Jornal Oficial
da União Europeia

PT
Série L

2025/301

20.2.2025

REGULAMENTO DELEGADO (UE) 2025/301 DA COMISSÃO

de 23 de outubro 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 e os prazos para a notificação inicial e os relatórios intercalar e final sobre incidentes de caráter severo relacionados com as TIC, bem como o conteúdo da notificação voluntária de ciberameaças significativas

(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 20.º, terceiro parágrafo,

Considerando o seguinte:

(1) A fim de assegurar a harmonização e a simplificação dos requisitos de notificação e comunicação de incidentes de caráter severo relacionados com as TIC a que se refere o artigo 19.º, n.º 4, do Regulamento (UE) 2022/2554, os prazos para a notificação de incidentes de caráter severo relacionados com as TIC deverão seguir uma abordagem coerente para todos os tipos de entidades financeiras. Por estas razões, os prazos também deverão seguir, tanto quanto possível, uma abordagem coerente com os requisitos estabelecidos na Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho ([2]) e ter um efeito pelo menos equivalente aos mesmos.

(2) A fim de evitar a imposição de encargos de comunicação indevidos às entidades financeiras no momento em que estas lidam com o incidente relacionado com as TIC, o conteúdo da notificação inicial deverá limitar-se às informações mais significativas. Para poderem tomar medidas de supervisão adequadas, as autoridades competentes devem receber informações sobre os incidentes de caráter severo relacionados com as TIC o mais rapidamente possível após a entidade financeira ter estabelecido essa classificação. Por conseguinte, o prazo para a apresentação de uma notificação inicial a que se refere o artigo 19.º, n.º 4, alínea a), do Regulamento (UE) 2022/2554 deverá ser o mais curto possível após a classificação de um incidente relacionado com as TIC como sendo de caráter severo, sem deixar de permitir flexibilidade, especialmente para modelos de negócio de serviços que não sejam particularmente críticos em termos de urgência, caso as entidades financeiras necessitem de mais tempo para tratar o incidente relacionado com as TIC após terem tomado conhecimento do mesmo.

(3) Após receberem a notificação inicial, as autoridades competentes deverão receber informações mais pormenorizadas sobre o incidente relacionado com as TIC no relatório intercalar e todas as informações pertinentes no relatório final. As informações constantes desses relatórios deverão permitir às autoridades competentes avaliar mais aprofundadamente o incidente relacionado com as TIC, bem como as medidas de supervisão que possam querer tomar.

(4) Os prazos de comunicação a que se refere o artigo 20.º, primeiro parágrafo, alínea a), subalínea ii), do Regulamento (UE) 2022/2554 deverão, por conseguinte, equilibrar a necessidade de as autoridades competentes receberem rapidamente as informações com a necessidade de proporcionar às entidades financeiras tempo suficiente para obterem informações completas e exatas.

(5) Tendo em conta os critérios estabelecidos no artigo 20.º, primeiro parágrafo, alínea a), do Regulamento (UE) 2022/2554, os prazos de comunicação não devem representar um encargo desproporcionado para as microempresas e outras entidades financeiras que não sejam significativas. Por outro lado, a fim de evitar encargos desproporcionados para as entidades financeiras, os prazos de comunicação deverão ter em conta os fins de semana e os feriados.

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

([2]) Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, relativa a medidas destinadas a garantir um elevado nível comum de cibersegurança na União que altera o Regulamento (UE) n.º 910/2014 e a Diretiva (UE) 2018/1972 e revoga a Diretiva (UE) 2016/1148 (Diretiva SRI 2) (JO L 333 de 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

(6) Uma vez que as ciberameaças significativas devem ser notificadas numa base voluntária, o conteúdo dessas notificações não deverá impor encargos às entidades financeiras e deverá ser mais limitado do que as informações solicitadas para incidentes de caráter severo relacionados com as TIC.

(7) O presente regulamento baseia-se nos projetos de normas técnicas de regulamentação apresentados à Comissão pelas Autoridades Europeias de Supervisão.

(8) As Autoridades Europeias de Supervisão realizaram consultas públicas abertas sobre os projetos de normas técnicas de regulamentação em que se baseia o presente regulamento, analisaram os potenciais custos e benefícios associados e solicitaram o parecer dos Grupos de Partes Interessadas criados em conformidade com o artigo 37.º dos Regulamentos (UE) n.º 1093/2010 ([3]), (UE) n.º 1094/2010 ([4]) e (UE) n.º 1095/2010 ([5]) do Parlamento Europeu e do Conselho.

