REGULAMENTO DELEGADO (UE) 2025/295 DA COMISSÃO

de 24 de outubro de 2024

que completa o Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que diz respeito às normas técnicas de regulamentação sobre a harmonização das condições que permitem o exercício de atividades de superintendência

(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, (UE) n.º 909/2014 e (UE) 2016/1011 ([1]), nomeadamente o artigo 41.º, n.º 2, segundo parágrafo,

Considerando o seguinte:

(1) O quadro relativo à resiliência operacional digital do setor financeiro estabelecido pelo Regulamento (UE) 2022/2554 introduz um quadro da União de superintendência dos terceiros prestadores de serviços de tecnologias da informação e comunicação (TIC) ao setor financeiro designados como críticos em conformidade com o artigo 31.º do referido regulamento.

(2) Um terceiro prestador de serviços de TIC que decida apresentar um pedido de designação voluntária como crítico deve facultar à Autoridade Europeia de Supervisão (AES) recetora todas as informações necessárias para demonstrar a sua criticalidade, de acordo com os princípios e critérios estabelecidos no Regulamento (UE) 2022/2554. Por este motivo, as informações a incluir no pedido de designação voluntária devem ser suficientemente pormenorizadas e abrangentes para permitir uma avaliação clara e completa da criticalidade nos termos do artigo 31.º, n.º 11, do referido regulamento. A AES competente deve rejeitar qualquer pedido incompleto e solicitar as informações em falta.

(3) A identificação jurídica dos terceiros prestadores de serviços de TIC abrangidos pelo âmbito de aplicação das presentes normas técnicas de regulamentação deve estar alinhada com o código de identificação estabelecido no regulamento de execução da Comissão adotado em conformidade com o artigo 28.º, n.º 9, do Regulamento (UE) 2022/2554.

(4) Após emitir recomendações dirigidas aos terceiros prestadores de serviços de TIC críticos, a autoridade fiscalizadora principal deve acompanhar o cumprimento das mesmas por parte dos destinatários. A fim de assegurar um acompanhamento eficiente e eficaz das ações empreendidas ou das medidas corretivas aplicadas pelos terceiros prestadores de serviços de TIC críticos em resposta a estas recomendações, a autoridade fiscalizadora principal deve poder solicitar os relatórios a que se refere o artigo 35.º, n.º 1, alínea c), do Regulamento (UE) 2022/2554, que devem ser concebidos como relatórios intercalares e relatórios finais.

(5) Para efeitos da avaliação especificada no artigo 42.º, n.º 1, do Regulamento (UE) 2022/2554, segundo a qual a autoridade fiscalizadora principal é obrigada a avaliar se a explicação fornecida pelo terceiro prestador de serviços de TIC crítico é suficiente, a notificação à autoridade fiscalizadora principal pela entidade terceira prestadora de serviços no domínio das TIC considerada crítica da sua intenção de seguir as recomendações recebidas deve ser complementada por uma descrição das ações e medidas que foram tomadas para atenuar os riscos descritos nas recomendações, juntamente com os respetivos prazos. Essa explicação deve assumir a forma de um plano corretivo.

(6) Uma vez que se espera que a autoridade fiscalizadora principal avalie os acordos de subcontratação do terceiro prestador de serviços de TIC crítico, há que desenvolver um modelo para a prestação de informações sobre tais acordos. O modelo deve ter em conta as diferenças entre as estruturas dos terceiros prestadores de serviços de TIC críticos e as das entidades financeiras.

