Jornal Oficial
da União Europeia

PT
Série L

2024/1773

25.6.2024

REGULAMENTO DELEGADO (UE) 2024/1773 DA COMISSÃO

de 13 de março de 2024

que complementa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita às normas técnicas de regulamentação que especificam o conteúdo pormenorizado da política relativa aos acordos contratuais em matéria de utilização de serviços de TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC

(Texto relevante para efeitos do EEE)

A COMISSÃO EUROPEIA,

Tendo em conta o Tratado sobre o Funcionamento da União Europeia,

Tendo em conta o 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 e (UE) n.º 909/2014 e (UE) 2016/1011 ([1]), nomeadamente o artigo 28.º, n.º 10, terceiro parágrafo,

Considerando o seguinte:

(1) O quadro relativo à resiliência operacional digital do setor financeiro estabelecido pelo Regulamento (UE) 2022/2554 exige que as entidades financeiras prevejam determinados princípios fundamentais para gerir o risco associado às TIC devido a terceiros, que são de especial importância quando as entidades financeiras colaboram com terceiros prestadores de serviços de TIC para apoiar as suas funções críticas ou importantes.

(2) As entidades financeiras, no âmbito do seu quadro de gestão do risco associado às TIC, devem adotar e rever regularmente uma estratégia para o risco associado às TIC devido a terceiros. Em conformidade com o artigo 28.º, n.º 2, do Regulamento (UE) 2022/2554, essa estratégia deve incluir uma política de utilização de serviços de TIC, que apoiem funções críticas ou importantes, prestados por terceiros prestadores de serviços de TIC. É aplicável numa base individual e, se for caso disso, numa base subconsolidada e consolidada.

(3) As entidades financeiras variam consideravelmente em termos de dimensão, estrutura e organização interna, bem como da natureza e complexidade das suas atividades e operações. Aquando da elaboração da política relativa aos acordos contratuais sobre a utilização de serviços de TIC de apoio a funções críticas ou importantes por terceiros prestadores de serviços de TIC («política»), é necessário ter em conta essa diversidade, impondo simultaneamente determinados requisitos regulamentares fundamentais adequados a todas as entidades financeiras, e assegurar que esses requisitos sejam aplicados de forma proporcionada.

(4) Caso as entidades financeiras pertençam a um grupo, a empresa-mãe responsável pela disponibilização das demonstrações financeiras consolidadas ou subconsolidadas do grupo deve, por conseguinte, assegurar que a política seja aplicada de forma consistente e coerente no âmbito do grupo.

(5) Ao aplicar a política, os prestadores de serviços de TIC intragrupo, incluindo os que são total ou coletivamente detidos por entidades financeiras no âmbito do mesmo sistema de proteção institucional, devem ser considerados terceiros prestadores de serviços de TIC. Os riscos colocados pelos prestadores de serviços de TIC intragrupo podem ser diferentes, mas os requisitos que lhes são aplicáveis são os mesmos, nos termos do Regulamento (UE) 2022/2554. Do mesmo modo, a política deve aplicar-se aos subcontratantes que prestam serviços de TIC de apoio a funções críticas ou importantes ou a partes materiais das mesmas a terceiros prestadores de serviços de TIC, caso exista uma cadeia de terceiros prestadores de serviços de TIC.

(6) A responsabilidade final do órgão de administração pela gestão do risco associado às TIC de uma entidade financeira é um princípio geral que também é aplicável à utilização de terceiros prestadores de serviços de TIC. Esta responsabilidade deve traduzir-se na participação contínua do órgão de administração no controlo e monitorização da gestão dos riscos associados às TIC, incluindo na adoção e revisão, pelo menos uma vez por ano, da política.

([1]) JO L 333 de 27.12.2022, p. 1, ELI: http://data.europa.eu/eli/reg/2022/2554/oj.

(7) A fim de assegurar uma comunicação adequada de informações ao órgão de administração, a política deve especificar e identificar claramente as responsabilidades internas em matéria de aprovação, gestão, controlo e documentação dos acordos contratuais relativos à utilização de serviços de TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC («acordos contratuais»), incluindo os serviços de TIC prestados ao abrigo dos acordos contratuais a que se refere o artigo 28.º, n.º 1, alínea a), do Regulamento (UE) 2022/2554.

