Jornal Oficial
da União Europeia

PT
Série L

2024/1772

25.6.2024

REGULAMENTO DELEGADO (UE) 2024/1772 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 os critérios de classificação dos incidentes relacionados com as TIC e das ciberameaças, estabelecem limiares de materialidade e especificam os pormenores das notificações dos incidentes de caráter severo

(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 18.º, n.º 4, terceiro parágrafo,

Considerando o seguinte:

(1) O Regulamento (UE) 2022/2554 visa harmonizar e simplificar os requisitos de notificação de incidentes relacionados com as TIC e de incidentes operacionais ou de segurança relacionados com pagamentos relativos a instituições de crédito, instituições de pagamento, prestadores de serviços de informação sobre contas e instituições de moeda eletrónica («incidentes»). Tendo em conta que os requisitos de comunicação de informações abrangem 20 tipos diferentes de entidades financeiras, os critérios de classificação e os limiares de materialidade para determinar os incidentes de caráter severo e as ciberameaças significativas devem ser especificados de forma simples, harmonizada e coerente, que atenda às especificidades dos serviços e às atividades de todas as entidades financeiras relevantes.

(2) A fim de assegurar a proporcionalidade, os critérios de classificação e os limiares de materialidade devem refletir a dimensão e o perfil de risco global, bem como a natureza, escala e complexidade dos serviços de todas as entidades financeiras. Além disso, os critérios e os limiares de materialidade devem ser elaborados de modo a serem aplicados de forma coerente a todas as entidades financeiras, independentemente da sua dimensão e perfil de risco, e a não representarem encargos desproporcionados de comunicação de informações para as entidades financeiras de menor dimensão. No entanto, a fim de dar resposta a situações em que um número significativo de clientes é afetado por um incidente que, em si mesmo, não excede o limiar aplicável, deve ser estabelecido um limiar absoluto destinado principalmente às entidades financeiras de maior dimensão.

(3) Em relação aos quadros de notificação de incidentes existentes antes da entrada em vigor do Regulamento (UE) 2022/2554, deve ser assegurada a continuidade para as entidades financeiras. Por conseguinte, os critérios de classificação e os limiares de materialidade devem estar em consonância e inspirar-se nas orientações da EBA sobre a comunicação de incidentes de caráter severo nos termos da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho ([2]), nas orientações relativas à informação e notificação periódicas de alterações significativas a apresentar à ESMA pelos repositórios de transações, no quadro de comunicação de incidentes de cibersegurança do BCE/MUS e noutras orientações pertinentes. Os critérios de classificação e os limiares de materialidade devem também ser adequados ao caso das entidades financeiras que não estavam sujeitas a requisitos de notificação de incidentes antes do Regulamento (UE) 2022/2554.

(4) No que respeita ao critério de classificação «quantidade e número de transações afetadas», a noção de transações é lata e abrange diferentes atividades e serviços nos atos setoriais aplicáveis às entidades financeiras. Para efeitos desse critério de classificação, devem ser abrangidas as operações de pagamento e todas as formas de troca de instrumentos financeiros, criptoativos, mercadorias ou quaisquer outros ativos, também sob a forma de margem, garantia ou penhor, tanto contra numerário como contra qualquer outro ativo. Devem ser consideradas para efeitos de classificação todas as operações que envolvam ativos cujo valor possa ser expresso num valor monetário.

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

([2]) 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, ELI: http://data.europa.eu/eli/dir/2015/2366/oj).

(5) Os critérios de classificação devem assegurar que todos os tipos pertinentes de incidentes de caráter severo sejam abrangidos. Os ciberataques relacionados com a intrusão em sistemas de rede ou de informação podem não ser necessariamente contemplados em muitos critérios de classificação. No entanto, são importantes, uma vez que qualquer intrusão em sistemas de rede e de informação pode prejudicar a entidade financeira. Por conseguinte, os critérios de classificação «serviços críticos afetados» e «perdas de dados» devem ser especificados de forma a abranger estes tipos de incidentes de caráter severo, nomeadamente intrusões não autorizadas, cujos impactos, mesmo que não sejam imediatamente conhecidos, podem ter consequências graves, nomeadamente violações e fugas de dados.

