES apresentam esses projetos de normas técnicas de regulamentação à Comissão até 17 de julho de 2024.

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 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.

Secção II

Quadro de superintendência dos terceiros prestadores de serviços de TIC críticos

Artigo 31.º

Designação dos terceiros prestadores de serviços de TIC críticos

1. As AES, através do Comité Conjunto e mediante recomendação do fórum de superintendência criado nos termos do artigo 32.º, n.º 1:

a) Designam os terceiros prestadores de serviços de TIC que são críticos para as entidades financeiras, na sequência de uma avaliação que tenha em conta os critérios especificados no n.º 2;

b) Nomeiam como autoridade fiscalizadora principal para cada terceiro prestador de serviços de TIC crítico, a AES que é responsável, nos termos dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 ou (UE) n.º 1095/2010, pelas entidades financeiras que, em conjunto, detêm a maior quota do total de ativos no valor total dos ativos de todas as entidades financeiras que utilizam os serviços do terceiro prestador de serviços de TIC crítico pertinente, tal como demonstrado pela soma dos balanços individuais dessas entidades financeiras.

2. A designação a que se refere o n.º 1, alínea a), baseia-se em todos os critérios seguintes no tocante aos serviços de TIC prestados por um terceiro prestador de serviços de TIC:

a) O impacto sistémico na estabilidade, continuidade ou qualidade da prestação dos serviços financeiros caso o terceiro prestador de serviços de 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 e o valor total dos ativos das entidades financeiras que beneficiam dos serviços prestados por esse terceiro prestador de serviços de TIC pertinente;

b) O caráter sistémico ou a importância das entidades financeiras que dependem do terceiro prestador de serviços de TIC pertinente, 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 do respetivo terceiro prestador de serviços de 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 pelo terceiro prestador de serviços de TIC pertinente no que diz respeito a funções críticas ou importantes das entidades financeiras que, em última análise, envolvam o mesmo terceiro prestador de serviços de TIC, independentemente do facto de as entidades financeiras dependerem desses serviços direta ou indiretamente, através de acordos de subcontratação;

d) O grau de substituibilidade do terceiro prestador de serviços de TIC, tendo em conta os seguintes parâmetros:

   i) a falta de alternativas reais, mesmo que parciais, devido ao número limitado de terceiros prestadores de serviços de TIC ativos num mercado específico, à quota de mercado do terceiro prestador de serviços de TIC pertinente, à complexidade ou sofisticação técnicas envolvidas, nomeadamente em relação a qualquer tecnologia patenteada, ou ainda às características específicas da organização ou atividade do terceiro prestador de serviços de TIC,

   ii) dificuldades em relação à migração parcial ou total dos dados pertinentes e dos volumes de trabalho do terceiro prestador de serviços de TIC pertinente para outro terceiro prestador de serviços de TIC, devido aos custos financeiros significativos, ao tempo ou a outros recursos envolvidos no processo de migração ou devido ao aumento do risco associado às TIC ou outros riscos operacionais a que a entidade financeira possa ficar exposta por via dessa migração.

3. Se o terceiro prestador de serviços de TIC pertencer a um grupo, são tidos em conta os critérios a que se refere o n.º 2 em relação aos serviços de TIC prestados pelo grupo no seu conjunto.

4. Os terceiros prestadores de serviços de TIC críticos que façam parte de um grupo designam uma pessoa coletiva como ponto de coordenação, a fim de assegurar uma representação e comunicação adequadas com a autoridade fiscalizadora principal.

5. A autoridade fiscalizadora principal notifica o terceiro prestador de serviços de TIC do resultado da avaliação que conduziu à designação a que se refere o n.º 1, alínea a). No prazo de seis semanas a contar da data de notificação, o terceiro prestador de serviços de TIC pode apresentar à autoridade fiscalizadora principal uma declaração fundamentada com todas as informações pertinentes para efeitos da avaliação. A autoridade fiscalizadora principal tem em consideração a declaração fundamentada e pode solicitar a apresentação de informações adicionais no prazo de 30 dias de calendário a contar da receção dessa declaração.

Após a designação de um terceiro prestador de serviços de TIC como crítico, as AES, através do Comité Conjunto, notificam o terceiro prestador de serviços de TIC dessa designação e da data a partir da qual será efetivamente sujeito a atividades de superintendência. Essa data de início não pode ser posterior a um mês após a notificação. Os terceiros prestadores de serviços de TIC notificam as entidades financeiras às quais prestam serviços da sua designação como críticos.

6. A Comissão fica habilitada a adotar um ato delegado, nos termos do artigo 57.º, a fim de completar o presente regulamento especificando mais pormenorizadamente os critérios referidos no n.º 2 do presente artigo, até 17 de julho de 2024.

7. A designação referida no n.º 1, alínea a), não pode ser utilizada até que a Comissão adote um ato delegado nos termos do n.º 6.

8. A designação a que se refere o n.º 1, alínea a), não é aplicável:

i) Às entidades financeiras que prestam serviços de TIC a outras entidades financeiras;

ii) Aos terceiros prestadores de serviços de TIC que estejam sujeitos a quadros de superintendência criados com a finalidade de apoiar as atribuições a que se refere o artigo 127.º, n.º 2, do Tratado sobre o Funcionamento da União Europeia;

iii) Aos prestadores de serviços de TIC intragrupo;

iv) Aos terceiros prestadores de serviços de TIC que, num Estado-Membro específico, prestem serviços de TIC a entidades financeiras ativas exclusivamente nesse Estado-Membro.

9. As AES, através do Comité Conjunto, estabelecem, publicam e atualizam anualmente a lista de terceiros prestadores de serviços de TIC críticos a nível da União.

10. Para efeitos do n.º 1, alínea a), as autoridades competentes transmitem, anualmente e numa base agregada, os relatórios referidos no artigo 28.º, n.º 3, terceiro parágrafo, ao fórum de superintendência criado nos termos do artigo 32.º. O fórum de superintendência avalia as dependências das entidades financeiras em relação a terceiros no domínio das TIC com base nas informações recebidas das autoridades competentes.

11. Os terceiros prestadores de serviços de TIC que não estejam incluídos na lista referida no n.º 9 podem solicitar a sua designação como críticos, nos termos do n.º 1, alínea a).

Para efeitos do primeiro parágrafo, o terceiro prestador de serviços de TIC apresenta uma candidatura fundamentada à EBA, à ESMA ou à EIOPA, que, através do Comité Conjunto, decide designar ou não esse terceiro prestador de serviços de TIC como crítico, nos termos do n.º 1, alínea a).

A decisão a que se refere o segundo parágrafo é adotada e notificada ao terceiro prestador de serviços de TIC no prazo de seis meses a contar da receção da candidatura.

12. As entidades financeiras apenas recorrem aos serviços de um terceiro prestador de serviços de TIC estabelecido num país terceiro e que tenha sido designado como crítico nos termos do n.º 1, alínea a), caso este último tenha estabelecido uma filial na União no prazo de 12 meses a contar da designação.

13. O terceiro prestador de serviços de TIC crítico a que se refere o n.º 12 notifica a autoridade fiscalizadora principal de quaisquer alterações à estrutura de gestão da filial estabelecida na União.

Artigo 32.º

Estrutura do quadro de superintendência

1. O Comité Conjunto, nos termos do artigo 57.º, n.º 1, dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, cria o fórum de superintendência, enquanto subcomité, com a finalidade de apoiar o trabalho do Comité Conjunto e da autoridade fiscalizadora principal a que se refere o artigo 31.º, n.º 1, alínea b), no domínio do risco associado às TIC devido a terceiros em todos os setores financeiros. O fórum de superintendência elabora os projetos das posições comuns e os projetos dos atos comuns do Comité Conjunto nesse domínio.

O fórum de superintendência debate periodicamente os desenvolvimentos mais importantes no que diz respeito aos riscos e às vulnerabilidades associados às TIC e promove uma abordagem coerente da monitorização do risco associado às TIC devido a terceiros a nível da União.

2. O fórum de superintendência realiza anualmente uma avaliação coletiva dos resultados e das conclusões das atividades de superintendência desenvolvidas em relação a todos os terceiros prestadores de serviços de TIC críticos e promove medidas de coordenação para aumentar a resiliência operacional digital das entidades financeiras, fomentar as boas práticas em matéria de gestão do risco de concentração no domínio das TIC e explora fatores para atenuar a transferência intersetorial dos riscos.

3. O fórum de superintendência apresenta indicadores de referência abrangentes para os terceiros prestadores de serviços de TIC críticos, a adotar pelo Comité Conjunto enquanto posições comuns das AES nos termos do artigo 56.º, n.º 1, dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010.

4. O fórum de superintendência é composto:

a) Pelos presidentes das AES;

b) Por um representante de alto nível do pessoal atualmente em funções nas autoridades competentes pertinentes de cada Estado-Membro a que se refere o artigo 46.º;

c) Pelos administradores executivos de cada AES e um representante da Comissão, do CERS, do BCE e da ENISA, na qualidade de observadores;

d) Se for caso disso, por um representante suplementar de cada Estado-Membro, na qualidade de observador, de uma autoridade competente a que se refere o artigo 46.º;

e) Se for caso disso, por um representante das autoridades competentes designadas ou criadas nos termos da Diretiva (UE) 2022/2555, responsável pela supervisão de uma entidade essencial ou importante abrangida por essa diretiva, que tenha sido designado como terceiro prestador de serviços de TIC crítico, na qualidade de observador.