(8) A fim de ter em conta todos os possíveis riscos que possam surgir aquando da contratação de serviços de TIC de apoio a funções críticas ou importantes, a estrutura da política deve seguir todas as etapas de cada fase principal do ciclo de vida dos acordos contratuais com terceiros prestadores de serviços.

(9) Para atenuar os riscos identificados, a política deve especificar o planeamento dos acordos contratuais, incluindo a avaliação dos riscos, a devida diligência e o processo de aprovação de alterações novas ou significativas desses acordos contratuais. Por forma a gerir os riscos que possam surgir antes de celebrar um acordo contratual com um terceiro prestador de serviços de TIC, a política deve especificar um processo adequado e proporcionado para selecionar e avaliar a adequação dos potenciais terceiros prestadores de serviços de TIC e exigir que a entidade financeira tenha em conta uma lista não exaustiva de elementos de que os terceiros prestadores de serviços de TIC devem dispor. A lista deve incluir elementos relacionados com a reputação comercial dos prestadores de serviços, os seus recursos financeiros, humanos e técnicos, a segurança da sua informação, a sua estrutura organizativa, incluindo a gestão dos riscos, e os seus controlos internos.

(10) A fim de assegurar uma boa gestão dos riscos na prestação de serviços de TIC de apoio a funções críticas ou importantes por terceiros prestadores de serviços de TIC, a política deve conter informações sobre a aplicação, a monitorização e a gestão dos acordos contratuais, incluindo a nível consolidado e subconsolidado, se for caso disso. Tal inclui requisitos para as cláusulas contratuais relativas às obrigações mútuas das entidades financeiras e dos terceiros prestadores de serviços de TIC, que devem ser estabelecidas por escrito. De modo a assegurar uma supervisão eficiente e promover a resiliência em caso de alterações do modelo de negócio ou do ambiente empresarial, a política deve assegurar o direito das entidades financeiras ou de terceiros designados, bem como das autoridades competentes, a inspeções e de acesso a informações, devendo também especificar mais pormenorizadamente as estratégias de saída e os processos de rescisão.

(11) Desde que sejam tratados dados pessoais por terceiros prestadores de serviços de TIC, esta política e quaisquer acordos contratuais não podem prejudicar e devem complementar as obrigações decorrentes do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([2]), designadamente a existência de um contrato escrito que descreva o tratamento de dados pessoais, a obrigação de garantir a segurança do tratamento de dados pessoais e a definição dos demais elementos exigidos por esse regulamento.

([2]) 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, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

(12) O Comité Conjunto das Autoridades Europeias de Supervisão a que se refere o artigo 54.º do Regulamento (UE) n.º 1093/2010 do Parlamento Europeu e do Conselho ([3]), o artigo 54.º do Regulamento (UE) n.º 1094/2010 do Parlamento Europeu e do Conselho ([4]) e o artigo 54.º do Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho ([5]) realizou consultas públicas abertas sobre os projetos de normas técnicas de regulamentação em que se baseia o presente regulamento, analisou os potenciais custos e benefícios das normas propostas e solicitou o parecer do Grupo das Partes Interessadas do Setor Bancário criado em conformidade com o artigo 37.º do Regulamento (UE) n.º 1093/2010, do Grupo de Interessados do Setor dos Seguros e Resseguros e do Grupo de Interessados do Setor das Pensões Complementares de Reforma criados em conformidade com o artigo 37.º do Regulamento (UE) n.º 1094/2010, e do Grupo de Interessados do Setor dos Valores Mobiliários e dos Mercados criado em conformidade com o artigo 37.º do Regulamento (UE) n.º 1095/2010.