(6) Uma vez que as instituições de crédito estão sujeitas tanto ao quadro para a classificação dos incidentes nos termos do artigo 18.º do Regulamento (UE) 2022/2554 como ao quadro do risco operacional nos termos do Regulamento Delegado (UE) 2018/959 da Comissão ([3]), a abordagem para avaliar o impacto económico de um incidente com base no cálculo dos custos e perdas deve, tanto quanto possível, ser coerente entre ambos os quadros, a fim de evitar a introdução de requisitos incompatíveis ou contraditórios.

(7) O critério relativo à distribuição geográfica de um incidente previsto no artigo 18.º, n.º 1, alínea c), do Regulamento (UE) 2022/2554 deve centrar-se no impacto transfronteiriço do incidente, uma vez que o impacto de um incidente nas atividades de uma entidade financeira numa única jurisdição será tido em conta no quadro dos outros critérios estabelecidos nesse artigo.

(8) Dado que os critérios de classificação são interdependentes e estão ligados entre si, a abordagem para identificar os incidentes de caráter severo que devem ser comunicados em conformidade com o artigo 19.º, n.º 1, do Regulamento (UE) 2022/2554 deve basear-se numa combinação de critérios, em que alguns critérios estreitamente associados às definições de incidente relacionado com as TIC e de incidente de caráter severo relacionado com as TIC estabelecidas no artigo 3.º, n.ºs 8 e 10, do Regulamento (UE) 2022/2554 devem ter mais importância na classificação dos incidentes de caráter severo do que outros critérios.

(9) A fim de assegurar que os relatórios e as notificações de incidentes de caráter severo recebidos pelas autoridades competentes nos termos do artigo 19.º, n.º 1, do Regulamento (UE) 2022/2554 servem tanto para efeitos de supervisão como de prevenção do contágio ao resto do setor financeiro, os limiares de materialidade devem permitir a deteção dos incidentes de caráter severo, centrando-se nomeadamente no impacto nos serviços críticos específicos da entidade, nos limiares absolutos e relativos específicos dos clientes ou contrapartes financeiras, nas transações que indicam um impacto significativo na entidade financeira e na importância do impacto noutros Estados-Membros.

(10) Os incidentes que afetem serviços de TIC ou sistemas de rede e de informação de apoio a funções críticas ou importantes ou serviços financeiros que exijam autorização, ou o acesso mal-intencionado e não autorizado a sistemas de rede e de informação de apoio a funções críticas ou importantes, devem ser considerados incidentes que afetam os serviços críticos das entidades financeiras. O acesso mal-intencionado e não autorizado a sistemas de rede e de informação que apoiam funções críticas ou importantes das entidades financeiras representa um risco grave para a entidade financeira e, uma vez que pode afetar outras entidades financeiras, deve ser sempre considerado um incidente de caráter severo que deve ser notificado.

(11) Incidentes recorrentes ligados através de uma causa profunda aparente semelhante, que individualmente não sejam incidentes de caráter severo, podem indicar deficiências e vulnerabilidades significativas nos procedimentos de gestão de incidentes e de riscos da entidade financeira. Por conseguinte, os incidentes recorrentes devem ser coletivamente considerados de caráter severo quando ocorrem repetidamente durante um determinado período.

(12) Tendo em conta que as ciberameaças podem ter um impacto negativo na entidade financeira e no setor financeiro, as ciberameaças significativas que as entidades financeiras podem notificar devem indicar a probabilidade de ocorrência e a criticalidade do potencial impacto. Por conseguinte, a fim de assegurar uma avaliação clara e coerente da importância das ciberameaças, a classificação de uma ciberameaça como significativa deve depender da probabilidade de que os critérios de classificação dos incidentes de caráter severo e o respetivo limiar fossem atingidos se a ameaça se concretizasse, do tipo de ciberameaça e das informações de que a entidade financeira dispõe.