O fórum de superintendência pode, se for caso disso, solicitar o parecer de peritos independentes nomeados nos termos do n.º 6.

5. Cada Estado-Membro designa a autoridade competente pertinente cujo membro do pessoal desempenha a função de representante de alto nível a que se refere o n.º 4, primeiro parágrafo, alínea b), e informa desse facto a autoridade fiscalizadora principal.

As AES publicam no seu sítio Web a lista dos representantes de alto nível do pessoal em funções da autoridade competente pertinente, designados pelos Estados-Membros.

6. Os peritos independentes referidos no n.º 4, segundo parágrafo, são nomeados pelo fórum de superintendência de entre um grupo de peritos selecionados na sequência de um processo de candidatura público e transparente.

Os peritos independentes são nomeados com base nos seus conhecimentos especializados em matéria de estabilidade financeira, resiliência operacional digital e segurança das TIC. Agem de forma independente e objetiva no interesse exclusivo da União no seu conjunto e não procuram obter nem recebem instruções das instituições ou órgãos da União, dos governos dos Estados-Membros nem de qualquer outro organismo público ou privado.

7. Nos termos do artigo 16.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010, até 17 de julho de 2024, as AES emitem, para efeitos da presente secção, orientações sobre a cooperação entre as AES e as autoridades competentes que abrangem os procedimentos pormenorizados e as condições para a repartição e exercício das atribuições das autoridades competentes e das AES, bem como os pormenores relativos ao intercâmbio de informações que são necessários para que as autoridades competentes possam assegurar o acompanhamento das recomendações nos termos do artigo 35.º, n.º 1, alínea d), dirigidas aos terceiros prestadores de serviços de TIC críticos.

8. Os requisitos definidos na presente secção não prejudicam a aplicação da Diretiva (UE) 2022/2555 e das outras regras da União em matéria de superintendência aplicáveis aos prestadores de serviços de computação em nuvem.

9. As AES, através do Comité Conjunto e com base no trabalho preparatório realizado pelo fórum de superintendência, apresentam anualmente ao Parlamento Europeu, ao Conselho e à Comissão um relatório sobre a aplicação da presente secção.

Artigo 33.º

Atribuições da autoridade fiscalizadora principal

1. A autoridade fiscalizadora principal, nomeada nos termos do artigo 31.º, n.º 1, alínea b), é incumbida da superintendência dos terceiros prestadores de serviços de TIC críticos e é, para efeitos de todas as questões relacionadas com a superintendência, o ponto de contacto principal desses terceiros prestadores de serviços de TIC críticos.

2. Para efeitos do n.º 1, a autoridade fiscalizadora principal avalia se cada terceiro prestador de serviços de TIC crítico dispõe de regras, procedimentos, mecanismos e disposições abrangentes, sólidas e eficazes para gerir o risco associado às TIC que possa constituir para as entidades financeiras.

A avaliação a que se refere o primeiro parágrafo centra-se sobretudo nos serviços de TIC prestados pelo terceiro prestador de serviços de TIC crítico que apoia funções críticas ou importantes das entidades financeiras. Quando necessário para fazer face a todos os riscos pertinentes, essa avaliação é alargada aos serviços de TIC que não sejam funções críticas ou importantes.

3. A avaliação referida no n.º 2 abrange:

a) Os requisitos em matéria de TIC para assegurar, em especial, a segurança, a disponibilidade, a continuidade, a escalabilidade e a qualidade dos serviços que o terceiro prestador de serviços de TIC crítico presta às entidades financeiras, bem como a capacidade para manter sempre níveis muito elevados de disponibilidade, autenticidade, integridade ou confidencialidade dos dados;

b) A segurança física que contribui para assegurar a segurança 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, planos de continuidade das atividades no domínio das TIC e políticas de resposta e recuperação em matéria de 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 significativos relacionados com as TIC às entidades financeiras, bem como a gestão e resolução desses incidentes, em especial em caso de 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 de TIC a entidades financeiras.

4. Com base na avaliação a que se refere o n.º 2, e em coordenação com a rede de superintendência conjunta a que se refere o artigo 34.º, n.º 1, a autoridade fiscalizadora principal adota um plano de superintendência individual claro, pormenorizado e fundamentado que descreva os objetivos anuais em matéria de superintendência e as principais ações de superintendência planeadas para cada terceiro prestador de serviços de TIC crítico. Este plano é comunicado anualmente ao terceiro prestador de serviços de TIC crítico.

Antes da adoção do plano de superintendência, a autoridade fiscalizadora principal comunica o projeto de plano de superintendência ao terceiro prestador de serviços de TIC crítico.

Após a receção do projeto de plano de superintendência, o terceiro prestador de serviços de TIC crítico pode apresentar uma declaração fundamentada, no prazo de 15 dias de calendário, que demonstre o impacto esperado para os clientes que não sejam entidades abrangidas pelo âmbito de aplicação do presente regulamento e, se for caso disso, apresente soluções para atenuar os riscos.

5. Depois de os planos anuais de superintendência a que se refere o n.º 4 terem sido adotados e notificados aos terceiros prestadores de serviços de TIC críticos, as autoridades competentes só podem adotar medidas em relação a esses prestadores de comum acordo com a autoridade fiscalizadora principal.

Artigo 34.º

Coordenação operacional entre autoridades fiscalizadoras principais

1. A fim de assegurar uma abordagem coerente das atividades de superintendência e por forma a possibilitar estratégias de superintendência geral coordenadas e abordagens operacionais e metodologias de trabalho coerentes, as três autoridades fiscalizadoras principais nomeadas nos termos do artigo 31.º, n.º 1, alínea b), criam uma rede de superintendência conjunta para se coordenarem entre si nas fases preparatórias e para coordenaram a realização de atividades de superintendência relativamente aos respetivos terceiros prestadores de serviços de TIC críticos, bem como no decurso de qualquer ação que possa ser necessária nos termos do artigo 42.º.

2. Para efeitos do n.º 1, as autoridades fiscalizadoras principais elaboram um protocolo de superintendência comum que especifique os procedimentos pormenorizados a seguir para realizar a coordenação no quotidiano e assegurar intercâmbios e reações céleres. O protocolo é revisto periodicamente a fim de refletir as necessidades operacionais, em especial a evolução das disposições práticas de superintendência.

3. As autoridades fiscalizadoras principais podem, numa base *ad hoc*, solicitar ao BCE e à ENISA que prestem aconselhamento técnico, partilhem experiências práticas ou participem em reuniões de coordenação específicas da rede de superintendência conjunta.

Artigo 35.º

Poderes da autoridade fiscalizadora principal

1. Para efeitos da execução das funções definidas na presente secção, a autoridade fiscalizadora principal, no que diz respeito aos terceiros prestadores de serviços de TIC críticos, fica habilitada a:

a) Solicitar todas as informações e toda a documentação pertinentes nos termos do artigo 37.º;

b) Realizar investigações e inspeções de caráter geral nos termos dos artigos 38.º e 39.º, respetivamente;

c) Solicitar, após a conclusão das atividades de superintendência, relatórios que especifiquem as medidas que foram adotadas ou as correções que foram implementadas pelos terceiros prestadores de serviços de TIC críticos em relação às recomendações a que se refere a alínea d) do presente número;

d) Emitir recomendações nos domínios a que se refere o artigo 33.º, n.º 3, especialmente em relação aos seguintes elementos:

   i) utilização de requisitos ou processos de segurança e qualidade específicos no domínio das TIC, em especial no que respeita à introdução de correções, atualizações, encriptação e outras medidas de segurança que a autoridade fiscalizadora principal considere pertinentes para assegurar a segurança dos serviços prestados às entidades financeiras no domínio das TIC,

   ii) utilização de condições e termos, incluindo a respetiva execução técnica, ao abrigo dos quais o terceiro prestador de serviços de TIC crítico presta serviços de TIC às entidades financeiras e que a autoridade fiscalizadora principal considere pertinentes para prevenir que surjam falhas pontuais, a ampliação 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) qualquer subcontratação planeada, sempre que a autoridade fiscalizadora principal considere que essa subcontratação, incluindo acordos de subcontratação que os terceiros prestadores de serviços de TIC críticos planeiem celebrar com os terceiros prestadores de serviços de TIC ou com subcontratantes de TIC estabelecidos num país terceiro, pode acarretar riscos para a prestação dos serviços pela entidade financeira, ou para a estabilidade financeira, com base na análise da informação recolhida nos termos dos artigos 37.º e 38.º,

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

      — o subcontratante previsto é um terceiro prestador de serviços de TIC ou um subcontratante de TIC estabelecido num país terceiro,

      — a subcontratação diz respeito a funções críticas ou importantes da entidade financeira, e

— a autoridade fiscalizadora principal considera que o recurso a essa subcontratação representa um risco claro e grave para a estabilidade financeira da União ou para as entidades financeiras, nomeadamente para a capacidade de as entidades financeiras cumprirem os requisitos de supervisão.