(13) A Autoridade Europeia para a Proteção de Dados foi consultada em conformidade com o disposto no artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([6]) e emitiu um parecer em 24 de janeiro de 2024,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Perfil de risco global e complexidade

A política relativa à utilização de serviços de TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC («política») deve ter em conta a dimensão e o perfil de risco global da entidade financeira, bem como a natureza, a escala e os elementos de maior ou menor complexidade dos seus serviços, atividades e operações, incluindo os seguintes elementos:

a) O tipo de serviços de TIC incluídos no acordo contratual relativo à utilização de serviços de TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC («acordo contratual») entre a entidade financeira e o terceiro prestador de serviços de TIC;

b) A localização do terceiro prestador de serviços de TIC ou a localização da sua empresa-mãe;

c) Se os serviços de TIC de apoio a funções críticas ou importantes são prestados por um terceiro prestador de serviços de TIC localizado num Estado-Membro ou num país terceiro, tendo igualmente em conta o local a partir do qual os serviços de TIC são prestados e o local onde os dados são tratados e conservados;

d) A natureza dos dados partilhados com o terceiro prestador de serviços de TIC;

e) Se o terceiro prestador de serviços de TIC integra o mesmo grupo que a entidade financeira à qual os serviços são prestados;

([3]) 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, ELI: http://data.europa.eu/eli/reg/2010/1093/oj).

([4]) 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, ELI: http://data.europa.eu/eli/reg/2010/1094/oj).

([5]) 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, ELI: http://data.europa.eu/eli/reg/2010/1095/oj).

([6]) 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, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

f) A utilização de terceiros prestadores de serviços de TIC que estejam autorizados, registados ou sujeitos a supervisão ou superintendência por uma autoridade competente de um Estado-Membro ou sujeitos ao quadro de superintendência previsto no capítulo V, secção II, do Regulamento (UE) 2022/2554, bem como a utilização de terceiros prestadores de serviços de TIC que não o estejam;

g) A utilização de terceiros prestadores de serviços de TIC que estejam autorizados, registados ou sujeitos a supervisão ou superintendência por uma autoridade de supervisão de um país terceiro, bem como a utilização de terceiros prestadores de serviços de TIC que não o estejam;

h) Se a prestação de serviços de TIC de apoio a funções críticas ou importantes se concentra num único terceiro prestador de serviços de TIC ou num pequeno número desses prestadores de serviços;

i) A transferibilidade dos serviços de TIC de apoio a funções críticas ou importantes para outro terceiro prestador de serviços de TIC, nomeadamente em resultado de especificidades tecnológicas;

j) O potencial impacto das perturbações na prestação dos serviços de TIC de apoio a funções críticas ou importantes na continuidade das atividades da entidade financeira e na disponibilidade dos seus serviços.

Artigo 2.º

Aplicação a nível do grupo

Caso o presente regulamento seja aplicável numa base subconsolidada ou consolidada, a empresa-mãe responsável pela disponibilização das demonstrações financeiras consolidadas ou subconsolidadas do grupo deve assegurar que a política seja aplicada de forma coerente em todas as entidades financeiras que fazem parte do grupo e adequada para a aplicação efetiva do presente regulamento a todos os níveis relevantes do grupo.

Artigo 3.º

Mecanismos de governação

1. O órgão de administração deve rever a política pelo menos uma vez por ano e atualizá-la sempre que necessário. As alterações introduzidas na política devem ser aplicadas em tempo útil e logo que possível no âmbito dos acordos contratuais pertinentes. A entidade financeira deve documentar o calendário previsto para a aplicação.

2. A política deve estabelecer ou remeter para uma metodologia que determine quais os serviços de TIC que apoiam funções críticas ou importantes. A política deve também especificar o momento em que esta avaliação deve ser realizada e revista.

3. A política deve atribuir claramente as responsabilidades internas pela aprovação, gestão, controlo e documentação dos acordos contratuais relevantes e assegurar que sejam mantidas competências, experiência e conhecimentos adequados no seio da entidade financeira para supervisionar eficazmente os acordos contratuais relevantes, incluindo os serviços de TIC prestados ao abrigo desses acordos.