([3]) Regulamento Delegado (UE) 2018/959 da Comissão, de 14 de março de 2018, que complementa o Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho no que diz respeito à especificação da metodologia de avaliação ao abrigo da qual as autoridades competentes autorizam as instituições a utilizar Métodos de Medição Avançada para o risco operacional (JO L 169 de 6.7.2018, p. 1, ELI: http://data.europa.eu/eli/reg_del/2018/959/oj).

(13) Tendo em conta que as autoridades competentes de outros Estados-Membros devem ser notificadas dos incidentes que afetem as entidades financeiras e os clientes na sua jurisdição, a avaliação do impacto noutra jurisdição, em conformidade com o artigo 19.º, n.º 7, do Regulamento (UE) 2022/2554, deve basear-se na causa profunda do incidente, no potencial contágio através de terceiros prestadores e nas infraestruturas dos mercados financeiros, bem como no impacto do incidente em grupos significativos de clientes ou contrapartes financeiras.

(14) Os processos de comunicação e notificação a que se refere o artigo 19.º, n.ºs 6 e 7, do Regulamento (UE) 2022/2554 devem permitir que os respetivos destinatários avaliem o impacto dos incidentes. Por conseguinte, as informações transmitidas devem abranger todos os pormenores constantes dos relatórios de incidentes apresentados pela entidade financeira à autoridade competente.

(15) Caso um incidente constitua uma violação de dados pessoais nos termos do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho ([4]) e da Diretiva 2002/58/CE do Parlamento Europeu e do Conselho ([5]), o presente regulamento não deve afetar as obrigações de registo e notificação de violações de dados pessoais estabelecidas nessa legislação da União. As autoridades competentes devem cooperar e trocar informações sobre todas as questões pertinentes com as autoridades referidas no Regulamento (UE) 2016/679 e na Diretiva 2002/58/CE.

(16) O presente regulamento baseia-se nos projetos de normas técnicas de regulamentação apresentados à Comissão pelas Autoridades Europeias de Supervisão, em consulta com a Agência da União Europeia para a Cibersegurança (ENISA) e o Banco Central Europeu (BCE).

(17) 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 ([6]), o artigo 54.º do Regulamento (UE) n.º 1094/2010 do Parlamento Europeu e do Conselho ([7]) e o artigo 54.º do Regulamento (UE) n.º 1095/2010 do Parlamento Europeu e do Conselho ([8]) 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.

([4]) 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).

([5]) Diretiva 2002/58/CE do Parlamento Europeu e do Conselho, de 12 de julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações eletrónicas (Diretiva relativa à privacidade e às comunicações eletrónicas) (JO L 201 de 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([6]) 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).

([7]) 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).

([8]) 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).

(18) 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 [9] e emitiu um parecer em 24 de janeiro de 2024,

ADOTOU O PRESENTE REGULAMENTO:

CAPÍTULO I

CRITÉRIOS DE CLASSIFICAÇÃO

Artigo 1.º

Clientes, contrapartes financeiras e transações

1. O número de clientes afetados pelo incidente, tal como referido no artigo 18.º, n.º 1, alínea a), do Regulamento (UE) 2022/2554, deve refletir o número de todos os clientes afetados, quer sejam pessoas singulares ou coletivas, que são ou foram incapazes de utilizar o serviço prestado pela entidade financeira durante o incidente ou que foram negativamente afetados pelo incidente. Esse número deve também incluir os terceiros explicitamente abrangidos pelo acordo contratual entre a entidade financeira e o cliente enquanto beneficiários do serviço afetado.

2. O número de contrapartes financeiras afetadas pelo incidente, tal como referido no artigo 18.º, n.º 1, alínea a), do Regulamento (UE) 2022/2554, deve refletir o número de todas as contrapartes financeiras afetadas que tenham celebrado um acordo contratual com a entidade financeira.

3. Em relação à relevância dos clientes e contrapartes financeiras afetados pelo incidente, tal como referido no artigo 18.º, n.º 1, alínea a), do Regulamento (UE) 2022/2554, a entidade financeira deve ter em conta em que medida o impacto sobre um cliente ou uma contraparte financeira afetará a realização dos objetivos empresariais da entidade financeira, bem como o potencial impacto do incidente na eficiência do mercado.

