REGULAMENTO DE EXECUÇÃO (UE) 2025/302 DA COMISSÃO

de 23 de outubro de 2024

que estabelece normas técnicas de execução para a aplicação do Regulamento (UE) 2022/2554 do Parlamento Europeu e do Conselho no que respeita aos formulários, modelos e procedimentos normalizados que as entidades financeiras devem utilizar para comunicar incidentes de caráter severo relacionados com as TIC e notificar uma ciberameaça significativa

(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, quarto parágrafo,

Considerando o seguinte:

(1) A fim de assegurar que as entidades financeiras comunicam os incidentes de caráter severo às respetivas autoridades competentes de forma coerente, bem como assegurar que fornecem a essas autoridades dados de boa qualidade, importa especificar quais os campos de dados que as entidades financeiras devem fornecer nas várias fases da comunicação a que se refere o artigo 19.º, n.º 4, do Regulamento (UE) 2022/2554. É importante que essas informações sejam apresentadas de forma que permita uma visão única do incidente. Por conseguinte, é necessário estabelecer um modelo único de comunicação para esses efeitos.

(2) As entidades financeiras deverão preencher os campos de dados do modelo de comunicação que correspondem aos requisitos de informação da respetiva notificação ou relatório. No entanto, as entidades financeiras que já disponham de informações que devem fornecer numa fase posterior da comunicação, ou seja, nos relatórios intercalar ou final, deverão ser autorizadas a antecipar a apresentação dos dados.

(3) Uma vez que incidentes múltiplos ou recorrentes podem constituir um incidente de caráter severo, conforme referido no artigo 8.º do Regulamento Delegado (UE) 2024/1772 da Comissão ([2]), a conceção do modelo de comunicação e dos campos de dados deverá permitir que as entidades financeiras comuniquem esses incidentes recorrentes.

(4) A fim de assegurar informações exatas e atualizadas, o modelo de comunicação deverá permitir às entidades financeiras, aquando da apresentação do relatório intercalar e do relatório final, atualizarem todas as informações apresentadas anteriormente e, se necessário, reclassificarem os incidentes de caráter severo como incidentes de caráter não severo.

(5) A identificação jurídica das entidades deverá ser alinhada com os identificadores especificados nas normas técnicas de execução adotadas nos termos do artigo 28.º, n.º 9, do Regulamento (UE) 2022/2554.

(6) Caso as entidades financeiras subcontratem a terceiros as obrigações de comunicação de incidentes de caráter severo relacionados com as TIC, as autoridades competentes deverão ter conhecimento da identidade do terceiro que efetua a comunicação em nome da entidade financeira, antes da apresentação da primeira notificação ou comunicação, a fim de verificar a legitimidade do terceiro que efetua a comunicação.

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

([2]) 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).

(7) A fim de identificar facilmente o impacto de um incidente ocorrido ou causado por um terceiro prestador de serviços e que afete várias entidades financeiras num único Estado-Membro, bem como de reduzir o esforço de comunicação para as entidades financeiras, o modelo de comunicação deverá permitir a apresentação de um relatório agregado que abranja informações agregadas sobre o impacto do incidente em todas as entidades financeiras afetadas que classificaram o incidente como sendo de caráter severo.

(8) O modelo de comunicação deverá ser concebido de forma tecnologicamente neutra, a fim de permitir a sua aplicação no quadro de várias soluções de comunicação de incidentes já existentes ou que possam ser desenvolvidas para a aplicação dos requisitos do Regulamento (UE) 2022/2554.

(9) A conceção do modelo de comunicação e dos campos de dados deverá facilitar a comunicação de incidentes de caráter severo relacionados com as TIC por terceiros a quem as entidades financeiras subcontrataram a sua obrigação de comunicação em conformidade com o artigo 19.º, n.º 5, do Regulamento (UE) 2022/2554.

(10) O presente regulamento baseia-se no projeto de normas técnicas de execução apresentado à Comissão pelas Autoridades Europeias de Supervisão.