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

(7) Assim que emitir recomendações dirigidas a um terceiro prestador de serviços de TIC crítico, e após as autoridades competentes terem informado as entidades financeiras pertinentes dos riscos identificados nessas recomendações, a autoridade fiscalizadora principal deve acompanhar e avaliar a aplicação, por parte do terceiro prestador de serviços de TIC crítico, das ações e das medidas corretivas para dar cumprimento às recomendações. As autoridades competentes devem acompanhar e avaliar em que medida as entidades financeiras estão expostas aos riscos identificados nas recomendações. A fim de assegurar condições de concorrência equitativas para a realização das respetivas funções, em particular quando os riscos associados às recomendações forem graves e transversais a um elevado número de entidades financeiras de vários Estados-Membros. tanto as autoridades competentes como a autoridade fiscalizadora principal devem partilhar entre si todas as conclusões pertinentes que sejam necessárias para o exercício das respetivas atribuições. O objetivo da partilha de informações é assegurar que o retorno de informação da autoridade fiscalizadora principal ao terceiro prestador de serviços no domínio das TIC crítico em relação às ações e medidas corretivas que este último está a aplicar tenha em conta o impacto nos riscos das entidades financeiras e que as atividades de supervisão realizadas pelas autoridades competentes possam utilizar como base a avaliação realizada pela autoridade fiscalizadora principal.

(8) A fim de permitir uma partilha de informações eficiente e eficaz, as autoridades competentes devem avaliar, no âmbito das suas atividades de supervisão, em que medida as entidades financeiras por elas supervisionadas estão expostas aos riscos identificados nas recomendações. Esta avaliação deve ser realizada de forma proporcionada e com base no risco. A autoridade fiscalizadora principal deve solicitar às autoridades competentes que partilhem os resultados desta avaliação nos casos específicos em que os riscos associados às recomendações sejam graves e transversais a um elevado número de entidades financeiras de vários Estados-Membros. A fim de tirar o maior partido possível dos recursos das autoridades competentes, ao solicitar os resultados desta avaliação, a autoridade fiscalizadora principal deve ter sempre em conta que o objetivo de tais pedidos é avaliar a aplicação de ações e medidas corretivas dos terceiros prestadores de serviços de TIC críticos.

(9) 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 ([2]) e emitiu parecer em 22 de julho de 2024.

(10) O presente regulamento tem por base os projetos de normas técnicas de regulamentação apresentados pelas AES à Comissão.

(11) O Comité Conjunto das AES 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 associados 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 Parlamento Europeu e do Conselho ([3]), 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 do Parlamento Europeu e do Conselho ([4]), 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 do Parlamento Europeu e do Conselho ([5]),

([2]) 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).

([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).

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Informações que devem ser facultadas pelo terceiro prestador de serviços de TIC no pedido de designação como crítico

1. O terceiro prestador de serviços de tecnologias da informação e comunicação (TIC) deve fornecer as seguintes informações no pedido fundamentado, apresentado nos termos do artigo 31.º, n.º 11, do Regulamento (UE) 2022/2554, com vista à designação voluntária como crítico nos termos do artigo 31.º, n.º 1, alínea a), desse regulamento:

a) Nome da entidade jurídica;

b) Código de identificação da entidade jurídica;

c) Nome da pessoa de contacto e dados de contacto do terceiro prestador de serviços de TIC crítico;

d) País em que se situa a sede social da entidade jurídica;

e) Descrição da estrutura empresarial, incluindo, pelo menos, informações sobre a sua empresa-mãe e outras empresas coligadas que prestam serviços de TIC a entidades financeiras da União. Essas informações devem incluir, se for caso disso:

   i) nome das entidades jurídicas,

   ii) código de identificação da entidade jurídica,

   iii) país em que se situa a sede social da entidade jurídica;

f) Uma estimativa da quota de mercado do terceiro prestador de serviços de TIC no setor financeiro da União e uma estimativa da quota de mercado por tipo de entidade financeira, com base na lista constante do artigo 2.º, n.º 1, do Regulamento (UE) 2022/2554, no ano de apresentação do pedido de designação como crítico e no ano anterior a esse pedido;

g) Uma descrição de cada serviço de TIC prestado a entidades financeiras da União, incluindo:

   i) uma descrição da natureza da atividade e do tipo de serviços de TIC prestados a entidades financeiras,

   ii) quando disponível, uma lista das funções das entidades financeiras apoiadas pelos serviços de TIC prestados,

   iii) quando disponíveis, informações sobre se os serviços de TIC prestados às entidades financeiras apoiam funções críticas ou importantes.