4. Sem prejuízo da responsabilidade final da entidade financeira pela supervisão eficaz dos acordos contratuais relevantes, a política deve exigir a avaliação do terceiro prestador de serviços de TIC a fim de determinar se dispõe de recursos suficientes para assegurar que a entidade financeira cumpra todas as suas obrigações legais e regulamentares relativas aos serviços de TIC de apoio a funções críticas ou importantes prestados.

5. A política deve identificar claramente o cargo ou o membro da direção de topo responsável pela monitorização dos acordos contratuais relevantes. A política deve especificar a forma como esse cargo ou membro da direção de topo deve cooperar com as funções de controlo, a não ser que integre essas mesmas funções, e definir os canais de comunicação de informações ao órgão de administração, incluindo a natureza das informações a comunicar e os documentos a apresentar. Deve igualmente estabelecer a frequência desses relatórios.

6. A política deve assegurar que os acordos contratuais sejam coerentes com:

a) O quadro de gestão do risco associado às TIC a que se refere o artigo 6.º do Regulamento (UE) 2022/2554;

b) A política de segurança das informações a que se refere o artigo 9.º, n.º 4, do Regulamento (UE) 2022/2554;

c) A política de continuidade das atividades no domínio das TIC a que se refere o artigo 11.º do Regulamento (UE) 2022/2554;

d) Os requisitos em matéria de comunicação de incidentes estabelecidos no artigo 19.º do Regulamento (UE) 2022/2554.

7. A política deve exigir que os serviços de TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC sejam objeto de uma revisão independente e sejam incluídos no plano de auditoria.

8. A política deve especificar explicitamente que os acordos contratuais:

a) Não exoneram a entidade financeira e o seu órgão de administração das suas obrigações regulamentares e das suas responsabilidades para com os seus clientes;

b) Não impedem uma supervisão eficaz de uma entidade financeira e não infringem quaisquer restrições de supervisão em matéria de serviços e atividades;

c) Exigem que os terceiros prestadores de serviços de TIC cooperem com as autoridades competentes;

d) Exigem que a entidade financeira, os seus auditores e as autoridades competentes tenham acesso efetivo aos dados e às instalações relacionados com a utilização de serviços de TIC que apoiem funções críticas ou importantes.

Artigo 4.º

Principais fases do ciclo de vida em termos de adoção e utilização dos acordos contratuais

A política deve especificar os requisitos, incluindo as regras, as responsabilidades e os processos, para cada fase principal do ciclo de vida do acordo contratual, abrangendo, pelo menos, o seguinte:

a) As responsabilidades do órgão de administração, incluindo a sua participação, se for caso disso, no processo de tomada de decisões sobre a utilização de serviços de TIC de apoio a funções críticas ou importantes prestados por terceiros prestadores de serviços de TIC;

b) O planeamento dos acordos contratuais, incluindo a avaliação dos riscos, a devida diligência prevista nos artigos 5.º e 6.º e o processo de aprovação de alterações novas ou significativas dos acordos contratuais, tal como estabelecido no artigo 8.º, n.º 4;

c) O envolvimento de unidades de negócio, controlos internos e outras unidades relevantes no que diz respeito aos acordos contratuais;

d) A execução, a monitorização e a gestão dos acordos contratuais a que se referem os artigos 7.º, 8.º e 9.º, incluindo a nível consolidado e subconsolidado, se for caso disso;

e) A documentação e a conservação de registos, tendo em conta os requisitos relativos ao registo de informações estabelecidos no artigo 28.º, n.º 3, do Regulamento (UE) 2022/2554;

f) As estratégias de saída e os processos de rescisão estabelecidos no artigo 10.º.

Artigo 5.º

Avaliação *ex ante* dos riscos

1. A política deve exigir que as necessidades operacionais da entidade financeira sejam definidas antes da celebração de um acordo contratual.

2. A política deve exigir que seja realizada uma avaliação dos riscos a nível da entidade financeira e, se for caso disso, a nível consolidado e subconsolidado antes da celebração de um acordo contratual.