(11) As Autoridades Europeias de Supervisão realizaram consultas públicas abertas sobre os projetos de normas técnicas de execução em que se baseia o presente regulamento, analisaram os potenciais custos e benefícios associados e solicitaram o parecer do Grupo das Partes Interessadas do Setor Bancário criado 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.

(12) 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 estabelecidos no Regulamento (UE) 2018/1725,

ADOTOU O PRESENTE REGULAMENTO:

Artigo 1.º

Modelo para a comunicação de incidentes de caráter severo relacionados com as TIC

1. As entidades financeiras devem utilizar o modelo estabelecido no anexo I para apresentar a notificação inicial, o relatório intercalar e o relatório final a que se refere o artigo 19.º, n.º 4, do Regulamento (UE) 2022/2554 do seguinte modo:

a) As entidades financeiras que apresentem uma notificação inicial devem preencher os campos de dados do modelo que correspondem às informações a fornecer em conformidade com o artigo 2.º do Regulamento Delegado (UE) 2025/301 da Comissão ([7]), e podem, caso já disponham dessas informações, preencher campos de dados cujo preenchimento não seja necessário para uma notificação inicial, mas seja exigido para um relatório intercalar ou final;

([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).

([7]) 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 (JO L 2025/301, de 21.11.2018, ELI: http://data.europa.eu/eli/reg_del/2025/301/oj).

b) As entidades financeiras que apresentem um relatório intercalar devem preencher os campos de dados do modelo que correspondem às informações a fornecer em conformidade com o artigo 3.º do Regulamento Delegado (UE) 2025/301, e podem, caso já disponham das informações pertinentes, preencher campos de dados cujo preenchimento não seja exigido para uma notificação inicial, mas seja exigido para o relatório final.

c) As entidades financeiras que apresentem um relatório final devem preencher os campos de dados do modelo que correspondem às informações a fornecer em conformidade com o artigo 4.º do Regulamento Delegado (UE) 2025/301.

2. As entidades financeiras devem assegurar que as informações contidas na notificação inicial, bem como nos relatórios intercalar e final, sejam completas e exatas.

3. As entidades financeiras devem fornecer valores estimados com base noutros dados e informações disponíveis, na medida do possível, caso não estejam disponíveis dados exatos no momento da comunicação para a notificação inicial ou para o relatório intercalar.

4. Ao apresentarem um relatório intercalar ou final, as entidades financeiras devem utilizar o modelo estabelecido no anexo I para apresentar todas as informações exigidas e atualizar, quando aplicável, as informações anteriormente fornecidas na notificação inicial ou no relatório intercalar.

5. Ao preencherem o modelo estabelecido no anexo I, as entidades financeiras devem seguir o glossário de dados e as instruções constantes do anexo II.

Artigo 2.º

Apresentação conjunta da notificação inicial e dos relatórios intercalar e final

As entidades financeiras podem combinar a apresentação da notificação inicial, do relatório intercalar e do relatório final, fornecendo dois deles ou todos em simultâneo, desde que as atividades regulares tenham sido retomadas ou a análise das causas profundas tenha sido concluída e que sejam cumpridos os prazos estabelecidos no artigo 5.º do Regulamento Delegado (UE) 2025/301.

Artigo 3.º

Incidentes recorrentes relacionados com as TIC

As entidades financeiras que fornecem informações sobre incidentes recorrentes de caráter não severo relacionados com as TIC que preencham cumulativamente as condições para um incidente de caráter severo relacionado com as TIC, conforme estabelecido no artigo 8.º, n.º 2, do Regulamento Delegado (UE) 2024/1772, devem fornecer essas informações de forma agregada.

Artigo 4.º

Utilização de canais eletrónicos seguros

1. As entidades financeiras devem utilizar canais eletrónicos seguros disponibilizados pela respetiva autoridade competente para apresentarem a notificação inicial e os relatórios intercalar e final.