Para efeitos da subalínea iv) da presente alínea, os terceiros prestadores de serviços de TIC utilizam o modelo a que se refere o artigo 41.º, n.º 1, alínea b), para transmitir à autoridade fiscalizadora principal as informações relativas à subcontratação.

2. No exercício dos poderes a que se refere o presente artigo, a autoridade fiscalizadora principal:

a) Assegura a coordenação periódica no âmbito da rede de superintendência conjunta e, em especial, procura adotar abordagens coerentes, conforme adequado, no que diz respeito à superintendência de terceiros prestadores de serviços de TIC críticos;

b) Tem devidamente em conta o quadro estabelecido pela Diretiva (UE) 2022/2555 e, se necessário, consulta as autoridades competentes pertinentes designadas ou criadas nos termos dessa diretiva, a fim de evitar uma duplicação de medidas técnicas e organizativas que possam ser aplicadas aos terceiros prestadores de serviços de TIC críticos nos termos dessa diretiva;

c) Procura minimizar, na medida do possível, o risco de perturbação dos serviços prestados por terceiros prestadores de serviços de TIC críticos a clientes que não sejam entidades abrangidas pelo âmbito de aplicação do presente regulamento.

3. A autoridade fiscalizadora principal consulta o fórum de superintendência antes de exercer os poderes referidos no n.º 1.

Antes de emitir recomendações nos termos do n.º 1, alínea d), a autoridade fiscalizadora principal dá ao terceiro prestador de serviços de TIC a oportunidade de fornecer, no prazo de 30 dias de calendário, informações pertinentes que demonstrem o impacto esperado para os clientes que não sejam entidades abrangidas pelo âmbito de aplicação do presente regulamento e, se for caso disso, apresentem soluções para atenuar os riscos.

4. A autoridade fiscalizadora principal informa a rede de superintendência conjunta do resultado do exercício de poderes a que se refere o n.º 1, alíneas a) e b). A autoridade fiscalizadora principal transmite, sem demora injustificada, os relatórios a que se refere o n.º 1, alínea c), à rede de superintendência conjunta e às autoridades competentes das entidades financeiras que utilizam os serviços de TIC prestados por esse terceiro prestador de serviços de TIC crítico.

5. Os terceiros prestadores de serviços de TIC críticos cooperam de boa-fé com a autoridade fiscalizadora principal e auxiliam-na no exercício das suas atribuições.

6. Em caso de incumprimento total ou parcial das medidas exigidas no âmbito do exercício dos poderes previstos no n.º 1, alíneas a), b) e c), e depois de decorrido um prazo de pelo menos 30 dias de calendário a contar da data em que o terceiro prestador de serviços de TIC crítico recebeu a notificação das respetivas medidas, a autoridade fiscalizadora principal adota uma decisão que impõe uma sanção pecuniária compulsória para obrigar o terceiro prestador de serviços de TIC crítico a cumprir essas medidas.

7. A sanção pecuniária compulsória que se refere o n.º 6 é imposta numa base diária até ao cumprimento efetivo das medidas, mas nunca por um período superior a seis meses a contar da notificação da decisão de imposição de uma sanção pecuniária compulsória ao terceiro prestador de serviços de TIC crítico.

8. O montante da sanção pecuniária compulsória, calculado a partir da data estipulada na decisão que a impõe, é de, no máximo, 1 % do volume de negócios mundial médio diário do terceiro prestador de serviços de TIC crítico no exercício anterior. Ao determinar o montante da sanção pecuniária, a autoridade fiscalizadora principal tem em conta, no que respeita ao incumprimento das medidas referido no n.º 6, os seguintes critérios:

a) A gravidade e a duração do incumprimento;

b) Se o incumprimento foi cometido com dolo ou por negligência;

c) O nível de cooperação do terceiro prestador de serviços de TIC com a autoridade fiscalizadora principal.

Para efeitos do primeiro parágrafo, a fim de assegurar uma abordagem coerente, a autoridade fiscalizadora principal procede a consultas da rede de superintendência conjunta.

9. As sanções pecuniárias são de natureza administrativa e executórias. A aplicação rege-se 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 para deliberar sobre as queixas relacionadas com irregularidades de aplicação. Os montantes das sanções pecuniárias são afetados ao orçamento geral da União Europeia.

10. A autoridade fiscalizadora principal divulga ao público todas as sanções pecuniárias compulsórias que tenham imposto, a menos que tal divulgação possa afetar gravemente os mercados financeiros ou causar danos desproporcionados aos interessados.

11. Antes de impor uma sanção pecuniária compulsória nos termos do n.º 6, a autoridade fiscalizadora principal dá aos representantes do terceiro prestador de serviços de TIC crítico objeto do processo a oportunidade de serem ouvidos sobre as conclusões e baseia as suas decisões exclusivamente nas conclusões em relação às quais o terceiro prestador de serviços de TIC crítico tenha tido oportunidade de se pronunciar.

Os direitos de defesa das pessoas objeto do processo são plenamente respeitados no decurso do processo. O terceiro prestador de serviços de TIC crítico objeto do processo tem o direito de 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 36.º

Exercício de poderes pela autoridade fiscalizadora principal fora da União

1. Quando os objetivos em matéria de superintendência não puderem ser alcançados por meio da interação com a filial criada para efeitos do artigo 31.º, n.º 12, ou do exercício de atividades de superintendência em instalações situadas na União, a autoridade fiscalizadora principal pode exercer os poderes referidos nas disposições seguintes, em quaisquer instalações situadas num país terceiro que sejam propriedade de um terceiro prestador de serviços de TIC crítico, ou utilizadas de alguma forma para efeitos da prestação de serviços a entidades financeiras da União por esse prestador, no que diz respeito às suas operações comerciais, funções ou serviços, incluindo quaisquer escritórios, instalações, terrenos e edifícios administrativos, comerciais ou operacionais ou outros imóveis:

a) No artigo 35.º, n.º 1, alínea a); e

b) No artigo 35.º, n.º 1, alínea b), nos termos do artigo 38.º, n.º 2, alíneas a), b) e d), no artigo 39.º, n.º 1, e no artigo 39.º, n.º 2, alínea a).

Os poderes a que se refere o primeiro parágrafo podem ser exercidos, sob reserva de todas as seguintes condições:

i) a autoridade fiscalizadora principal considerar necessário realizar uma inspeção num país terceiro a fim de poder desempenhar plena e eficazmente as suas obrigações ao abrigo do presente regulamento,

ii) a inspeção num país terceiro estiver diretamente relacionada com a prestação de serviços de TIC a entidades financeiras na União,

iii) o terceiro prestador de serviços de TIC crítico consentir na realização de uma inspeção num país terceiro, e

iv) a autoridade competente do país terceiro em causa for oficialmente notificada pela autoridade fiscalizadora principal e não levantar objeções.

2. Sem prejuízo das respetivas competências das instituições da União e dos Estados-Membros, para efeitos do n.º 1, a EBA, a ESMA ou a EIOPA, celebram acordos de cooperação administrativa com a autoridade pertinente do país terceiro, a fim de permitir a boa realização de inspeções no país terceiro em causa pela autoridade fiscalizadora principal e pela equipa por si designada para realizar a sua missão nesse país terceiro. Estes acordos de cooperação não criam obrigações jurídicas no que respeita à União e aos seus Estados-Membros nem impedem os Estados-Membros e as suas autoridades competentes de celebrarem acordos bilaterais ou multilaterais com esses países terceiros e com as suas autoridades pertinentes.

Além disso, especificam, pelo menos, os seguintes elementos:

a) Os procedimentos para a coordenação das atividades de superintendência realizadas ao abrigo do presente regulamento e de qualquer monitorização análoga do risco associado às TIC devido a terceiros no setor financeiro efetuada pela autoridade competente do país terceiro em causa, incluindo os pormenores da transmissão do acordo desta última a fim de permitir a realização, pela autoridade fiscalizadora principal e pela equipa por si designada, das investigações gerais e inspeções no local a que se refere o n.º 1, primeiro parágrafo, no território sob a sua jurisdição;

b) O mecanismo de transmissão de todas as informações relevantes entre a EBA, a ESMA ou a EIOPA, e a autoridade pertinente do país terceiro em causa, em especial no que se refere às informações que possam ser solicitadas pela autoridade fiscalizadora principal nos termos do artigo 37.º;

c) Os mecanismos de notificação imediata pela autoridade pertinente do país terceiro em causa à EBA, à ESMA ou à EIOPA, dos casos em que se considere que um terceiro prestador de serviços de TIC estabelecido num país terceiro e designado como crítico nos termos do artigo 31.º, n.º 1, alínea a), infringiu os requisitos que é obrigado a respeitar por força do direito aplicável no país terceiro em causa aquando da prestação de serviços a instituições financeiras nesse país terceiro, bem como as vias de recurso e as sanções aplicadas;

d) A transmissão periódica de atualizações sobre a evolução em matéria de regulamentação ou supervisão no que diz respeito à monitorização do risco associado às TIC devido a terceiros nas instituições financeiras no país terceiro em causa;

e) As modalidades que possibilitem, se necessário, a participação de um representante da autoridade competente do país terceiro nas inspeções realizadas pela autoridade fiscalizadora principal e pela equipa por si designada.