A avaliação dos riscos deve ter em conta todos os requisitos pertinentes estabelecidos no Regulamento (UE) 2022/2554 e na legislação setorial aplicável da União. Deve ter em conta, em especial, o impacto da prestação de serviços de TIC de apoio a funções críticas ou importantes por terceiros prestadores de serviços de TIC na entidade financeira e todos os riscos colocados pela prestação desses serviços de TIC de apoio a funções críticas ou importantes por terceiros prestadores de serviços de TIC, incluindo os seguintes:

a) Riscos operacionais;

b) Riscos jurídicos;

c) Riscos associados às TIC;

d) Riscos de reputação;

e) Riscos associados à proteção de dados confidenciais ou pessoais;

f) Riscos associados à disponibilidade de dados;

g) Riscos associados ao local onde os dados são tratados e conservados;

h) Riscos associados à localização do terceiro prestador de serviços de TIC;

i) Riscos de concentração no domínio das TIC a nível da entidade.

Artigo 6.º

Devida diligência

1. A política deve estabelecer um processo adequado e proporcionado de seleção e avaliação dos potenciais terceiros prestadores de serviços de TIC, tendo em conta se o terceiro prestador de serviços de TIC é ou não um prestador de serviços de TIC intragrupo, bem como exigir que a entidade financeira avalie, antes de celebrar um acordo contratual, se o terceiro prestador de serviços de TIC:

a) Possui a reputação empresarial, competências suficientes, conhecimentos especializados e recursos financeiros, humanos e técnicos adequados, normas de segurança das informações, uma estrutura organizativa, processos de gestão do risco e controlos internos adequados e, se for caso disso, as autorizações ou registos necessários para prestar os serviços de TIC de apoio à função crítica ou importante de forma fiável e profissional;

b) Tem capacidade para acompanhar a evolução tecnológica pertinente, identificar práticas de liderança em matéria de segurança das TIC e aplicá-las, se for caso disso, para dispor de um quadro de resiliência operacional digital eficaz e sólido;

c) Recorre ou prevê recorrer a subcontratantes no domínio das TIC para prestar serviços de TIC de apoio a funções críticas ou importantes ou a partes materiais das mesmas;

d) Está localizado, ou trata ou conserva os dados num país terceiro e, se for esse o caso, se esta prática afeta o nível de riscos operacionais ou de reputação ou o risco de ser afetado por medidas restritivas, incluindo embargos e sanções, que possam prejudicar a capacidade do terceiro prestador de serviços de TIC para prestar serviços de TIC ou a entidade financeira para receber esses serviços de TIC;

e) Aceita celebrar acordos contratuais que garantam a possibilidade efetiva de a própria entidade financeira, de terceiros designados e de as autoridades competentes realizarem auditorias junto do terceiro prestador de serviços de TIC, incluindo no local;

f) Age de forma ética e socialmente responsável, respeita os direitos humanos e os direitos da criança, incluindo a proibição do trabalho infantil, respeita os princípios aplicáveis em matéria de proteção do ambiente e garante condições de trabalho adequadas.

2. A política deve especificar o nível de garantia exigido no que respeita à eficácia do quadro de gestão dos riscos associados aos terceiros prestadores de serviços de TIC para os serviços de TIC de apoio a funções críticas ou importantes a prestar por um terceiro prestador de serviços de TIC. A política deve exigir que o processo de devida diligência inclua uma avaliação da existência de medidas de atenuação dos riscos e de continuidade das atividades e da forma como é assegurado o seu funcionamento no âmbito do terceiro prestador de serviços de TIC.

3. A política deve determinar o processo de devida diligência para selecionar e avaliar os potenciais terceiros prestadores de serviços de TIC e indicar quais dos seguintes elementos devem ser utilizados para especificar o nível de garantia exigido em matéria de desempenho do terceiro prestador de serviços de TIC:

a) Auditorias ou avaliações independentes realizadas pela própria entidade financeira ou em seu nome;

b) O recurso a relatórios de auditoria independentes elaborados a pedido do terceiro prestador de serviços de TIC;

c) O recurso a relatórios de auditoria elaborados pela função de auditoria interna do terceiro prestador de serviços de TIC;

d) A utilização de certificações de terceiros adequadas;

e) A utilização de outras informações relevantes de que a entidade financeira disponha ou de outras informações fornecidas pelo terceiro prestador de serviços de TIC.