4. Em relação à quantidade ou ao número de transações afetadas pelo incidente, tal como referido no artigo 18.º, n.º 1, alínea a), do Regulamento (UE) 2022/2554, a entidade financeira deve ter em conta todas as transações afetadas que envolvam um valor monetário e em que pelo menos uma parte da transação seja realizada na União.

5. Se não for possível determinar o número real de clientes ou contrapartes financeiras afetados ou o número ou a quantidade real de transações afetadas, a entidade financeira deve estimar esses números ou quantidades com base nos dados disponíveis de períodos de referência comparáveis.

Artigo 2.º

Impacto em termos de reputação

1. Para efeitos da determinação do impacto do incidente em termos de reputação, tal como referido no artigo 18.º, n.º 1, alínea a), do Regulamento (UE) 2022/2554, as entidades financeiras devem considerar que ocorreu um impacto em termos de reputação se estiver preenchido pelo menos um dos seguintes critérios:

a) O incidente foi noticiado nos órgãos de comunicação social;

b) O incidente deu origem a queixas repetidas de diferentes clientes ou contrapartes financeiras relativas a serviços de contacto direto com clientes ou a relações de negócio críticas;

c) A entidade financeira não será capaz, ou é provável que não seja capaz, de cumprir obrigações regulamentares em resultado do incidente;

d) A entidade financeira perderá, ou é provável que perca, clientes ou contrapartes financeiras com um impacto significativo na sua atividade em resultado do incidente.

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

2. Ao avaliar o impacto do incidente em termos de reputação, as entidades financeiras devem ter em conta o nível de visibilidade que o incidente adquiriu, ou é provável que adquira, em relação a cada critério enumerado no n.º 1.

Artigo 3.º

Duração e tempo de indisponibilidade do serviço

1. As entidades financeiras devem medir a duração de um incidente, tal como referido no artigo 18.º, n.º 1, alínea b), do Regulamento (UE) 2022/2554, desde o momento em que o incidente ocorre até ao momento em que é resolvido.

Se as entidades financeiras não puderem determinar o momento em que o incidente ocorreu, devem medir a duração do incidente a partir do momento em que foi detetado. Se as entidades financeiras tiverem conhecimento de que o incidente ocorreu antes da sua deteção, devem medir a duração a partir do momento em que o incidente for detetado em registos de redes ou sistemas ou noutras fontes de dados.

Caso as entidades financeiras ainda não saibam quando o incidente será resolvido ou não possam verificar as inscrições nos registos ou noutras fontes de dados, devem aplicar estimativas.

2. As entidades financeiras devem medir o tempo de indisponibilidade de serviço na sequência de um incidente, tal como referido no artigo 18.º, n.º 1, alínea b), do Regulamento (UE) 2022/2554, desde o momento em que o serviço se torne total ou parcialmente indisponível para clientes, contrapartes financeiras ou outros utilizadores internos ou externos até ao momento em que as atividades ou operações regulares tenham sido restabelecidas ao nível de serviço prestado antes do incidente. Se o tempo de indisponibilidade do serviço causar um atraso na prestação do serviço após o restabelecimento das atividades ou operações regulares, o tempo de indisponibilidade deve ser medido desde o início do incidente até ao momento em que a prestação do serviço em atraso for plenamente retomada.

Se as entidades financeiras não puderem determinar o momento em que teve início a indisponibilidade do serviço, devem medir esse tempo de indisponibilidade a partir do momento em que foi detetado.

Artigo 4.º

Distribuição geográfica

Para efeitos de determinação da distribuição geográfica relativamente às zonas afetadas pelo incidente, tal como referido no artigo 18.º, n.º 1, alínea c), do Regulamento (UE) 2022/2554, as entidades financeiras devem avaliar se o incidente tem ou teve impacto noutros Estados-Membros e, em especial, a importância desse impacto em qualquer um dos seguintes casos:

a) Clientes e contrapartes financeiras de outros Estados-Membros;

b) Sucursais ou outras entidades financeiras pertencentes ao grupo que exerçam atividades noutros Estados-Membros;

c) Infraestruturas do mercado financeiro ou terceiros prestadores, que possam afetar entidades financeiras de outros Estados-Membros aos quais prestam serviços, na medida em que essas informações estejam disponíveis.