3. Quando a autoridade fiscalizadora principal não estiver em condições de realizar atividades de superintendência fora da União, a que se referem os n.os 1 e 2, a autoridade fiscalizadora principal:

a) Exerce os poderes que lhe são conferidos pelo artigo 35.º com base em todos os factos e documentos à sua disposição;

b) Documenta e explica quaisquer consequências da sua incapacidade para realizar as atividades de superintendência previstas a que se refere o presente artigo.

As potenciais consequências a que se refere a alínea b) do presente número são tidas em conta nas recomendações da autoridade fiscalizadora principal emitidas nos termos do artigo 35.º, n.º 1, alínea d).

Artigo 37.º

Pedidos de informações

1. A autoridade fiscalizadora principal pode solicitar aos terceiros prestadores de serviços de TIC críticos, através de um pedido simples ou de uma decisão, que forneçam todas as informações necessárias para que a autoridade fiscalizadora principal possa cumprir as suas obrigações ao abrigo do presente regulamento, nomeadamente todos os documentos comerciais ou operacionais, contratos, políticas, documentação, 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 às quais o terceiro prestador de serviços de TIC crítico tenha subcontratado funções ou atividades operacionais.

2. Ao enviar um simples pedido de informações nos termos do n.º 1, a autoridade fiscalizadora principal:

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

b) Indica a finalidade do pedido;

c) Especifica as informações solicitadas;

d) Fixa um prazo para a prestação das informações;

e) Informa o representante do terceiro prestador de serviços de TIC crítico ao qual as informações são solicitadas de que não é obrigado a fornecê-las mas que, caso aceda voluntariamente ao pedido, as informações prestadas não podem ser incorretas nem induzir em erro.

3. Ao solicitar, mediante uma decisão, que lhe sejam fornecidas informações nos termos do n.º 1, a autoridade fiscalizadora principal:

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

b) Indica a finalidade do pedido;

c) Especifica as informações solicitadas;

d) Fixa um prazo para a prestação das informações;

e) Faz referência às sanções pecuniárias compulsórias previstas no artigo 35.º, n.º 6, no caso de as informações prestadas serem incompletas ou não serem fornecidas no prazo referido na alínea d) do presente número;

f) Menciona o direito a recorrer da decisão junto da Câmara de Recurso das AES e o direito de requerer a apreciação da decisão pelo Tribunal de Justiça da União Europeia (Tribunal de Justiça) nos termos dos artigos 60.º e 61.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1094/2010 e (UE) n.º 1095/2010.

4. Os representantes dos terceiros prestadores de serviços de TIC críticos fornecem as informações solicitadas. Os advogados devidamente mandatados podem fornecer as informações pedidas em nome dos seus mandantes. O terceiro prestador de serviços de TIC crítico é plenamente responsável em caso de prestação de informações incompletas, incorretas ou que induzam em erro.

5. A autoridade fiscalizadora principal transmite, sem demora, uma cópia da decisão de fornecer informações às autoridades competentes das entidades financeiras que utilizam os serviços dos respetivos terceiros prestadores de serviços de TIC críticos, bem como à rede de superintendência conjunta.

Artigo 38.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 conjunta a que se refere o artigo 40.º, n.º 1, pode, sempre que necessário, realizar as investigações junto dos terceiros prestadores de serviços de TIC críticos;

2. A autoridade fiscalizadora principal dispõe de poderes para:

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

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

c) Convocar representantes dos terceiros prestadores de serviços de TIC críticos 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 consintam em ser inquiridas a fim de recolher informações relacionadas com o objeto de uma investigação;

e) Requerer a apresentação de registos telefónicos e dados de tráfego.

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 indica também as sanções pecuniárias compulsórias previstas no artigo 35.º, n.º 6, sempre que a apresentação dos registos, dados, procedimentos documentados ou qualquer outro material solicitados, ou as respostas às perguntas feitas aos representantes do terceiro prestador de serviços de TIC, não forem fornecidas ou estiverem incompletas.

4. Os representantes dos terceiros prestadores de serviços de TIC críticos são obrigados a colaborar com as investigações com base numa decisão da autoridade fiscalizadora principal. A decisão especifica o objeto e a finalidade da investigação, as sanções pecuniárias compulsórias previstas no artigo 35.º, n.º 6, 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 ao início da investigação, a autoridade fiscalizadora principal informa as autoridades competentes das entidades financeiras que recorrem aos serviços de TIC prestados pelo terceiro prestador de serviços de TIC crítico da investigação e da identidade das pessoas autorizadas.

A autoridade fiscalizadora principal comunica à rede de superintendência conjunta todas as informações transmitidas nos termos do primeiro parágrafo.

Artigo 39.º

Inspeções

1. A fim de cumprir as suas obrigações ao abrigo do presente regulamento, a autoridade fiscalizadora principal, auxiliada pelas equipas de avaliação conjunta a que se refere o artigo 40.º, n.º 1, pode entrar e realizar as necessárias inspeções no local em qualquer uma das instalações comerciais, terrenos ou propriedades dos terceiros prestadores de serviços de TIC, tais como sedes, centros de operações e instalações secundárias, bem como realizar inspeções à distância.

Para efeitos do exercício de poderes a que se refere o primeiro parágrafo, a autoridade fiscalizadora principal consulta a rede de superintendência conjunta.

2. Os funcionários e outras pessoas autorizadas pela autoridade fiscalizadora principal para realizar uma inspeção no local dispõem de poderes para:

a) Entrar em quaisquer dessas instalações comerciais, terrenos ou propriedades; e

b) Selar quaisquer dessas instalações comerciais, livros ou registos, durante o período da inspeção e na medida do necessário à inspeção.

Os funcionários e outras pessoas autorizadas pela autoridade fiscalizadora principal podem exercer esses poderes mediante a apresentação de uma autorização escrita que especifique o objeto e a finalidade da inspeção e as sanções pecuniárias compulsórias previstas no artigo 35.º, n.º 6, quando os representantes dos terceiros prestadores de serviços de TIC críticos não colaborarem com a investigação.

3. Com a devida antecedência em relação ao início da inspeção, a autoridade fiscalizadora principal informa as autoridades competentes das entidades financeiras que recorrem a esse terceiro prestador de serviços de TIC.

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

5. Antes de qualquer inspeção planeada ao local, a autoridade fiscalizadora principal notifica com antecedência razoável os terceiros prestadores de serviços de TIC críticos, 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. O terceiro prestador de serviços de TIC crítico colabora com as inspeções no local ordenadas por decisão da autoridade fiscalizadora principal. A decisão especifica o objeto e a finalidade da inspeção, fixa a data em que se deve iniciar a inspeção e indica as sanções pecuniárias compulsórias previstas no artigo 35.º, n.º 6, 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.

7. Quando os funcionários e outras pessoas autorizadas pela autoridade fiscalizadora principal constatarem que um terceiro prestador de serviços de TIC crítico se opõe a uma inspeção ordenada nos termos do presente artigo, a autoridade fiscalizadora principal informa o terceiro prestador de serviços de TIC crítico das consequência dessa oposição, nomeadamente da possibilidade de as autoridades competentes das entidades financeiras requererem que as entidades financeiras pertinentes rescindam os contratos celebrados com esse terceiro prestador de serviços de TIC crítico.

Artigo 40.º

Superintendência contínua

1. Aquando da realização de atividades de superintendência, em especial investigações de caráter geral ou inspeções, a autoridade fiscalizadora principal é auxiliada por uma equipa de avaliação conjunta criada para cada terceiro prestador de serviços de TIC crítico.

2. A equipa de avaliação conjunta a que se refere o n.º 1 é composta por membros do pessoal oriundos:

a) Das AES;

b) Das autoridades competentes pertinentes que supervisionam as entidades financeiras às quais o terceiro prestador de serviços de TIC crítico presta serviços;

c) Da autoridade nacional competente a que se refere o artigo 32.º, n.º 4, alínea e), numa base voluntária;

d) De uma autoridade nacional competente do Estado-Membro em que está estabelecido terceiro prestador de serviços de TIC crítico, numa base voluntária.

Os membros da equipa de avaliação conjunta devem ter conhecimentos especializados em questões relacionadas com as TIC e em matéria de risco operacional. A equipa de avaliação conjunta trabalha sob a coordenação de um membro do pessoal da autoridade fiscalizadora principal designada (o «coordenador da autoridade fiscalizadora principal»).

3. No prazo de três meses a contar da conclusão de uma investigação ou inspeção, a autoridade fiscalizadora principal, após consulta do fórum de superintendência, adota recomendações a dirigir ao terceiro prestador de serviços de TIC crítico ao abrigo dos poderes referidos no artigo 35.º.