2. As entidades financeiras que não consigam utilizar os canais eletrónicos seguros disponibilizados pela respetiva autoridade competente devem informar essa autoridade de um incidente de caráter severo relacionado com as TIC através de outros meios seguros, com o acordo da autoridade competente. Se a autoridade competente assim o exigir, as entidades financeiras devem voltar a apresentar a notificação inicial, o relatório intercalar ou o relatório final através do canal eletrónico seguro disponibilizado pela respetiva autoridade competente, logo que estejam em condições de o fazer.

Artigo 5.º

Reclassificação de incidentes de caráter severo relacionados com as TIC

Se, após uma avaliação mais aprofundada, a entidade financeira concluir que o incidente relacionado com as TIC anteriormente comunicado como sendo de caráter severo não cumpriu, em momento algum, os critérios de classificação e os limiares estabelecidos no artigo 8.º do Regulamento Delegado (UE) 2024/1772, deve comunicar à autoridade competente que reclassificou o incidente relacionado com as TIC de caráter severo para caráter não severo, fornecendo as informações sobre essa reclassificação no modelo estabelecido no anexo II do presente regulamento em relação aos campos «tipo de relatório» e «outras informações».

Artigo 6.º

Notificação da subcontratação das obrigações de comunicação

1. As entidades financeiras que subcontrataram a obrigação de comunicar incidentes de caráter severo relacionados com as TIC em conformidade com o artigo 19.º, n.º 5, do Regulamento (UE) 2022/2554 devem informar a respetiva autoridade competente desse acordo de subcontratação assim que o acordo de subcontratação é celebrado e, o mais tardar, antes da primeira notificação ou comunicação.

2. As entidades financeiras devem fornecer à autoridade competente o nome, os dados de contacto e o código de identificação do terceiro que apresentará em seu nome as notificações ou relatórios de incidentes de caráter severo relacionados com as TIC.

3. As entidades financeiras devem informar a respetiva autoridade competente logo que deixem de subcontratar as suas obrigações de comunicação a que se refere o artigo 19.º, n.º 5, do Regulamento (UE) 2022/2554.

Artigo 7.º

Comunicação agregada

1. Um terceiro prestador de serviços ao qual tenham sido subcontratadas obrigações de comunicação conforme referido no artigo 19.º, n.º 5, do Regulamento (UE) 2022/2554 pode utilizar o modelo constante do anexo I do presente regulamento para fornecer informações agregadas sobre um incidente de caráter severo relacionado com as TIC que afete várias entidades financeiras numa única notificação ou relatório e apresentar essa notificação ou comunicação à autoridade competente em nome de todas as entidades financeiras afetadas, desde que estejam preenchidas todas as seguintes condições:

a) O incidente de caráter severo relacionado com as TIC a comunicar tem origem ou é causado por um terceiro prestador de serviços de TIC;

b) Esse terceiro prestador de serviços presta o serviço de TIC relevante a mais do que uma entidade financeira ou a um grupo;

c) O incidente relacionado com as TIC é classificado como sendo de caráter severo por cada entidade financeira abrangida pela notificação ou relatório agregado;

d) O incidente de caráter severo relacionado com as TIC afeta entidades financeiras num único Estado-Membro e o relatório agregado diz respeito a entidades financeiras que são supervisionadas pela mesma autoridade competente;

e) As autoridades competentes autorizaram explicitamente este tipo de entidades financeiras a agregar os seus relatórios.

2. O n.º 1 não se aplica a instituições de crédito consideradas de relevância significativa, conforme referido no artigo 2.º, ponto 16, do Regulamento (UE) n.º 468/2014 do Banco Central Europeu ([8]), a operadores de plataformas de negociação e a contrapartes centrais, que só devem utilizar o modelo constante do anexo I para apresentar notificações ou relatórios de incidentes de caráter severo relacionados com as TIC individualmente à respetiva autoridade competente.