h) Uma lista das entidades financeiras que utilizam os serviços de TIC prestados pelo terceiro prestador de serviços de TIC, incluindo, quando disponíveis, as seguintes informações para cada uma das entidades financeiras às quais são prestados serviços:

   i) nome da entidade jurídica,

   ii) código de identificação da entidade jurídica, se conhecido pelo terceiro prestador de serviços de TIC,

   iii) tipo de entidade financeira, conforme especificado no artigo 2.º, n.º 1, do Regulamento (UE) 2022/2554,

   iv) a localização geográfica a partir da qual os serviços de TIC são prestados a essa entidade jurídica específica.

i) Quando disponível, uma lista dos terceiros prestadores de serviços de TIC críticos incluídos na mais recente lista disponível desses prestadores de serviços publicada pelas AES, nos termos do artigo 31.º, n.º 9, do Regulamento (UE) 2022/2554, e que dependem dos serviços prestados pelo requerente;

j) Uma autoavaliação no que diz respeito ao seguinte:

   i) o grau de substituibilidade de cada serviço de TIC prestado pelo requerente, tendo em conta o seguinte:

      — a quota de mercado do terceiro prestador de serviços de TIC no setor financeiro da União,

— o número de concorrentes pertinentes conhecidos, por tipo de serviços de TIC ou por grupo de serviços de TIC,

— descrição das especificidades relacionadas com os serviços de TIC oferecidos, nomeadamente no que toca a qualquer tecnologia patenteada, ou ainda às características específicas da organização ou atividade do terceiro prestador de serviços de TIC.

ii) Informações sobre a disponibilidade dos terceiros prestadores alternativos de serviços de TIC para prestarem os mesmos serviços de TIC que o terceiro prestador de serviços de TIC que apresenta o pedido;

k) Informações sobre a futura estratégia empresarial no que diz respeito à prestação de serviços e à disponibilização de infraestruturas de TIC a entidades financeiras na União, incluindo eventuais alterações previstas na estrutura do grupo ou da gestão, a entrada em novos mercados ou o exercício de novas atividades;

l) Identificação dos subcontratantes do terceiro prestador de serviços de TIC que tenham sido designados como terceiros prestadores de serviços de TIC críticos;

m) Quaisquer outros motivos pertinentes para o pedido do terceiro prestador de serviços de TIC para ser designado como crítico.

2. Se o terceiro prestador de serviços de TIC pertencer a um grupo, as informações a que se refere o n.º 1 são fornecidas em relação aos serviços de TIC prestados pelo grupo no seu conjunto.

Artigo 2.º

Conteúdo, estrutura e formato das informações a apresentar, divulgar ou comunicar por terceiros prestadores de serviços de TIC críticos

1. Os terceiros prestadores de serviços de TIC críticos devem fornecer à autoridade fiscalizadora principal, a pedido desta, todas as informações necessárias para que a autoridade fiscalizadora principal desempenhe as suas funções de superintendência em conformidade com os requisitos do Regulamento (UE) 2022/2554.

2. A informação a que se refere o n.º 1 inclui nomeadamente:

a) Informações sobre os acordos, e cópias dos documentos contratuais, entre:

i) o terceiro prestador de serviços de TIC crítico e as entidades financeiras a que se refere o artigo 2.º, n.º 1, do Regulamento (UE) 2022/2554,

ii) o terceiro prestador de serviços de TIC crítico e os seus subcontratantes, com vista a captar a cadeia de valor tecnológica dos serviços de TIC prestados às entidades financeiras na União.

b) Informações sobre a estrutura organizativa e do grupo do terceiro prestador de serviços de TIC crítico, incluindo a identificação de todas as entidades pertencentes ao mesmo grupo que prestam direta ou indiretamente serviços de TIC a entidades financeiras na União;

c) Informações sobre os principais acionistas, incluindo a sua estrutura e distribuição geográfica, de qualquer uma das seguintes entidades:

i) entidades que detenham, individualmente ou em conjunto com as suas entidades associadas, 25 % ou mais do capital ou dos direitos de voto do terceiro prestador de serviços de TIC crítico,

ii) entidades que tenham o direito de nomear ou destituir a maioria dos membros dos órgãos de administração, gestão ou supervisão do terceiro prestador de serviços de TIC crítico,

iii) entidades que controlem, nos termos de um acordo, a maioria dos direitos de voto dos acionistas ou membros do terceiro prestador de serviços de TIC crítico.