4. As recomendações referidas no n.º 3 são comunicadas imediatamente ao terceiro prestador de serviços de TIC crítico e às autoridades competentes das entidades financeiras às quais aquele presta serviços de TIC.

Para efeitos da realização das atividades de superintendência, a autoridade fiscalizadora principal pode tomar em consideração quaisquer certificações pertinentes de terceiros ou relatórios de auditorias internas ou externas de terceiros no domínio das TIC disponibilizadas pelo terceiro prestador de serviços de TIC críticos.

Artigo 41.º

Harmonização das condições que permitem o exercício de atividades de superintendência

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

a) As informações que devem ser facultadas por um terceiro prestador de serviços de TIC no pedido de designação voluntária como crítico previsto no artigo 31.º, n.º 11;

b) O conteúdo, a estrutura e o formato das informações a apresentar, divulgar ou comunicar pelos terceiros prestadores de serviços de TIC nos termos do artigo 35.º, n.º 1, incluindo o modelo para fornecer informações sobre acordos de subcontratação;

c) Os critérios para determinar a composição da equipa de avaliação conjunta, assegurando uma participação equilibrada de membros do pessoal das AES e das autoridades competentes pertinentes, a sua designação, as suas atribuições e modalidades de trabalho;

d) Os pormenores da avaliação pelas autoridades competentes das medidas tomadas pelos terceiros prestadores de serviços de TIC críticos com base nas recomendações da autoridade fiscalizadora principal nos termos do artigo 42.º, n.º 3.

2. As AES apresentam esses projetos de normas técnicas de regulamentação à Comissão até 17 de julho de 2024.

A Comissão fica habilitada a completar o presente regulamento através da adoção das normas técnicas de regulamentação a que se refere o n.º 1, nos termos do procedimento previsto nos 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 42.º

Acompanhamento pelas autoridades competentes

1. No prazo de 60 dias de calendário a contar da receção das recomendações emitidas pela autoridade fiscalizadora principal nos termos do artigo 35.º, n.º 1, alínea d), os terceiros prestadores de serviços de TIC críticos notificam a autoridade fiscalizadora principal da sua intenção de seguir as recomendações ou apresentam uma explicação fundamentada para o não fazer. A autoridade fiscalizadora principal transmite imediatamente essa informação às autoridades competentes das entidades financeiras em causa.

2. A autoridade fiscalizadora principal torna públicos os casos em que um terceiro prestador de serviços de TIC crítico não notifica a autoridade fiscalizadora principal nos termos do n.º 1 ou quando a explicação apresentada pelo terceiro prestador de serviços de TIC crítico não for suficiente. As informações publicadas incluem a identidade do terceiro prestador de serviços de TIC crítico, bem como informações sobre o tipo e a natureza do incumprimento. Essas informações devem limitar-se ao que é relevante e proporcionado para efeitos de alertar o público, a menos que essa publicação possa causar danos desproporcionados às partes envolvidas ou comprometer gravemente o bom funcionamento e a integridade dos mercados financeiros ou a estabilidade da totalidade ou de parte do sistema financeiro da União.

A autoridade fiscalizadora principal notifica o terceiro prestador de serviços de TIC dessa divulgação de informações ao público.

3. As autoridades competentes informam as entidades financeiras pertinentes dos riscos identificados nas recomendações dirigidas aos terceiros prestadores de serviços de TIC críticos, nos termos do artigo 35.º, n.º 1, alínea d).

Ao gerirem o risco associado às TIC devido a terceiros, as entidades financeiras têm em consideração os riscos a que se refere o primeiro parágrafo.

4. Sempre que uma autoridade competente considere que uma entidade financeira não tem em consta ou não aborda suficientemente, no âmbito da sua gestão do risco associado às TIC devido a terceiros, os riscos específicos identificados nas recomendações, notifica a entidade financeira da possibilidade de ser tomada uma decisão, no prazo de 60 dias de calendário a contar da receção dessa notificação, nos termos do n.º 6, na ausência de acordos contratuais adequadas destinadas a fazer face a esses riscos.

5. Após receberem as comunicações referidas no artigo 35.º, n.º 1, alínea c), e antes de tomarem a decisão a que se refere o n.º 6 do presente artigo, as autoridades competentes podem, a título voluntário, consultar as autoridades competentes designadas ou criadas nos termos da Diretiva (UE) 2022/2555, responsáveis pela supervisão de uma entidade essencial ou importante abrangida por essa diretiva, que tenha sido designado como terceiro prestador de serviços de TIC crítico.

6. As autoridades competentes podem, como medida de último recurso, na sequência da notificação e, se for caso disso, da consulta prevista nos n.ºs 4 e 5 do presente artigo, nos termos do artigo 50.º, tomar uma decisão exigindo que as entidades financeiras suspendam temporariamente, em parte ou na totalidade, a utilização ou o lançamento de um serviço prestado pelo terceiro prestador de serviços de TIC crítico até que os riscos identificados nas recomendações dirigidas aos terceiros prestadores de serviços de TIC críticos tenham sido abordados. Quando necessário, podem exigir que as entidades financeiras rescindam, em parte ou na totalidade, os acordos contratuais pertinentes celebrados com os terceiros prestadores de serviços de TIC críticos.

7. Caso um terceiro prestador de serviços de TIC crítico se recuse a acatar recomendações baseando-se numa abordagem divergente da recomendada pela autoridade fiscalizadora principal, e essa abordagem divergente seja suscetível de ter um impacto negativo num grande número de entidades financeiras, ou numa parte significativa do setor financeiro, e os alertas individuais emitidos pelas autoridades competentes não tenham resultado em abordagens coerentes que atenuem o potencial risco para a estabilidade financeira, a autoridade fiscalizadora principal pode, após consulta do fórum de superintendência, emitir pareceres não vinculativos e não públicos dirigidos às autoridades competentes, a fim de promover medidas de acompanhamento da supervisão coerentes e convergentes, conforme adequado.

8. Após receberem os relatórios referidos no artigo 35.º, n.º 1, alínea c), as autoridades competentes, ao tomarem as decisões referidas no n.º 6 do presente artigo, têm em conta o tipo e a dimensão do risco que não foi abordado pelo terceiro prestador de serviços de TIC crítico, 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 do terceiro prestador de serviços de TIC crítico;

c) Se o incumprimento facilitou, ocasionou ou esteve de alguma forma associado a um ato de criminalidade financeira;

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

e) Se a suspensão ou rescisão dos acordos contratuais comporta um risco para a continuidade das operações comerciais da entidade financeira, não obstante os esforços da entidade financeira no sentido de evitar perturbações na prestação dos seus serviços;

f) Se for caso disso, o parecer das autoridades competentes designadas ou criadas nos termos da Diretiva (UE) 2022/2555, responsáveis pela supervisão de uma entidade essencial ou importante abrangida por essa diretiva, que tenha sido designado como terceiro prestador de serviços de TIC crítico, solicitado numa base voluntária nos termos do n.º 5 do presente artigo.

As autoridades competentes concedem às entidades financeiras o período de tempo necessário para que possam ajustar os acordos contratuais celebrados com terceiros prestadores de serviços de TIC críticos, a fim de evitar efeitos negativos para a sua resiliência operacional digital e de lhes permitir implementar as estratégias de saída e os planos de transição a que se refere o artigo 28.º.

9. A decisão a que se refere o n.º 6 do presente artigo é notificada aos membros do fórum de superintendência a que se refere o artigo 32.º, n.º 4, alíneas a), b) e c), e à rede de superintendência conjunta.

Os terceiros prestadores de serviços de TIC críticos visados pelas decisões previstas no n.º 6 cooperam plenamente com as entidades financeiras afetadas, em especial no contexto do processo de suspensão ou rescisão dos seus acordos contratuais.

10. As autoridades competentes informam regularmente a autoridade fiscalizadora principal das abordagens e medidas adotadas no âmbito das suas atribuições de supervisão em relação às entidades financeiras, bem como dos acordos contratuais celebrados pelas entidades financeiras quando os terceiros prestadores de serviços de TIC críticos não tiverem acatado, em parte ou na totalidade, as recomendações que lhes foram dirigidas pela autoridade fiscalizadora principal.

11. A autoridade fiscalizadora principal pode, a pedido, prestar esclarecimentos adicionais sobre as recomendações emitidas a fim de fornecer orientações às autoridades competentes sobre as medidas de acompanhamento.

Artigo 43.º

Taxas de superintendência

1. A autoridade fiscalizadora principal, em conformidade com o ato delegado a que se refere o n.º 2 do presente artigo, cobra aos terceiros prestadores de serviços de TIC críticos taxas que cubram na totalidade as despesas necessárias para que a autoridade fiscalizadora principal exerça as suas atribuições de superintendência nos termos do presente regulamento, nomeadamente o reembolso de eventuais custos em que possa incorrer em resultado do trabalho realizado pela equipa de avaliação conjunta a que se refere o artigo 40.º, bem como os custos do aconselhamento prestado pelos peritos independentes a que se refere o artigo 32.º, n.º 4, segundo parágrafo, em relação a questões relacionadas com as atividades de superintendência direta.