3. Caso as autoridades competentes exijam informações sobre o impacto individual do incidente de caráter severo relacionado com as TIC numa única entidade financeira, a entidade financeira deve, a pedido da autoridade competente, apresentar uma notificação individual ou um relatório sobre o incidente de caráter severo relacionado com as TIC.

([8]) Regulamento (UE) n.º 468/2014 do Banco Central Europeu, de 16 de abril de 2014, que estabelece o quadro de cooperação, no âmbito do Mecanismo Único de Supervisão, entre o Banco Central Europeu e as autoridades nacionais competentes e com as autoridades nacionais designadas (Regulamento-Quadro do MUS) (BCE/2014/17) (JO L 141 de 14.5.2014, p. 1, ELI: http://data.europa.eu/eli/reg/2014/468/oj).

Artigo 8.º

Notificação de ciberameaças significativas

1. As entidades financeiras que notificam ciberameaças significativas às autoridades competentes em conformidade com o artigo 19.º, n.º 2, do Regulamento (UE) 2022/2554 devem utilizar o modelo estabelecido no anexo III do presente regulamento e seguir o glossário de dados e as instruções constantes do anexo IV do presente regulamento.

2. As entidades financeiras devem assegurar que as informações contidas na notificação de ciberameaças significativas sejam completas e exatas.

Artigo 9.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

ANEXO I

MODELOS PARA A COMUNICAÇÃO DE INCIDENTES DE CARÁTER SEVERO

Número do campo	Campo de dados	
Informações gerais acerca da entidade financeira		
1.1	Tipo de apresentação	
1.2	Nome da entidade que apresenta o relatório	
1.3	Código de identificação da entidade que apresenta o relatório	
1.4	Tipo de entidade financeira afetada	
1.5	Nome da entidade financeira afetada	
1.6	Código LEI da entidade financeira afetada	
1.7	Nome da pessoa de contacto principal	
1.8	Endereço de correio eletrónico da pessoa de contacto principal	
1.9	Telefone da pessoa de contacto principal	
1.10	Nome da pessoa de contacto secundária	
1.11	Endereço de correio eletrónico da pessoa de contacto secundária	
1.12	Telefone da pessoa de contacto secundária	
1.13	Nome da empresa-mãe em última instância	
1.14	Código LEI da empresa-mãe em última instância	
1.15	Moeda utilizada na comunicação	
Conteúdo da notificação inicial		
2.1	Código de referência do incidente atribuído pela entidade financeira	
2.2	Data e hora de deteção do incidente de caráter severo relacionado com as TIC	
2.3	Data e hora de classificação do incidente relacionado com as TIC como sendo de caráter severo	
2.4	Descrição do incidente de caráter severo relacionado com as TIC	
2.5	Critérios de classificação que desencadearam a comunicação do incidente	
2.6	Limiares de materialidade para o critério de classificação «Distribuição geográfica»	
2.7	Deteção do incidente de caráter severo relacionado com as TIC	

Número do campo	Campo de dados	
2.8	Indicação sobre se o incidente de caráter severo relacionado com as TIC tem origem num terceiro prestador ou noutra entidade financeira	
2.9	Ativação do plano de continuidade das atividades, se ativado	
2.10	Outras informações pertinentes	
Conteúdo do relatório intercalar		
3.1	Código de referência do incidente fornecido pela autoridade competente	
3.2	Data e hora de ocorrência do incidente de caráter severo relacionado com as TIC	
3.3	Data e hora da recuperação dos serviços, das atividades ou das operações	
3.4	Número de clientes afetados	
3.5	Percentagem de clientes afetados	
3.6	Número de contrapartes financeiras afetadas	
3.7	Percentagem de contrapartes financeiras afetadas	
3.8	Impacto nos clientes ou contrapartes financeiras pertinentes	
3.9	Número de operações afetadas	
3.10	Percentagem de operações afetadas	
3.11	Valor das operações afetadas	
3.12	Informação sobre se os números são reais ou estimados, ou se houve ou não impacto	
3.13	Impacto em termos de reputação	
3.14	Informações contextuais sobre o impacto em termos de reputação	
3.15	Duração do incidente de caráter severo relacionado com as TIC	
3.16	Tempo de indisponibilidade do serviço	
3.17	Informações sobre se os números relativos à duração e ao tempo de indisponibilidade do serviço são reais ou estimados.	
3.18	Tipos de impacto nos Estados-Membros	
3.19	Descrição da forma como o incidente de caráter severo relacionado com as TIC tem impacto noutros Estados-Membros	
3.20	Limiares de materialidade para o critério de classificação «Perdas de dados»	
3.21	Descrição das perdas de dados	