d) Informações sobre a quota de mercado do terceiro prestador de serviços de TIC crítico, por tipo de serviços, nos mercados pertinentes em que opera;

e) Informações sobre os mecanismos de governação interna do terceiro prestador de serviços de TIC crítico, incluindo a cadeia de responsabilidade em matéria de governação e as regras de responsabilização;

f) as atas das reuniões do órgão de administração do terceiro prestador de serviços de TIC crítico e de quaisquer outros comités internos pertinentes, de algum modo relacionados com as atividades e os riscos ligados aos serviços no domínio das TIC prestados por terceiros que apoiam funções de entidades financeiras na União;

g) Informações sobre a segurança das TIC do terceiro prestador de serviços de TIC crítico, incluindo estratégias pertinentes, objetivos, políticas, procedimentos, protocolos, processos, medidas de controlo para proteger dados sensíveis, controlos de acesso, práticas de encriptação, planos de resposta a incidentes e informações sobre o cumprimento de todos os regulamentos pertinentes e das normas nacionais e internacionais, se for caso disso;

h) Informações sobre as medidas técnicas e organizativas para assegurar a proteção e a confidencialidade dos dados, incluindo dados pessoais e não pessoais, as medidas de controlo aplicadas para proteger os dados sensíveis, os controlos de acesso, as práticas de encriptação e o plano de resposta a violações de dados; sempre que, no que diz respeito ao tratamento de dados pessoais, o terceiro prestador de serviços de TIC esteja sujeito à legislação de países terceiros, incluindo a pedidos de acesso de governos de países terceiros, a lista dos países e da legislação aplicável.

i) Informações sobre os mecanismos que o terceiro prestador de serviços de TIC crítico disponibiliza às entidades financeiras da União para fins de portabilidade dos dados, portabilidade das aplicações e interoperabilidade;

j) Informações sobre a localização dos centros de dados e dos centros de produção de TIC utilizados para prestar serviços às entidades financeiras, incluindo uma lista de todas as instalações e edifícios pertinentes do terceiro prestador de serviços de TIC crítico, designadamente fora da União;

k) Informações sobre a prestação de serviços por terceiros prestadores de serviços de TIC críticos de países terceiros, incluindo informações sobre as disposições jurídicas pertinentes aplicáveis aos dados pessoais e não pessoais tratados por tais terceiros prestadores de serviços;

l) Informações sobre as medidas tomadas para fazer face aos riscos decorrentes da prestação de serviços de TIC pelo terceiro prestador de serviços de TIC crítico e pelos seus subcontratantes de países terceiros;

m) Informações sobre o quadro de gestão do risco e o quadro de gestão de incidentes, incluindo as políticas, procedimentos, instrumentos, mecanismos e disposições de governação do terceiro prestador de serviços de TIC crítico e dos seus subcontratantes, uma lista e uma descrição dos incidentes graves com impacto direto ou indireto nas entidades financeiras da União e pormenores pertinentes para determinar a importância do incidente para as entidades financeiras e para avaliar os possíveis impactos transfronteiriços;

n) Informações sobre o quadro de gestão de alterações, incluindo as políticas, procedimentos e controlos do terceiro prestador de serviços de TIC crítico e dos seus subcontratantes;

o) Informações sobre o quadro global de resposta e recuperação do terceiro prestador de serviços de TIC crítico, incluindo os planos de continuidade das atividades e os mecanismos e procedimentos conexos, a política relativa ao ciclo de vida do desenvolvimento de programas informáticos, os planos de resposta e recuperação e os mecanismos e procedimentos conexos e as políticas, mecanismos e procedimentos de salvaguarda;

p) Informações sobre a monitorização do desempenho, a monitorização da segurança e o rastreio de incidentes, bem como informações sobre os mecanismos de comunicação relacionados com o desempenho dos serviços, os incidentes e o cumprimento dos acordos de nível de serviço (ANS) e dos objetivos de nível de serviço (ONS) estabelecidos ou de acordos semelhantes entre terceiros prestadores de serviços de TIC críticos e entidades financeiras na União;