Artigo 5.º

Perdas de dados

Para efeitos da determinação das perdas de dados decorrentes do incidente, tal como referido no artigo 18.º, n.º 1, alínea d), do Regulamento (UE) 2022/2554, as entidades financeiras devem ter em conta:

a) Em relação à disponibilidade dos dados, se o incidente tornou os dados de que a entidade financeira, os seus clientes ou as suas contrapartes necessitam temporária ou permanentemente inacessíveis ou inutilizáveis;

b) Em relação à autenticidade dos dados, se o incidente comprometeu a fiabilidade da fonte dos dados;

c) Em relação à integridade dos dados, se o incidente resultou numa alteração não autorizada dos dados que os tornou inexatos ou incompletos;

d) Em relação à confidencialidade dos dados, se o incidente resultou no acesso ou na divulgação dos dados a uma parte ou sistema não autorizado.

Artigo 6.º

Criticalidade dos serviços afetados

Para efeitos de determinação da criticalidade dos serviços afetados, tal como referido no artigo 18.º, n.º 1, alínea e), do Regulamento (UE) 2022/2554, as entidades financeiras avaliam se o incidente:

a) Afeta ou afetou serviços de TIC ou sistemas de rede e de informação que apoiam funções críticas ou importantes da entidade financeira;

b) Afeta ou afetou serviços financeiros prestados pela entidade financeira que exijam autorização, registo ou que sejam supervisionados pelas autoridades competentes;

c) Constitui ou constituiu um acesso bem-sucedido, mal-intencionado e não autorizado aos sistemas de rede e de informação da entidade financeira.

Artigo 7.º

Impacto económico

1. Para efeitos de determinação do impacto económico do incidente, tal como referido no artigo 18.º, n.º 1, alínea f), do Regulamento (UE) 2022/2554, as entidades financeiras devem, sem contabilizar as recuperações financeiras, ter em conta os seguintes tipos de custos e perdas diretos e indiretos em que incorreram em resultado do incidente:

a) Fundos ou ativos financeiros expropriados pelos quais são responsáveis, incluindo ativos perdidos por furto;

b) Custos de substituição ou relocalização de *software*, *hardware* ou infraestruturas;

c) Custos com pessoal, incluindo os custos associados à substituição ou relocalização do pessoal, ao recrutamento de pessoal suplementar, à remuneração de horas extraordinárias e ao restabelecimento de competências perdidas ou comprometidas;

d) Taxas por incumprimento de obrigações contratuais;

e) Custos de reparação e indemnização aos clientes;

f) Prejuízos causados pela perda de receitas;

g) Custos associados à comunicação interna e externa;

h) Custos de consultoria, incluindo custos associados a aconselhamento jurídico, a serviços forenses e a serviços de correção.

2. Os custos e perdas a que se refere o n.º 1 não incluem os custos necessários para o funcionamento corrente da empresa, nomeadamente:

a) Custos de manutenção geral de infraestruturas, equipamentos, *hardware* e *software*, bem como custos de atualização das competências do pessoal;

b) Custos internos ou externos para otimizar a atividade após o incidente, incluindo atualizações, melhorias e iniciativas de avaliação dos riscos;

c) Prémios de seguros.

3. As entidades financeiras devem calcular os montantes dos custos e perdas com base nos dados disponíveis no momento da notificação. Caso não seja possível determinar os montantes reais dos custos e perdas, as entidades financeiras devem estimar esses montantes.

4. Ao avaliar o impacto económico do incidente, as entidades financeiras devem adicionar os custos e perdas a que se refere o n.º 1.