Número do campo	Campo de dados	
3.22	Critério de classificação «Serviços críticos afetados»	
3.23	Tipo do incidente de caráter severo relacionado com as TIC	
3.24	Outros tipos de incidentes	
3.25	Ameaças e técnicas utilizadas pelo autor da ameaça	
3.26	Outros tipos de técnicas	
3.27	Informações sobre as áreas funcionais e os processos operacionais afetados	
3.28	Componentes afetados da infraestrutura de apoio aos processos operacionais	
3.29	Informações sobre os componentes afetados da infraestrutura de apoio aos processos operacionais	
3.30	Impacto nos interesses financeiros dos clientes	
3.31	Comunicação a outras autoridades	
3.32	Especificação de «outras» autoridades	
3.33	Ações/medidas temporárias tomadas ou previstas para recuperar do incidente	
3.34	Descrição de quaisquer ações e medidas temporárias tomadas ou previstas para recuperar do incidente	
3.35	Indicadores de exposição a riscos	
Conteúdo do relatório final		
4.1	Classificação de alto nível das causas profundas do incidente	
4.2	Classificação pormenorizada das causas profundas do incidente	
4.3	Classificação adicional das causas profundas do incidente	
4.4	Outros tipos de causas profundas	
4.5	Informações sobre as causas profundas do incidente	
4.6	Resumo da resolução do incidente	
4.7	Data e hora em que foi abordada a causa profunda do incidente	
4.8	Data e hora em que o incidente foi resolvido	
4.9	Informação sobre se a data de resolução permanente do incidente difere da data de execução inicialmente prevista	
4.10	Avaliação do risco para as funções críticas para efeitos de resolução	
4.11	Informações pertinentes para as autoridades de resolução	

Número do campo	Campo de dados	
4.12	Limiar de materialidade para o critério de classificação «Impacto económico»	
4.13	Montante dos custos e perdas brutos diretos e indiretos	
4.14	Montante das recuperações financeiras	
4.15	Informações sobre se os incidentes de caráter não severo são recorrentes	
4.16	Data e hora de ocorrência de incidentes recorrentes	

ANEXO II

GLOSSÁRIO DE DADOS E INSTRUÇÕES PARA A COMUNICAÇÃO DE INCIDENTES DE CARÁTER SEVERO

Campo de dados		Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
Informações gerais acerca da entidade financeira						
1.1.	Tipo de apresentação	Indicar o tipo de notificação ou relatório de incidente apresentado à autoridade competente.	Sim	Sim	Sim	Escolha: — notificação inicial, — relatório intercalar, — relatório final, — incidente de caráter severo reclassificado como sendo de caráter não severo.
1.2.	Nome da entidade que apresenta o relatório	Denominação legal completa da entidade que apresenta o relatório.	Sim	Sim	Sim	Alfanumérico
1.3.	Código de identificação da entidade que apresenta o relatório	Código de identificação da entidade que apresenta o relatório. Quando a notificação/o relatório for apresentada/o por uma entidade financeira, o código de identificação deve ser um identificador de entidade jurídica (LEI), que é um código único de 20 carateres alfanuméricos, com base na norma ISO 17442-1:2020 Um terceiro prestador de serviços que apresente um relatório em nome de uma entidade financeira pode utilizar um código de identificação como especificado nas normas técnicas de execução adotadas nos termos do artigo 28.º, n.º 9, do Regulamento (UE) 2022/2554.	Sim	Sim	Sim	Alfanumérico
1.4.	Tipo da entidade financeira afetada	Tipo da entidade a que se refere o artigo 2.º, n.º 1, alíneas a) a t), do Regulamento (UE) 2022/2554, relativamente à qual o relatório é apresentado. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, selecionar os diferentes tipos de entidades financeiras abrangidas pelo relatório agregado.	Sim	Sim	Sim	Escolha (escolha múltipla): — instituição de crédito, — instituição de pagamento, — instituição de pagamento isenta, — prestador de serviços de informação sobre contas, — instituição de moeda eletrónica, — instituição de moeda eletrónica isenta, — empresa de investimento, — prestador de serviços de criptoativos, — emitente de criptofichas referenciadas a ativos, — central de valores mobiliários, — contraparte central, — plataforma de negociação, — repositório de transações,