q) Informações sobre o quadro do terceiro prestador de serviços de TIC crítico em matéria de gestão de terceiros no domínio das TIC, incluindo estratégias, políticas, procedimentos, processos e controlos, bem como pormenores sobre o dever de diligência e a avaliação dos riscos que o terceiro prestador de serviços de TIC crítico executa relativamente aos seus subcontratantes antes de celebrar um acordo com os mesmos e para monitorizar a relação, abrangendo todos os riscos pertinentes de contraparte e no domínio das TIC;

r) Excertos dos sistemas de monitorização e análise do terceiro prestador de serviços de TIC crítico e dos seus subcontratantes, que abranjam, entre outras coisas, a monitorização da rede, a monitorização dos servidores, a monitorização das aplicações, a monitorização da segurança, a análise da vulnerabilidade, a gestão de registos, a monitorização do desempenho, a gestão de incidentes e medições com base em objetivos de fiabilidade, como os ONS;

s) Excertos de qualquer sistema ou aplicação de produção, pré-produção e testagem utilizado pelo terceiro prestador de serviços de TIC crítico e pelos seus subcontratantes para prestar, direta ou indiretamente, serviços a entidades financeiras na União;

t) Relatórios de conformidade e relatórios de auditoria disponíveis, bem como quaisquer constatações de auditoria pertinentes, incluindo auditorias realizadas por autoridades nacionais na União e fora dela, sempre que os acordos de cooperação com as autoridades competentes prevejam esse intercâmbio de informações, ou certificações obtidas pelo terceiro prestador de serviços de TIC crítico ou pelos seus subcontratantes, incluindo relatórios de auditores internos e externos, certificações ou avaliações da conformidade que apliquem normas específicas do setor. Tal inclui informações sobre qualquer tipo de testes independentes disponíveis da resiliência dos sistemas de TIC do terceiro prestador de serviços de TIC crítico, incluindo qualquer tipo de testes de penetração baseados em ameaças realizados pelo terceiro prestador de serviços de TIC;

u) Informações sobre quaisquer avaliações efetuadas pelo prestador de serviços por terceiros prestadores de serviços de TIC críticos de países terceiros a seu pedido ou em seu nome em relação à adequação e integridade dos indivíduos que detêm posições-chave no terceiro prestador de serviços de TIC críticos;

v) Informações sobre qualquer plano corretivo para dar resposta a recomendações nos termos do artigo 3.º, e informações conexas pertinentes para confirmar a aplicação de medidas corretivas;

w) informações sobre os regimes de formação dos trabalhadores e os programas de sensibilização para a segurança disponíveis, incluindo, se for caso disso, informações sobre investimentos, recursos e métodos do terceiro prestador de serviços de TIC crítico na formação do seu pessoal para tratar dados financeiros sensíveis e manter elevados níveis de segurança;

x) Informações sobre as atividades do terceiro prestador de serviços de TIC crítico e demonstrações financeiras, incluindo informações sobre o orçamento e os recursos relacionados com as TIC e a segurança.

Artigo 3.º

Informações a fornecer pelos terceiros prestadores de serviços de TIC críticos após a emissão de recomendações

1. O terceiro prestador de serviços de TIC crítico deve fornecer à autoridade fiscalizadora principal um relatório com um plano corretivo em relação às recomendações e medidas corretivas que o terceiro prestador de serviços de TIC crítico tenciona aplicar a fim de atenuar os riscos identificados nas recomendações a que se refere o artigo 35.º, n.º 1, alínea d), do Regulamento (UE) 2022/2254. O relatório deve ser coerente com os prazos fixados pela autoridade fiscalizadora principal para cada recomendação.

2. A fim de permitir a monitorização da execução das ações empreendidas ou das medidas corretivas aplicadas pelo terceiro prestador de serviços de TIC crítico em resposta às recomendações recebidas, o terceiro prestador de serviços de TIC crítico partilha com a autoridade fiscalizadora principal, mediante pedido:

a) Relatórios intercalares e documentos de apoio conexos que indiquem os progressos realizados na execução das ações e medidas estabelecidas no relatório que o terceiro prestador de serviços de TIC críticos apresentou à autoridade fiscalizadora principal, dentro do prazo definido por esta;

b) Relatórios finais e documentos de apoio conexos que indiquem as ações empreendidas ou as medidas corretivas aplicadas pelo terceiro prestador de serviços de TIC crítico a fim de atenuar os riscos identificados nas recomendações recebidas.