CAPÍTULO II

INCIDENTES DE CARÁTER SEVERO E LIMIARES DE MATERIALIDADE

Artigo 8.º

Incidentes de caráter severo

1. Um incidente é considerado um incidente de caráter severo para efeitos do artigo 19.º, n.º 1, do Regulamento (UE) 2022/2554 se tiver afetado os serviços críticos a que se refere o artigo 6.º e se estiver preenchida uma das seguintes condições:

a) Foi atingido o limiar de materialidade a que se refere o artigo 9.º, n.º 5, alínea b);

b) Foram atingidos dois ou mais dos outros limiares de materialidade a que se refere o artigo 9.º, n.ºs 1 a 6.

2. Os incidentes recorrentes que, individualmente, não sejam considerados incidentes de caráter severo nos termos do n.º 1 devem ser considerados incidentes de caráter severo se preencherem todas as condições seguintes:

a) Ocorreram pelo menos duas vezes num período de seis meses;

b) Têm a mesma causa profunda aparente, como referido no artigo 20.º, primeiro parágrafo, alínea b), do Regulamento (UE) 2022/2554;

c) Preenchem coletivamente os critérios para serem considerados como um incidente de caráter severo conforme estabelecido no n.º 1.

As entidades financeiras devem avaliar mensalmente a existência de incidentes recorrentes.

O presente número não se aplica às microempresas nem às entidades financeiras enumeradas no artigo 16.º, n.º 1, do Regulamento (UE) 2022/2554.

Artigo 9.º

Limiares de materialidade para a determinação dos incidentes de caráter severo

1. O limiar de materialidade para o critério «clientes, contrapartes financeiras e transações» é atingido se estiver preenchida qualquer uma das seguintes condições:

a) O número de clientes afetados é superior a 10 % de todos os clientes que utilizam o serviço afetado;

b) O número de clientes afetados que utilizam o serviço afetado é superior a 100 000;

c) O número de contrapartes financeiras afetadas é superior a 30 % de todas as contrapartes financeiras que exercem atividades relacionadas com a prestação do serviço afetado;

d) O número de transações afetadas é superior a 10 % do número médio diário de transações realizadas pela entidade financeira relacionadas com o serviço afetado;

e) A quantidade de transações afetadas é superior a 10 % do valor médio diário das transações realizadas pela entidade financeira relacionadas com o serviço afetado;

f) Foram afetados clientes ou contrapartes financeiras que tenham sido identificados como relevantes nos termos do artigo 1.º, n.º 3.

Se não for possível determinar o número real de clientes ou contrapartes financeiras afetados ou o número ou a quantidade real de transações afetadas, a entidade financeira deve estimar esses números ou quantidades com base nos dados disponíveis de períodos de referência comparáveis.

2. O limiar de materialidade para o critério «impacto em termos de reputação» é atingido se estiver preenchida qualquer uma das condições estabelecidas no artigo 2.º, alíneas a) a d).

3. O limiar de materialidade para o critério «duração e tempo de indisponibilidade do serviço» é atingido se estiver preenchida qualquer uma das seguintes condições:

a) A duração do incidente é superior a 24 horas;

b) O tempo de indisponibilidade do serviço é superior a duas horas para os serviços de TIC que apoiam funções críticas ou importantes.

4. O limiar de materialidade para o critério de «distribuição geográfica» é atingido se o incidente tiver um impacto em dois ou mais Estados-Membros, em conformidade com o artigo 4.º.

5. O limiar de materialidade para o critério «perdas de dados» é atingido se estiver preenchida qualquer uma das seguintes condições:

a) Qualquer impacto, tal como referido no artigo 5.º, na disponibilidade, autenticidade, integridade ou confidencialidade dos dados tem ou virá a ter consequências negativas para a realização dos objetivos empresariais da entidade financeira ou para a sua capacidade para cumprir obrigações regulamentares;

b) Qualquer acesso bem-sucedido, mal-intencionado e não autorizado não abrangido pela alínea a) ocorre em sistemas de rede e de informação, sempre que esse acesso possa resultar em perdas de dados.

6. O limiar de materialidade para o critério «impacto económico» é atingido quando os custos e perdas incorridos pela entidade financeira causados pelo incidente excederem, ou for provável que excedam, 100 000 EUR.