O montante de uma taxa cobrada a um terceiro prestador de serviços de TIC crítico cobre todos os custos decorrentes do cumprimento dos deveres previstos na presente secção e é proporcional ao seu volume de negócios.

2. A Comissão fica habilitada a adotar um ato delegado nos termos do artigo 57.º para completar o presente regulamento determinando o montante das taxas e as modalidades de pagamento até 17 de julho de 2024.

Artigo 44.º

Cooperação internacional

1. Sem prejuízo do disposto no artigo 36.º, a EBA, a ESMA e a EIOPA podem, nos termos do artigo 33.º dos Regulamentos (UE) n.º 1093/2010, (UE) n.º 1095/2010 e (UE) n.º 1094/2010, respetivamente, celebrar acordos administrativos com autoridades de regulamentação e de supervisão de países terceiros para fomentar a cooperação internacional em matéria de risco associado às TIC devido a terceiros nos diferentes setores financeiros, em especial desenvolvendo boas práticas para a apreciação das práticas e dos controlos de gestão do risco associado às TIC, das medidas de mitigação e da resposta aos incidentes nesse contexto.

2. As AES, através do Comité Conjunto, apresentam, de cinco em cinco anos, 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 a que se refere o n.º 1, centrados na evolução do risco associados às TIC devido a terceiros e nas suas implicações para a estabilidade financeira, a integridade do mercado, a proteção dos investidores e o funcionamento do mercado interno.

CAPITULO VI

Acordos de partilha de informações

Artigo 45.º

Acordos de partilha de informações específicas e sensíveis relativas a ciberataques

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

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

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

c) Seja implementada através de acordos de partilha de informações que protejam a natureza potencialmente sensível das informações partilhadas e que se pautem por regras de conduta que respeitem totalmente a confidencialidade comercial, a proteção dos dados pessoais, nos termos do Regulamento (UE) 2016/679, e as orientações sobre a política de concorrência.

2. Para efeitos do n.º 1, alínea c), os acordos de partilha de informações definem as condições de participação e, se for caso disso, as modalidades do envolvimento das autoridades públicas e a capacidade em que estas podem estar associadas aos acordos de partilha de informações, do envolvimento dos terceiros prestadores de serviços de TIC e dos elementos operacionais, nomeadamente a utilização de plataformas TIC dedicadas.

3. As entidades financeiras notificam as autoridades competentes da sua participação nos acordos de partilha de informações a que se refere o n.º 1, após validação dessa mesma participação ou, quando aplicável, após a cessação da sua participação, assim que esta produza efeitos.

CAPITULO VII

Autoridades competentes

Artigo 46.º

Autoridades competentes

Sem prejuízo das disposições relativas ao quadro de superintendência dos terceiros prestadores de serviços de TIC críticos a que se refere o capítulo V, secção II, do presente regulamento, o cumprimento do presente regulamento é assegurado pelas seguintes autoridades competentes em conformidade com os poderes conferidos pelos respetivos atos jurídicos:

a) No caso das instituições de crédito e das instituições isentas nos termos da Diretiva 2013/36/UE, a autoridade competente designada nos termos do artigo 4.º dessa diretiva, e no caso das instituições de crédito classificadas como significativas nos termos do artigo 6.º, n.º 4, do Regulamento (UE) n.º 1024/2013, o BCE, de acordo com os poderes e atribuições conferidos por esse regulamento;

b) No caso das instituições de pagamento, incluindo instituições de pagamento isentas nos termos da Diretiva (UE) 2015/2366, das instituições de moeda eletrónica, incluindo as que estão isentas nos termos da Diretiva 2009/110/CE, e dos prestadores de serviços de informação sobre contas referidos no artigo 33.º, n.º 1, da Diretiva (UE) 2015/2366, a autoridade competente designada nos termos do artigo 22.º da Diretiva (UE) 2015/2366;

c) No caso das empresas de investimento, a autoridade competente designada nos termos do artigo 4.º da Diretiva (UE) 2019/2034 do Parlamento Europeu e do Conselho ([38]);

d) No caso dos prestadores de serviços de criptoativos autorizados ao abrigo do regulamento relativo aos mercados de criptoativos e dos emitentes de criptofichas (tokens) referenciadas a ativos, a autoridade competente designada nos termos da disposição pertinente desse regulamento;

e) No caso das centrais de valores mobiliários, a autoridade competente designada nos termos do artigo 11.º do Regulamento (UE) n.º 909/2014;

f) No caso das contrapartes centrais, a autoridade competente designada nos termos do artigo 22.º do Regulamento (UE) n.º 648/2012;

g) No caso das plataformas de negociação e dos prestadores de serviços de comunicação de dados, a autoridade competente designada nos termos do artigo 67.º da Diretiva 2014/65/UE, e a autoridade competente na aceção do artigo 2.º, n.º 1, ponto 18, do Regulamento (UE) n.º 600/2014;

h) No caso dos repositórios de transações, a autoridade competente designada nos termos do artigo 55.º do Regulamento (UE) n.º 648/2012;

i) No caso dos gestores de fundos de investimento alternativos, a autoridade competente designada nos termos do artigo 44.º da Diretiva 2011/61/UE;

j) No caso das sociedades gestoras, a autoridade competente designada nos termos do artigo 97.º da Diretiva 2009/65/CE;

k) No caso das empresas de seguros e resseguros, a autoridade competente designada nos termos do artigo 30.º da Diretiva 2009/138/CE;

l) No caso dos mediadores de seguros, mediadores de resseguros e mediadores de seguros a título acessório, a autoridade competente designada nos termos do artigo 12.º da Diretiva (UE) 2016/97;

m) No caso das instituições de realização de planos de pensões profissionais, a autoridade competente designada nos termos do artigo 47.º da Diretiva (UE) 2016/2341;

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

o) No caso dos administradores de índices de referência críticos, a autoridade competente designada nos termos dos artigos 40.º e 41.º do Regulamento (UE) 2016/1011;

([38]) Diretiva (UE) 2019/2034 do Parlamento Europeu e do Conselho, de 27 de novembro de 2019, relativa à supervisão prudencial das empresas de investimento e que altera as Diretivas 2002/87/CE, 2009/65/CE, 2011/61/UE, 2013/36/UE, 2014/59/UE e 2014/65/UE (JO L 314 de 5.12.2019, p. 64).

p) No caso dos prestadores de serviços de financiamento colaborativo, a autoridade competente designada nos termos do artigo 29.º do Regulamento (UE) 2020/1503;

q) No caso dos repositórios de titularizações, a autoridade competente designada nos termos do artigo 10.º e do artigo 14.º, n.º 1, do Regulamento (UE) 2017/2402.

Artigo 47.º

Cooperação com as estruturas e autoridades estabelecidas pela Diretiva (UE) 2022/2555

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 14.º da Diretiva (UE) 2022/2555, as AES e as autoridades competentes podem participar nas atividades do grupo de cooperação relativos a assuntos que digam respeito às suas atividades de supervisão em relação às entidades financeiras. As AES e as autoridades competentes podem solicitar participar nas atividades do grupo de cooperação que estejam relacionados com as entidades essenciais ou importantes abrangidas pela Diretiva (UE) 2022/2555 que também tenham sido designadas terceiros prestadores de serviços de TIC críticos nos termos do artigo 31.º do presente regulamento.

2. Se for caso disso, as autoridades competentes podem consultar e partilhar informações com os pontos de contacto únicos e as CSIRT designados ou criados nos termos da Diretiva (UE) 2022/2555.

3. Se for caso disso, as autoridades competentes podem solicitar qualquer aconselhamento e assistência técnica pertinentes às autoridades competentes designadas ou criadas nos termos da Diretiva (UE) 2022/2555 e estabelecer mecanismos de cooperação que permitam a criação de mecanismos de coordenação eficazes e de resposta rápida.

4. Os mecanismos a que se refere o n.º 3 do presente artigo podem, nomeadamente, especificar os procedimentos relativos à coordenação, respetivamente, das atividades de supervisão e de superintendência, em relação a entidades essenciais ou importantes abrangidas pela Diretiva (UE) 2022/2555 que tenham sido designadas terceiros prestadores de serviços de TIC críticos nos termos do artigo 31.º do presente regulamento, inclusive no que diz respeito à realização, nos termos do direito nacional, de investigações e inspeções no local, bem como aos mecanismos de intercâmbio de informações entre as autoridades competentes ao abrigo do presente regulamento e as autoridades competentes designadas ou criadas nos termos dessa diretiva, o que inclui o acesso às informações solicitadas por essas últimas autoridades.

Artigo 48.º

Cooperação entre autoridades

1. As autoridades competentes cooperam estreitamente entre si e, se for caso disso, com a autoridade fiscalizadora principal.

2. As autoridades competentes e a autoridade fiscalizadora principal trocam entre si, em tempo útil, todas as informações pertinentes relativas aos terceiros prestadores de serviços de TIC críticos que lhes sejam necessárias para cumprirem as suas obrigações ao abrigo do presente regulamento, em especial no que diz respeito aos riscos identificados, às abordagens e às medidas tomadas no âmbito das atribuições de superintendência da autoridade fiscalizadora principal.