Artigo 4.º

Estrutura e formato das informações fornecidas pelos terceiros prestadores de serviços de TIC críticos

1. As informações solicitadas são fornecidas à autoridade fiscalizadora principal pelo terceiro prestador de serviços de TIC crítico no formato estabelecido por essa autoridade e através dos canais eletrónicos seguros específicos indicados no respetivo pedido.

2. Ao fornecerem informações à autoridade fiscalizadora principal, os terceiros prestadores de serviços de TIC críticos:

a) Seguem a estrutura indicada pela autoridade fiscalizadora principal no seu pedido de informações;

b) Identificam claramente o elemento de informação pertinente na documentação apresentada.

3. As informações que o terceiro prestador de serviços de TIC crítico apresenta, divulga ou comunica à autoridade fiscalizadora principal devem ser redigidas numa língua de uso corrente na esfera financeira internacional.

Artigo 5.º

Modelo para fornecer informações sobre acordos de subcontratação

Um terceiro prestador de serviços de TIC crítico que seja obrigado a partilhar informações sobre os acordos de subcontratação fornece tais informações à autoridade fiscalizadora principal de acordo com o modelo constante do anexo.

Artigo 6.º

Avaliação, pelas autoridades competentes, dos riscos abordados nas recomendações da autoridade fiscalizadora principal

1. No âmbito da sua supervisão das entidades financeiras, a autoridade competente avalia o impacto nas entidades financeiras decorrente das medidas que o terceiro prestador de serviços de TIC crítico tomou com base nas recomendações emitidas pela autoridade fiscalizadora principal, em conformidade com o princípio da proporcionalidade.

2. Ao realizar a avaliação a que se refere o n.º 1, a autoridade competente tem em conta todos os seguintes elementos:

a) a adequação e a coerência das medidas corretivas aplicadas pelas entidades financeiras para atenuar os riscos identificados nas recomendações,

b) a avaliação, pela autoridade fiscalizadora principal, da conformidade do terceiro prestador de serviços de TIC crítico com as medidas e ações incluídas no relatório, caso tenha impacto na exposição das entidades financeiras sob a sua alçada aos riscos identificados nas recomendações;

c) o parecer de quaisquer outras autoridades competentes que tenham sido consultadas em conformidade com o artigo 42.º, n.º 5, do Regulamento (UE) 2022/2554,

d) se a autoridade fiscalizadora principal considerou que as ações e as medidas corretivas aplicadas pelo terceiro prestador de serviços de TIC crítico são adequadas para atenuar a exposição das entidades financeiras sob a sua alçada aos riscos identificados nas recomendações.

3. A pedido da autoridade fiscalizadora principal, a autoridade competente fornece, num prazo razoável, os resultados da avaliação prevista no n.º 1. Ao solicitar os resultados desta avaliação, a autoridade fiscalizadora principal tem em conta o princípio da proporcionalidade e a dimensão dos riscos associados às recomendações, incluindo os impactos transfronteiriços desses riscos, caso sejam afetadas entidades financeiras que operem em mais do que um Estado-Membro.

4. Quando pertinente, a autoridade competente solicita às entidades financeiras que forneçam todas as informações necessárias para efetuar a avaliação a que se refere o n.º 1.

Artigo 7.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 24 de outubro de 2024.