4. As entidades financeiras devem assegurar um nível adequado de garantia do desempenho do terceiro prestador de serviços de TIC, tendo em conta os elementos enumerados no n.º 3, alíneas a) a e). Sempre que aplicável, deve ser utilizado mais do que um dos elementos enumerados nessas alíneas.

Artigo 7.º

Conflitos de interesses

1. A política deve especificar as medidas adequadas para identificar, prevenir e gerir conflitos de interesses reais ou potenciais decorrentes da utilização de terceiros prestadores de serviços de TIC, que devem ser tomadas antes da celebração de acordos contratuais relevantes, e deve prever um acompanhamento contínuo desses conflitos de interesses.

2. Sempre que sejam prestados serviços de TIC de apoio a funções críticas ou importantes por prestadores de serviços de TIC intragrupo, a política deve especificar que as decisões sobre as condições, incluindo as condições financeiras, dos serviços de TIC devem ser tomadas de forma objetiva.

Artigo 8.º

Cláusulas contratuais

1. A política deve especificar que o acordo contratual relevante deve ser escrito e incluir todos os elementos referidos no artigo 30.º, n.ºs 2 e 3, do Regulamento (UE) 2022/2554. A política deve também incluir elementos relativos aos requisitos a que se refere o artigo 1.º, n.º 1, alínea a), do Regulamento (UE) 2022/2554, bem como outra legislação da União e nacional pertinente, consoante o caso.

2. A política deve especificar que os acordos contratuais relevantes devem incluir o direito da entidade financeira de acesso às informações, bem como de realização de inspeções, auditorias e testes às TIC. Para o efeito, a política deve exigir que a entidade financeira utilize os seguintes métodos, sem prejuízo da responsabilidade final da entidade financeira:

a) A sua própria auditoria interna ou uma auditoria efetuada por um terceiro designado;

b) Se for caso disso, auditorias conjuntas e testes agrupados às TIC, incluindo testes de penetração baseados em ameaças, organizados em conjunto com outras entidades financeiras adjudicantes ou empresas que utilizam serviços de TIC do mesmo terceiro prestador de serviços de TIC e realizados por essas entidades ou empresas financeiras adjudicantes ou por um terceiro por elas designado;

c) Certificações de terceiros, se for caso disso;

d) Sempre que adequado, relatórios de auditoria interna ou de terceiros disponibilizados pelo terceiro prestador de serviços de TIC.

3. A entidade financeira não pode, ao longo do tempo, basear-se exclusivamente nas certificações a que se refere o n.º 2, alínea c), nem nos relatórios de auditoria a que se refere a alínea d) desse número. A política só deve permitir a utilização dos métodos a que se refere o n.º 2, alíneas c) e d), se a entidade financeira:

a) Estiver satisfeita com o plano de auditoria do terceiro prestador de serviços de TIC no que diz respeito aos acordos contratuais relevantes;

b) Assegurar que o âmbito das certificações ou dos relatórios de auditoria abrange os sistemas e os controlos fundamentais por si identificados e assegurar o cumprimento dos requisitos regulamentares pertinentes;

c) Avaliar de forma exaustiva e contínua o conteúdo das certificações ou dos relatórios de auditoria e verificar se os relatórios ou certificações não estão desatualizados;

d) Assegurar que os principais sistemas e controlos sejam abordados em futuras versões da certificação ou do relatório de auditoria;

e) Estiver satisfeita com a aptidão da entidade de certificação ou auditoria;

f) Considerar que as certificações são emitidas e as auditorias são realizadas de acordo com normas profissionais relevantes amplamente reconhecidas e incluem um teste da eficácia operacional dos principais controlos em vigor;

g) Tiver o direito contratual de solicitar, com uma frequência razoável e legítima do ponto de vista da gestão dos riscos, alterações do âmbito das certificações ou dos relatórios de auditoria a outros sistemas e controlos pertinentes;

h) Tiver o direito contratual de realizar auditorias individuais e conjuntas, se assim o entender, no que diz respeito aos acordos contratuais e de aplicar esses direitos de acordo com a frequência definida.