Campo de dados		Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
						— gestor de fundos de investimento alternativos, — sociedade gestora, — prestador de serviços de comunicação de dados, — empresa de seguros e de resseguros, — mediador de seguros, mediador de resseguros e mediador de seguros a título acessório, — instituição de realização de planos de pensões profissionais, — agência de notação de risco, — administrador de índices de referência críticos, — prestador de serviços de financiamento colaborativo, — repositório de titularizações.
1.5.	Nome da entidade financeira afetada	Denominação legal completa da entidade financeira afetada pelo incidente de caráter severo relacionado com as TIC e obrigada a comunicá-lo à respetiva autoridade competente nos termos do artigo 19.º do Regulamento (UE) 2022/2554. Em caso de comunicação agregada: a) Lista de todos os nomes das entidades financeiras afetadas pelo incidente de caráter severo relacionado com as TIC, separados por ponto e vírgula; b) O terceiro prestador de serviços que apresenta um relatório ou notificação de incidente de caráter severo de forma agregada, conforme referido no artigo 7.º do presente regulamento, deve enumerar os nomes de todas as entidades financeiras afetadas pelo incidente, separados por ponto e vírgula.	Sim, se a entidade financeira afetada pelo incidente for diferente da entidade que apresenta o relatório e em caso de comunicação agregada.	Sim, se a entidade financeira afetada pelo incidente for diferente da entidade que apresenta o relatório e em caso de comunicação agregada	Sim, se a entidade financeira afetada pelo incidente for diferente da entidade que apresenta o relatório e em caso de comunicação agregada	Alfanumérico
1.6.	Código LEI da entidade financeira afetada	Identificador de entidade jurídica (LEI) da entidade financeira afetada pelo incidente de caráter severo relacionado com as TIC, atribuído em conformidade com a Organização Internacional de Normalização. Em caso de comunicação agregada: a) Uma lista de todos os códigos LEI das entidades financeiras afetadas pelo incidente de caráter severo relacionado com as TIC, separados por ponto e vírgula;	Sim, se a entidade financeira afetada pelo incidente de caráter severo relacionado	Sim, se a entidade financeira afetada pelo incidente de caráter severo relacionado com as TIC for	Sim, se a entidade financeira afetada pelo incidente de caráter severo relacionado	Código único de 20 carateres alfanuméricos, com base na norma ISO 17442-1:2020