(9) A Autoridade Europeia para a Proteção de Dados foi consultada nos termos do disposto no artigo 42.º, n.º 1, do Regulamento (UE) 2018/1725 do Parlamento Europeu e do Conselho ([6]) e emitiu parecer positivo em 22 de julho de 2024. Qualquer tratamento de dados pessoais abrangido pelo âmbito de aplicação do presente regulamento deverá ser efetuado em conformidade com os princípios e disposições aplicáveis em matéria de proteção de dados constantes do Regulamento (UE) 2018/1725,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Informações gerais a fornecer nas notificações iniciais e nos relatórios intercalares e finais sobre incidentes de caráter severo relacionados com as TIC

As entidades financeiras devem incluir na notificação inicial, no relatório intercalar e no relatório final, como referido no artigo 19.º, n.º 4, do Regulamento (UE) 2022/2554, as seguintes informações gerais:

a) O tipo de apresentação (notificação inicial, relatório intercalar ou relatório final);

b) O nome da entidade financeira, o seu código LEI e o tipo de entidade financeira, como referido no artigo 2.º, n.º 1, do Regulamento (UE) 2022/2554;

c) O nome e o código de identificação da entidade que apresenta a notificação inicial, o relatório intercalar ou o relatório final em nome da entidade financeira;

d) Se for caso disso, os nomes e códigos LEI de todas as entidades financeiras abrangidas pela notificação inicial, relatório intercalar ou relatório final agregados;

e) Os dados de contacto das pessoas responsáveis pela comunicação com a autoridade competente sobre o incidente de caráter severo relacionado com as TIC;

f) Se for caso disso, a identificação da empresa-mãe do grupo ao qual pertence a entidade financeira;

g) Em caso de impacto monetário, a divisa em que se baseiam os montantes.

([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).

Artigo 2.º

Informações específicas a fornecer nas notificações iniciais

As notificações iniciais a que se refere o artigo 19.º, n.º 4, alínea a), do Regulamento (UE) 2022/2554 devem conter, pelo menos, todas as seguintes informações específicas:

a) O código de referência atribuído ao incidente pela entidade financeira;

b) A data de deteção, a hora de deteção e a classificação do incidente, nos termos do artigo 8.º do Regulamento Delegado (UE) 2024/1772 da Comissão ([7]);

c) Uma descrição do incidente relacionado com as TIC;

d) Os critérios, estabelecidos nos artigos 1.º a 8.º do Regulamento Delegado (UE) 2024/1772, com base nos quais a entidade financeira classificou o incidente relacionado com as TIC como sendo de caráter severo;

e) Os Estados-Membros afetados pelo incidente relacionado com as TIC;

f) Informações sobre a forma como o incidente relacionado com as TIC foi detetado;

g) Se disponíveis, informações sobre a origem do incidente relacionado com as TIC;

h) Informações sobre se a entidade financeira ativou um plano de continuidade das atividades;

i) Se for caso disso, informações sobre a reclassificação do incidente relacionado com as TIC de caráter severo para de caráter não severo;

j) Se disponíveis, quaisquer outras informações pertinentes.

Artigo 3.º

Informações específicas a fornecer nos relatórios intercalares

Os relatórios intercalares a que se refere o artigo 19.º, n.º 4, alínea b), do Regulamento (UE) 2022/2554 devem conter, pelo menos, todas as seguintes informações específicas:

a) Se for caso disso, o código de referência do incidente fornecido pela autoridade competente;

b) A data e hora de ocorrência do incidente relacionado com as TIC;

c) Se for caso disso, a data e hora em que a entidade financeira retomou as suas atividades regulares;

d) Informações sobre como foram cumpridos os critérios estabelecidos nos artigos 1.º a 8.º do Regulamento Delegado (UE) 2024/1772, com base nos quais a entidade financeira classificou o incidente relacionado com as TIC como sendo de caráter severo;

e) O tipo de incidente relacionado com as TIC;

f) Se for caso disso, as ameaças e técnicas utilizadas pelo autor da ameaça;

g) Áreas funcionais e processos empresariais afetados;

h) Componentes afetados da infraestrutura de apoio aos processos operacionais;

i) Impacto nos interesses financeiros dos clientes;

j) Informações sobre a comunicação de incidentes relacionados com as TIC a outras autoridades;

k) Ações ou medidas temporárias tomadas ou previstas pela entidade financeira para recuperar do incidente relacionado com as TIC;

l) Se for caso disso, informações sobre os indicadores de exposição a riscos.

([7]) 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 (JO L, 2024/1772, 25.6.2024, ELI: http://data.europa.eu/eli/reg_del/2024/1772/oj).

Artigo 4.º

Informações específicas a fornecer nos relatórios finais

Os relatórios finais a que se refere o artigo 19.º, n.º 4, alínea c), do Regulamento (UE) 2022/2554 devem conter todas as seguintes informações específicas:

a) Informações sobre as causas profundas do incidente relacionado com as TIC;

b) Datas e horas em que o incidente relacionado com as TIC foi resolvido e em que foi (foram) abordada(s) a(s) causa(s) profunda(s);

c) Informações sobre a resolução do incidente relacionado com as TIC;

d) Se for caso disso, informações pertinentes para as autoridades de resolução;

e) Informações sobre os custos e perdas diretos e indiretos decorrentes do incidente relacionado com as TIC e informações sobre recuperações financeiras;

f) Se for caso disso, informações sobre incidentes relacionados com as TIC de caráter recorrente.