4. A política deve assegurar que quaisquer alterações significativas do acordo contratual sejam formalizadas num documento escrito datado e assinado por todas as partes e especificar o processo de renovação dos acordos contratuais.

Artigo 9.º

Monitorização dos acordos contratuais

1. A política deve exigir que os acordos contratuais especifiquem as medidas e os indicadores-chave a monitorizar, de forma contínua, o desempenho dos terceiros prestadores de serviços de TIC, incluindo medidas para fiscalizar o cumprimento dos requisitos em matéria de confidencialidade, disponibilidade, integridade e autenticidade dos dados e das informações, bem como a conformidade dos terceiros prestadores de serviços de TIC com as políticas e procedimentos relevantes da entidade financeira. A política deve também especificar as medidas aplicáveis quando os acordos de nível de serviço não são cumpridos, incluindo, se for caso disso, sanções contratuais.

2. A política deve especificar a forma como a entidade financeira deve avaliar se os terceiros prestadores de serviços de TIC utilizados para os serviços de TIC de apoio a funções críticas ou importantes cumprem normas de desempenho e qualidade adequadas, em conformidade com o acordo contratual e as políticas da entidade financeira. A política deve, em especial, assegurar que:

a) Os terceiros prestadores de serviços de TIC apresentem à entidade financeira relatórios adequados sobre as suas atividades e serviços, incluindo relatórios periódicos, relatórios de incidentes, relatórios sobre a prestação dos serviços, relatórios sobre a segurança das TIC e relatórios sobre medidas e testes de continuidade das atividades;

b) O desempenho dos terceiros prestadores de serviços de TIC seja avaliado através de indicadores-chave de desempenho, indicadores-chave de controlo, auditorias, autocertificações e análises independentes, em conformidade com o quadro de gestão do risco associado às TIC da entidade financeira;

c) A entidade financeira receba outras informações pertinentes dos terceiros prestadores de serviços de TIC;

d) A entidade financeira seja notificada, se for caso disso, de incidentes relacionados com as TIC e de incidentes operacionais ou de segurança relacionados com pagamentos;

e) Sejam realizadas uma análise e auditorias independentes para verificar o cumprimento das obrigações e políticas legais e regulamentares.

3. A política deve especificar que a avaliação a que se refere o n.º 2 deve ser documentada e os seus resultados devem ser utilizados para atualizar a avaliação de risco da entidade financeira a que se refere o artigo 6.º.

4. A política deve estabelecer as medidas adequadas que a entidade financeira deve adotar se identificar deficiências na prestação dos serviços de TIC de apoio a funções críticas ou importantes ou no cumprimento de acordos contratuais ou obrigações legais por parte dos terceiros prestadores de serviços de TIC, incluindo incidentes relacionados com as TIC e incidentes operacionais ou de segurança relacionados com pagamentos. Deve igualmente especificar a forma como a aplicação dessas medidas deve ser fiscalizada, a fim de assegurar que sejam efetivamente cumpridas num prazo definido, tendo em conta a importância das deficiências.

Artigo 10.º

Saída e rescisão dos acordos contratuais

A política deve incluir requisitos para um plano de saída documentado para cada acordo contratual e para a revisão e teste periódicos do plano de saída documentado. Ao estabelecer o plano de saída, devem ser tidos em conta os seguintes elementos:

a) Interrupções de serviço imprevistas e persistentes;

b) Falha ou desadequação da prestação dos serviços de TIC;

c) Rescisão inesperada do acordo contratual.

O plano de saída deve ser realista, viável, baseado em cenários plausíveis e pressupostos razoáveis, e incluir um calendário de execução planeado compatível com as condições de saída e de rescisão estabelecidas nos acordos contratuais.

Artigo 11.º

Entrada em vigor

O presente regulamento entra em vigor no vigésimo dia seguinte ao da sua publicação no *Jornal Oficial da União Europeia*.

O presente regulamento é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros.

Feito em Bruxelas, em 13 de março de 2024.

Pela Comissão
A Presidente
Ursula VON DER LEYEN