Artigo 49.º

Exercícios, comunicação e cooperação transetorial no domínio financeiro

1. As AES, através do Comité Conjunto e em colaboração com as autoridades competentes, as autoridades de resolução a que se refere o artigo 3.º da Diretiva 2014/59/UE, o BCE, o Conselho Único de Resolução, no que respeita às informações relativas às entidades abrangidas pelo âmbito de aplicação do Regulamento (UE) n.º 806/2014, o CERS e a ENISA, conforme adequado, 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 ciber-riscos 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 de caráter severo transfronteiriço relacionado com as TIC ou caso uma ameaça conexa possa ter um impacto sistémico no setor financeiro da União no seu conjunto.

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

2. As autoridades competentes, as AES e o BCE cooperam estreitamente entre si e procedem ao intercâmbio de informações para efeitos do cumprimento das suas obrigações nos termos dos artigos 47.º a 54.º. As autoridades competentes coordenam estreitamente a sua supervisão de modo a identificarem e corrigirem as violações do 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 50.º

Sanções administrativas e medidas corretivas

1. As autoridades competentes estão 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, o seguinte:

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) Realizar inspeções ou investigações no local, que incluem, nomeadamente:

   i) convocar representantes das entidades financeiras 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,

   ii) inquirir quaisquer outras pessoas singulares ou coletivas que consintam em ser inquiridas a fim de recolher informações relacionadas com o objeto de uma investigação;

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 nos termos do artigo 52.º, os Estados-Membros estipulam regras que estabeleçam sanções administrativas e medidas corretivas adequadas em caso de violação do presente regulamento e asseguram a sua aplicação efetiva.

As referidas sanções ou medidas são eficazes, proporcionadas e dissuasivas.

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

a) Emitir uma injunção que exija à pessoa singular ou coletiva que cesse a conduta que constitui uma violação do presente regulamento e se abstenha de a repetir;

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

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

d) Exigir, na medida em que o direito nacional o permita, os registos existentes do tráfego de dados detidos por um operador de telecomunicações, se houver motivos razoáveis para suspeitar de uma violação do presente regulamento e se esses registos puderem ser relevantes para uma investigação dessas 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 o n.º 2, alínea c), e o n.º 4 forem 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 asseguram 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 51.º

Exercício do poder de aplicar sanções administrativas e medidas corretivas

1. As autoridades competentes exercem os poderes para impor as sanções administrativas e as medidas corretivas a que se refere o artigo 50.º em conformidade com os respetivos regimes jurídicos nacionais, se for caso disso, da seguinte forma:

a) Diretamente;

b) Em colaboração com outras autoridades;

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

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 50.º, as autoridades competentes têm 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) A dimensão, 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 singular ou coletiva;

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

Artigo 52.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 violação do presente regulamento, os Estados-Membros asseguram 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 por violação 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 53.º

Deveres de notificação

Os Estados-Membros notificam à Comissão, à ESMA, à EBA e à EIOPA até 17 de janeiro de 2025 as disposições legislativas, regulamentares e administrativas que dão execução ao presente capítulo, incluindo quaisquer disposições de direito penal aplicáveis. Os Estados-Membros notificam à Comissão, à ESMA, à EBA e à EIOPA, sem demora injustificada, quaisquer alterações subsequentes dessas disposições.

Artigo 54.º

Publicação das sanções administrativas

1. As autoridades competentes publicam nos respetivos sítios Web oficiais, sem demora injustificada, qualquer decisão que imponha uma sanção administrativa não passível de recurso depois de o destinatário da sanção ter sido notificado dessa decisão.

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

3. Quando a autoridade competente, no seguimento de uma avaliação casuística, considerar que a publicação da identidade, no caso das pessoas coletivas, ou da identidade e dos dados pessoais, no caso de pessoas singulares, pode ser desproporcionada, inclusive comportando riscos no que respeita à proteção dos dados pessoais, 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 adota uma das seguintes soluções em relação à decisão que impõe uma sanção administrativa:

a) Adiar a sua publicação até 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 clemência da sanção imposta.

4. Caso se decida pela publicação anónima de uma sanção administrativa, nos termos do 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 publicam 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 asseguram que todas as publicações referidas nos n.os 1 a 4 permanecem no seu sítio Web oficial apenas durante o período necessário para que o presente artigo produza efeitos. Este período não pode exceder cinco anos a contar da sua publicação.

Artigo 55.º

Segredo profissional

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

2. Todas as pessoas que trabalhem ou tenham trabalhado por conta de autoridades competentes nos termos 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 segredo profissional.

3. As informações abrangidas pelo segredo profissional, incluindo o intercâmbio de informações entre as autoridades competentes ao abrigo do presente regulamento e as autoridades competentes designadas ou criadas nos termos da Diretiva (UE) 2022/2555, 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 segredo 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.

Artigo 56.º

Proteção de dados

1. As AES e as autoridades competentes só estão autorizadas a tratar dados pessoais se tal for necessário para o exercício das obrigações e deveres que lhes incumbem por força do presente regulamento, em especial em matéria de investigação, inspeção, pedidos de informação, comunicação, publicação, avaliação, verificação, avaliação e elaboração de planos de superintendência. Os dados pessoais são tratados nos termos do Regulamento (UE) 2016/679 ou do Regulamento (UE) 2018/1725, consoante o que for aplicável.

2. Salvo disposição em contrário noutros atos setoriais, os dados pessoais a que se refere o n.º 1 são conservados até ao cumprimento das funções de supervisão aplicáveis e, em qualquer caso, por um período máximo de 15 anos, exceto no caso de processos judiciais pendentes que exijam a conservação ulterior desses dados.

CAPÍTULO VIII

Atos delegados

Artigo 57.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 31.º, n.º 6, e no artigo 43.º, n.º 2, é conferido à Comissão por um prazo de cinco anos a contar de 17 de janeiro de 2024. 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 31.º, n.º 6, e no artigo 43.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 nos termos do artigo 31.º, n.º 6, e do artigo 43.º, n.º 2, só entram em vigor se não tiverem sido formuladas objeções pelo Parlamento Europeu ou pelo Conselho no prazo de três meses a contar da notificação do ato ao Parlamento Europeu e ao Conselho, ou se, antes do termo desse prazo, o Parlamento Europeu e o Conselho tiverem informado a Comissão de que não têm objeções a formular. O referido prazo é prorrogável por três meses por iniciativa do Parlamento Europeu ou do Conselho.

CAPÍTULO IX

Disposições transitórias e finais

Secção I

Artigo 58.º

Cláusula de revisão

1. Até 17 de janeiro de 2028, a Comissão, após consulta das AES e do CERS, conforme adequado, procede a uma revisão e apresenta um relatório ao Parlamento Europeu e ao Conselho, acompanhado, se necessário, de uma proposta legislativa. A revisão inclui, pelo menos, os seguintes elementos:

a) Os critérios aplicáveis à designação dos terceiros prestadores de serviços de TIC críticos nos termos do artigo 31.º, n.º 2;

b) A natureza voluntária da notificação de ciberameaças significativas a que se refere o artigo 19.º;

c) O regime a que se refere o artigo 31.º, n.º 12, e os poderes da autoridade fiscalizadora principal previstos no artigo 35.º, n.º 1, alínea d), subalínea iv), primeiro travessão, a fim de avaliar a eficácia dessas disposições no que diz respeito à garantia de uma superintendência eficaz dos terceiros prestadores de serviços de TIC críticos estabelecidos num país terceiro, bem como a necessidade de estabelecer uma filial na União.

   Para efeitos do primeiro parágrafo da presente alínea, a revisão inclui uma análise do regime a que se refere o artigo 31.º, n.º 12, incluindo as condições de acesso das entidades financeiras da União aos serviços de países terceiros e a disponibilidade desses serviços no mercado da União, e tem em conta a evolução dos mercados dos serviços abrangidos pelo presente regulamento, a experiência prática das entidades financeiras e das autoridades de supervisão financeira no que diz respeito, respetivamente, à aplicação e à supervisão desse regime, e eventuais desenvolvimentos pertinentes em termos de regulamentação e supervisão a nível internacional;

d) A conveniência de incluir no âmbito de aplicação do presente regulamento as entidades financeiras referidas no artigo 2.º, n.º 3, alínea e), que recorrem a sistemas de vendas automatizados, à luz da futura evolução do mercado no que diz respeito à utilização desses sistemas;

e) O funcionamento e a eficácia da rede de superintendência conjunta em termos de apoio à coerência da superintendência e à eficiência do intercâmbio de informações no âmbito do quadro de superintendência.