CAPÍTULO III

CIBERAMEAÇAS SIGNIFICATIVAS

Artigo 10.º

Limiares de materialidade elevados para a determinação de ciberameaças significativas

Para efeitos do artigo 18.º, n.º 2, do Regulamento (UE) 2022/2554, uma ciberameaça é considerada significativa se estiverem preenchidas todas as condições seguintes:

a) A ciberameaça, caso ocorra, pode afetar ou ter afetado funções críticas ou importantes da entidade financeira, ou afetar outras entidades financeiras, terceiros prestadores, clientes ou contrapartes financeiras, com base nas informações de que a entidade financeira dispõe;

b) A ciberameaça tem uma elevada probabilidade de ocorrência na entidade financeira ou noutras entidades financeiras, tendo em conta, pelo menos, os seguintes elementos:

   i) riscos aplicáveis relacionados com a ciberameaça a que se refere a alínea a), incluindo potenciais vulnerabilidades dos sistemas da entidade financeira que possam ser exploradas,

   ii) as capacidades e a intenção dos autores de ameaças, na medida em que sejam do conhecimento da entidade financeira,

   iii) a persistência da ameaça e eventuais conhecimentos acumulados sobre incidentes que tenham afetado a entidade financeira ou o seu terceiro prestador, clientes ou contrapartes financeiras;

c) A ciberameaça, caso se tivesse concretizado, poderia preencher qualquer um dos seguintes critérios:

   i) o critério relativo à criticalidade dos serviços estabelecido no artigo 18.º, n.º 1, alínea e), do Regulamento (UE) 2022/2554, tal como especificado no artigo 6.º do presente regulamento,

   ii) o limiar de materialidade estabelecido no artigo 9.º, n.º 1,

   iii) o limiar de materialidade estabelecido no artigo 9.º, n.º 4.

Se, dependendo do tipo de ciberameaça e das informações disponíveis, a entidade financeira concluir que os limiares de materialidade estabelecidos no artigo 9.º, n.ºs 2, 3, 5 e 6, poderão ter sido atingidos, esses limiares podem também ser tidos em conta.

CAPÍTULO IV

RELEVÂNCIA DOS INCIDENTES DE CARÁTER SEVERO PARA AS AUTORIDADES COMPETENTES DE OUTROS ESTADOS-MEMBROS E PORMENORES DOS RELATÓRIOS A PARTILHAR COM OUTRAS AUTORIDADES COMPETENTES

Artigo 11.º

Relevância dos incidentes de caráter severo para as autoridades competentes de outros Estados-Membros

A avaliação da relevância do incidente de caráter severo para as autoridades competentes de outros Estados-Membros, tal como referido no artigo 19.º, n.º 7, do Regulamento (UE) 2022/2554, deve basear-se na determinação sobre se o incidente tem uma causa profunda com origem noutro Estado-Membro ou se o incidente tem ou teve um impacto significativo noutro Estado-Membro em qualquer um dos seguintes casos:

a) Clientes ou contrapartes financeiras;

b) Uma sucursal da entidade financeira ou outra entidade financeira pertencente ao grupo;

c) Uma infraestrutura do mercado financeiro ou um terceiro prestador que possa afetar entidades financeiras às quais presta serviços.

Artigo 12.º

Pormenores dos incidentes de caráter severo a partilhar com outras autoridades competentes

Os pormenores dos incidentes de caráter severo a comunicar pelas autoridades competentes a outras autoridades competentes nos termos do artigo 19.º, n.º 6, do Regulamento (UE) 2022/2554 e as notificações a apresentar pela EBA, pela ESMA ou pela EIOPA e pelo BCE às autoridades competentes relevantes de outros Estados-Membros nos termos do artigo 19.º, n.º 7, do mesmo regulamento devem conter o mesmo nível de informação, sem qualquer anonimização, que os relatórios e notificações de incidentes de caráter severo recebidos de entidades financeiras em conformidade com o artigo 19.º, n.º 4, do Regulamento (UE) 2022/2554.

CAPÍTULO V

DISPOSIÇÕES FINAIS

Artigo 13.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