Artigo 5.º

Prazos para a notificação inicial e para os relatórios intercalar e final

1. As entidades financeiras devem apresentar a notificação inicial e os relatórios intercalar e final a que se refere o artigo 19.º, n.º 4, alíneas a), b) e c), do Regulamento (UE) 2022/2554 nos seguintes prazos:

a) Para o relatório inicial: o mais cedo possível, mas, em qualquer caso, no prazo de quatro horas a contar da classificação do incidente relacionado com as TIC como sendo um incidente de caráter severo relacionado com as TIC e o mais tardar 24 horas a contar do momento em que a entidade financeira tomou conhecimento do incidente relacionado com as TIC;

b) Para o relatório intercalar: o mais tardar no prazo de 72 horas a contar da apresentação da notificação inicial, mesmo que o estado ou o tratamento do incidente não se tenham alterado, conforme referido no artigo 19.º, n.º 4, alínea b), do Regulamento (UE) 2022/2554. As entidades financeiras devem apresentar um relatório intercalar atualizado sem demora injustificada e, em qualquer caso, quando as atividades regulares tiverem sido repostas;

c) Para o relatório final: o mais tardar um mês após a apresentação do relatório intercalar ou, se for o caso, após o último relatório intercalar atualizado.

2. Se a entidade financeira não tiver classificado um incidente relacionado com as TIC como sendo de caráter severo no prazo de 24 horas a contar do momento em que tomou conhecimento do incidente relacionado com as TIC, mas classificar esse incidente relacionado com as TIC como sendo de caráter severo numa fase posterior, deve apresentar a notificação inicial no prazo de quatro horas a contar da classificação do incidente relacionado com as TIC como sendo um incidente de caráter severo.

3. As entidades financeiras que não possam apresentar a notificação inicial, o relatório intercalar ou o relatório final nos prazos estabelecidos no n.º 1 devem informar a autoridade competente desse facto sem demora injustificada, mas o mais tardar nos respetivos prazos para a apresentação da notificação ou do relatório, e devem explicar as razões do atraso.

4. Se o prazo para a apresentação de uma notificação inicial, de um relatório intercalar ou de um relatório final coincidir com um dia de fim de semana ou um feriado no Estado-Membro da entidade financeira que apresenta a comunicação, esta pode apresentar a notificação inicial ou os relatórios intercalar ou final até ao meio-dia do dia útil seguinte.

5. O n.º 4 não se aplica à apresentação de uma notificação inicial ou de um relatório intercalar por instituições de crédito, contrapartes centrais, operadores de plataformas de negociação e outras entidades financeiras identificadas como entidades essenciais ou importantes nos termos do artigo 3.º da Diretiva (UE) 2022/2555.

6. As autoridades competentes podem decidir que o n.º 4 não se aplica à apresentação de uma notificação inicial ou de um relatório intercalar por entidades financeiras, com exceção das referidas no n.º 5, que sejam significativas ou tenham um caráter sistémico para o setor financeiro a nível nacional ou da União. As autoridades competentes notificam a sua decisão às entidades financeiras identificadas. A decisão da autoridade competente só é aplicável em relação aos incidentes comunicados após a data de notificação da decisão pela autoridade competente às entidades financeiras identificadas.

Artigo 6.º

Conteúdo da notificação voluntária de ciberameaças significativas

O conteúdo da notificação voluntária sobre ciberameaças significativas a que se refere o artigo 19.º, n.º 2, do Regulamento (UE) 2022/2554 deve abranger todos os seguintes elementos:

a) Informações gerais sobre a entidade financeira que apresenta a notificação, conforme previsto no artigo 1.º;

b) A data e hora da deteção da ciberameaça significativa e quaisquer outros carimbos temporais pertinentes relacionados com a ciberameaça significativa;

c) Uma descrição da ciberameaça significativa;

d) Informação sobre o potencial impacto da ciberameaça significativa na entidade financeira, nos seus clientes ou em contrapartes financeiras;

e) Os critérios de classificação que teriam desencadeado um relatório de incidente de caráter severo previsto nos artigos 1.º a 8.º do Regulamento Delegado (UE) 2024/1772 se a ciberameaça se tivesse materializado;

f) Informações sobre o estado da ciberameaça significativa e quaisquer alterações na atividade de ameaça;

g) Se for caso disso, uma descrição das medidas tomadas pela entidade financeira para impedir a materialização das ciberameaças significativas;

h) Informações sobre qualquer notificação da ciberameaça significativa a outras entidades financeiras ou autoridades;

i) Se for caso disso, informações sobre os indicadores de exposição a riscos;

j) Se disponíveis, quaisquer outras informações pertinentes.

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 23 de outubro de 2024.

Pela Comissão
A Presidente
Ursula VON DER LEYEN