2. No contexto da revisão da Diretiva (UE) 2015/2366, a Comissão avalia a necessidade de aumentar a ciber-resiliência dos sistemas de pagamento e das atividades de processamento de pagamentos, bem como a conveniência de alargar o âmbito de aplicação do presente regulamento aos operadores de sistemas de pagamento e às entidades envolvidas em atividades de processamento de pagamentos. À luz dessa avaliação, a Comissão apresenta, no âmbito da revisão da Diretiva (UE) 2015/2366, um relatório ao Parlamento Europeu e ao Conselho, o mais tardar, até 17 de julho de 2023.

Com base neste relatório de revisão, e após consulta das AES, do BCE e do CERS, a Comissão pode apresentar, se for caso disso e no âmbito da proposta legislativa que possa vir a adotar nos termos do artigo 108.º, segundo parágrafo, da Diretiva (UE) 2015/2366, uma proposta destinada a assegurar que todos os operadores de sistemas de pagamento e entidades envolvidas em atividades de processamento de pagamentos sejam sujeitos a uma superintendência adequada, tendo simultaneamente em conta a superintendência dos bancos centrais.

3. Até 17 de janeiro de 2026, a Comissão, após consulta das AES e do Comité dos Organismos Europeus de Supervisão de Auditoria, procede a uma revisão e apresenta um relatório ao Parlamento Europeu e ao Conselho, acompanhado, se necessário, de uma proposta legislativa, sobre a adequação do reforço dos requisitos aplicáveis aos revisores oficiais de contas e às sociedades de revisores oficiais de contas no que respeita à resiliência operacional digital, através da inclusão dos revisores oficiais de contas e das sociedades de revisores oficiais de contas no âmbito de aplicação do presente regulamento ou através de alterações à Diretiva 2006/43/CE do Parlamento Europeu e do Conselho ([39]).

Secção II

Alterações

Artigo 59.º

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

O Regulamento (CE) n.º 1060/2009 é alterado do seguinte modo:

1) No anexo I, secção A, ponto 4, o primeiro parágrafo 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 para gerir os sistemas de TIC, de acordo com o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*).

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, 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, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).»;

2) No anexo III, o ponto 12 passa a ter a seguinte redação:

«12. As agências de notação de risco violam o artigo 6.º, n.º 2, em conjugação com anexo I secção A, ponto 4, se não tiverem procedimentos administrativos e contabilísticos sólidos, mecanismos de controlo interno, processos eficazes de avaliação dos riscos ou mecanismos eficazes para o controlo e a salvaguarda para gerir os sistemas de TIC, de acordo com o Regulamento (UE) 2022/2554; ou não aplicarem ou mantiverem procedimentos de tomada de decisões ou estruturas organizativas requeridos nos termos do referido ponto.»

Artigo 60.º

Alteração 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 no domínio das TIC geridos nos termos do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*).

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, 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, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).»;

([39]) Diretiva 2006/43/CE do Parlamento Europeu e do Conselho, de 17 de maio de 2006, relativa à revisão legal das contas anuais e consolidadas, que altera as Diretivas 78/660/CEE e 83/349/CEE do Conselho e que revoga a Diretiva 84/253/CEE do Conselho (JO L 157 de 9.6.2006, p. 87).

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 uma política de continuidade das atividades no domínio das TIC e planos de resposta e recuperação em matéria de TIC elaborados e executados nos termos do Regulamento (UE) 2022/2554, destinados a assegurar 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:

«3. 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 em caso de catástrofe, excluindo a política 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, n.º 3, o primeiro parágrafo passa a ter a seguinte redação:

«3. A fim de assegurar uma aplicação coerente do presente artigo, a ESMA desenvolve projetos de normas técnicas de regulamentação destinadas a especificar os pormenores, que não sejam os relativos aos requisitos relacionados com a gestão do risco associado às TIC, do pedido 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 de TIC geridos nos termos do Regulamento (UE) 2022/2554.

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 a política de continuidade das atividades no domínio das TIC e os planos de resposta e recuperação em matéria de TIC estabelecidos nos termos do Regulamento (UE) 2022/2554, destinados a assegurar 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:

6) No anexo I, a secção II é alterada do seguinte modo:

a) As alíneas a) e b) passam a ter a seguinte redação:

«a) Os repositórios de transações infringem o artigo 79.º, n.º 1, se não assegurarem a identificação das fontes de risco operacional ou a limitação desse risco através do desenvolvimento de sistemas, controlos e procedimentos adequados, incluindo sistemas de TIC geridos nos termos do Regulamento (UE) 2022/2554;

b) Os repositórios de transações infringem o artigo 79.º, n.º 2, se não estabelecerem, aplicarem ou mantiverem uma política adequada de continuidade das atividades e planos de recuperação em caso de catástrofe estabelecidos nos termos do Regulamento (UE) 2022/2554, destinados a assegurar a manutenção das suas funções, a recuperação atempada das operações e o cumprimento das suas obrigações.»;

b) A alínea c) é suprimida;

7) O Anexo III é alterado do seguinte modo:

a) A secção II é alterada do seguinte modo:

i) a alínea c) passa a ter a seguinte redação:

«c) Uma CCP de nível 2 infringe o artigo 26.º, n.º 3, se não mantiver ou utilizar uma estrutura organizativa que garanta a continuidade e o correto funcionamento dos seus serviços e das suas atividades ou se não empregar sistemas, recursos ou procedimentos adequados e proporcionados, incluindo sistemas de TIC geridos nos termos do Regulamento (UE) 2022/2554;»,

ii) é suprimida a alínea f);

b) Na secção III, a alínea a) passa a ter a seguinte redação:

«a) Uma CCP de nível 2 infringe o artigo 34.º, n.º 1, se não estabelecer, aplicar ou mantiver uma política adequada de continuidade das atividades e planos de resposta e recuperação estabelecidos nos termos do Regulamento (UE) 2022/2554, destinados a assegurar a preservação das suas funções, a recuperação atempada das operações e o cumprimento das suas obrigações, os quais devem prever, no mínimo, a recuperação de todas as transações em curso no momento da perturbação, para permitir que a CCP continue a funcionar de forma fiável e complete as liquidações nas datas previstas;».

Artigo 61.º

Alteração 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 nos termos do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*), 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) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, 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, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).»;

2) É suprimido o n.º 2;

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 em caso de catástrofe, incluindo a política de continuidade das atividades no domínio das TIC e os planos de resposta e recuperação em matéria de TIC estabelecidos nos termos do Regulamento (UE) 2022/2554, a fim de assegurar 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 assegurando que os sistemas de tecnologias de informação críticos possam retomar as operações a partir do momento do incidente, tal como previsto no artigo 12.º, n.ºs 5 e 7, do Regulamento (UE) 2022/2554.»;

4) O n.º 6 passa a ter a seguinte redação:

«6. As CSD identificam, controlam e gerem os riscos que poderão representar para as suas atividades os participantes-chave nos sistemas de liquidação de valores mobiliários que gerem, bem como os prestadores de serviços e fornecedores e outras CSD ou infraestruturas de mercado. Quando tal lhes for solicitado, as CSD prestam às autoridades competentes e às autoridades relevantes informações sobre os riscos dessa natureza que tenham identificado. As CSD informam igualmente sem demora a autoridade competente e as autoridades relevantes de quaisquer incidentes operacionais, que não estejam relacionados com o risco associado às TIC, resultantes desses riscos.»;

5) No n.º 7, o primeiro parágrafo passa a ter a seguinte redação:

«7. A ESMA elabora, em estreita cooperação com os membros do SEBC, projetos de normas técnicas de regulamentação que especifiquem os riscos operacionais a que se referem os n.ºs 1 e 6, que não sejam risco associado às TIC, e os métodos a utilizar para testar, tratar ou reduzir esses riscos, incluindo a política de continuidade das atividades e os planos de recuperação em caso de catástrofe a que se referem os n.ºs 3 e 4, bem como os métodos de avaliação dos mesmos.».

Artigo 62.º

Alteração 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 passa a ter a seguinte redação:

   «4. Os APA cumprem os requisitos relativos à segurança dos sistemas de rede e informação estabelecidos no Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*).

   _____

   (*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, 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, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).»;

   b) No n.º 8, a alínea c) passa a ter a seguinte redação:

   «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 passa a ter a seguinte redação:

   «5. Os CTP cumprem os requisitos relativos à segurança dos sistemas de rede e informação estabelecidos no Regulamento (UE) 2022/2554.»;

   b) No n.º 8, a 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 passa a ter a seguinte redação:

   «3. Os ARM cumprem os requisitos relativos à segurança dos sistemas de rede e informação estabelecidos no Regulamento (UE) 2022/2554»;

   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 63.º

Alteração do Regulamento (UE) 2016/1011

Ao artigo 6.º do Regulamento (UE) 2016/1011, é aditado o seguinte número:

«6. No caso dos índices de referência críticos, os administradores 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 para gerir os sistemas de TIC, de acordo com o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho (*).

_____

(*) Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, 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, (UE) n.º 909/2014 e (UE) 2016/1011 (JO L 333 de 27.12.2022, p. 1).».

Artigo 64.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 17 de janeiro de 2025.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Estrasburgo, em 14 de dezembro de 2022.

Pelo Parlamento Europeu	*Pelo Conselho*
A Presidente	*O Presidente*
R. METSOLA	M. BEK