Pela Comissão
A Presidente
Ursula VON DER LEYEN

ANEXO

MODELO PARA A PARTILHA DE INFORMAÇÕES SOBRE OS ACORDOS DE SUBCONTRATAÇÃO

Categoria de informação	Elementos-chave de informação
Informações gerais	— Nome do terceiro prestador de serviços de TIC crítico. — Código de identificação do terceiro prestador de serviços de TIC crítico. — Nome da pessoa de contacto e dados de contacto do terceiro prestador de serviços de TIC crítico. — Data de apresentação do modelo.
Panorâmica dos acordos de subcontratação	— Mapeamento dos acordos de subcontratação, incluindo uma breve descrição da finalidade e âmbito das relações de subcontratação (incluindo uma indicação do nível de criticidade ou importância dos acordos de subcontratação para o terceiro prestador de serviços de TIC crítico). — Especificação e descrição dos tipos de serviços de TIC subcontratados e da sua importância para os serviços de TIC prestados pelas entidades financeiras, de acordo com as normas técnicas de execução adotadas nos termos do artigo 28.º, n.º 9, do Regulamento (UE) 2022/2554. — A especificação dos tipos de serviços de TIC deve ser efetuada utilizando a lista do anexo IV das normas técnicas de execução adotadas nos termos do artigo 28.º, n.º 9, do Regulamento (UE) 2022/2554.
Informações sobre o subcontratante	— Nome e dados da entidade jurídica (incluindo o código de identificação) de cada subcontratante. — Informações de contacto dos membros do pessoal responsáveis por cada uma das relações de subcontratação na estrutura de gestão do terceiro prestador de serviços de TIC crítico. — Panorâmica, para cada subcontratante, dos conhecimentos especializados, da experiência e das qualificações relacionadas com os serviços de TIC contratados.
Descrição dos serviços prestados pelos subcontratantes	— Descrição pormenorizada dos serviços de TIC específicos prestados por cada subcontratante. — Repartição das responsabilidades e tarefas atribuídas aos subcontratantes, especificando as diferentes funções nas diferentes fases dos processos de TIC. — As informações sobre o nível de acesso dos subcontratantes a dados ou sistemas pessoais ou sensíveis ligados aos serviços de TIC prestados às entidades financeiras. — Informações sobre os sítios a partir dos quais são prestados os serviços dos subcontratantes e sobre as medidas tomadas para fazer face aos riscos decorrentes dos serviços prestados fora da União.
Governação e supervisão da subcontratação	— Descrição do quadro contratual e de governação em vigor para gerir as relações de subcontratação, incluindo cláusulas que restringem a utilização de dados sensíveis. — Explicação dos processos de seleção, contratação e acompanhamento dos subcontratantes. — Panorâmica das métricas de desempenho, dos objetivos e acordos de nível de serviço e dos indicadores-chave de desempenho utilizados para avaliar o desempenho e acompanhar a fiabilidade do subcontratante.
Gestão de riscos e conformidade	— Avaliação dos perfis de risco do subcontratante e do potencial impacto nos serviços de TIC prestados às entidades financeiras. — Explicação das medidas de atenuação dos riscos aplicadas para fazer face aos riscos relacionados com a subcontratação. — Pormenores sobre a conformidade do subcontratante com a regulamentação pertinente, nomeadamente em matéria de proteção de dados e normas setoriais.

Categoria de informação	Elementos-chave de informação
Planos de continuidade das atividades e de contingência	— Panorâmica dos planos de continuidade das atividades e de resposta e recuperação do subcontratante. — Descrição das disposições em vigor para assegurar a continuidade do serviço em caso de perturbações ou cessação da atividade por parte do subcontratante. — Frequência dos testes dos planos de continuidade das atividades e dos planos de resposta e recuperação pelos subcontratantes, datas dos testes mais recentes nos últimos 3 anos e indicação sobre se o terceiro prestador de serviços de TIC crítico esteve envolvido nesses testes.
Comunicação de informações	— Descrição dos mecanismos de comunicação de informações entre o terceiro prestador de serviços de TIC crítico e os seus subcontratantes e sobre a respetiva frequência.
Reparação e gestão de incidentes	— Descrição dos procedimentos para fazer face a incidentes, infrações ou incumprimentos relacionados com o subcontratante.
Certificações e auditorias	— Informações sobre quaisquer certificações, auditorias independentes ou avaliações realizadas sobre subcontratantes para validar os seus controlos de segurança, normas de qualidade ou conformidade regulamentar. — Data e frequência das auditorias aos subcontratantes efetuadas pelo terceiro prestador de serviços de TIC crítico.