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	b) O terceiro prestador de serviços que apresenta uma notificação de incidente de caráter severo ou de forma agregada, conforme referido no artigo 7.º do presente regulamento, deve enumerar os códigos LEI de todas as entidades financeiras afetadas pelo incidente, separados por ponto e vírgula. A ordem de apresentação dos códigos LEI e dos nomes das entidades financeiras deve ser idêntica.	com as TIC for diferente da entidade que apresenta o relatório e em caso de comunicação agregada.	diferente da entidade que apresenta o relatório e em caso de comunicação agregada.	com as TIC for diferente da entidade que apresenta o relatório e em caso de comunicação agregada	
1.7. Nome da pessoa de contacto principal	Nome e apelido da pessoa de contacto principal da entidade financeira. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, o nome da pessoa de contacto principal na entidade que apresenta o relatório agregado.	Sim	Sim	Sim	Alfanumérico
1.8. Endereço de correio eletrónico da pessoa de contacto principal	Endereço eletrónico da pessoa de contacto principal que pode ser utilizado pela autoridade competente para a comunicação de seguimento. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, o endereço eletrónico da pessoa de contacto principal na entidade que apresenta o relatório agregado.	Sim	Sim	Sim	Alfanumérico
1.9. Telefone da pessoa de contacto principal	Número de telefone da pessoa de contacto principal que pode ser utilizado pela autoridade competente para a comunicação de seguimento. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, o número de telefone da pessoa de contacto principal na entidade que apresenta o relatório agregado. O número de telefone deve ser comunicado com todos os prefixos internacionais (por exemplo, +33XXXXXXXXX).	Sim	Sim	Sim	Alfanumérico
1.10. Nome da pessoa de contacto secundária	Nome e apelido da pessoa de contacto secundária ou nome da equipa responsável da entidade financeira ou de uma entidade que apresenta o relatório em nome da entidade financeira.	Sim	Sim	Sim	Alfanumérico
1.11. Endereço de correio eletrónico da pessoa de contacto secundária	Endereço de correio eletrónico da pessoa de contacto secundária ou um endereço de correio eletrónico funcional da equipa que pode ser utilizado pela autoridade competente para a comunicação de seguimento.	Sim	Sim	Sim	Alfanumérico

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
1.12. Telefone da pessoa de contacto secundária	Número de telefone da pessoa de contacto secundária, ou de uma equipa, que pode ser utilizado pela autoridade competente para a comunicação de seguimento. O número de telefone deve ser comunicado com todos os prefixos internacionais (por exemplo, +33XXXXXXXXX).	Sim	Sim	Sim	Alfanumérico
1.13. Nome da empresa-mãe em última instância	Nome da empresa-mãe em última instância do grupo a que a entidade financeira afetada pertence, se aplicável.	Sim, se a EF pertencer a um grupo	Sim, se a EF pertencer a um grupo	Sim, se a EF pertencer a um grupo	Alfanumérico
1.14. Código LEI da empresa-mãe em última instância	LEI da empresa-mãe em última instância do grupo a que a entidade financeira afetada pertence, se aplicável. Atribuído em conformidade com a Organização Internacional de Normalização.	Sim, se a EF pertencer a um grupo	Sim, se a EF pertencer a um grupo	Sim, se a EF pertencer a um grupo	Código único de 20 carateres alfanuméricos, com base na norma ISO 17442-1:2020
1.15. Moeda utilizada na comunicação	Moeda utilizada para a comunicação de incidentes.	Sim	Sim	Sim	Escolha a preencher utilizando os códigos da norma ISO 4217 para as diferentes moedas

Conteúdo da notificação inicial

2.1. Código de referência do incidente atribuído pela entidade financeira	Código de referência único, emitido pela entidade financeira, que identifica inequivocamente o incidente de caráter severo relacionado com as TIC. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, o código de referência do incidente atribuído pelo terceiro prestador de serviços.	Sim	Sim	Sim	Alfanumérico
2.2. Data e hora de deteção do incidente relacionado com as TIC	Data e hora em que a entidade financeira tomou conhecimento do incidente relacionado com as TIC. No caso de incidentes recorrentes, a data e hora em que foi detetado o último incidente relacionado com as TIC.	Sim	Sim	Sim	Norma ISO 8601 UTC (AAAA-MM-DD hh:mm:ss)

	Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
2.3.	Data e hora de classificação do incidente como sendo de caráter severo	Data e hora em que o incidente relacionado com as TIC foi classificado como sendo de caráter severo de acordo com os critérios de classificação estabelecidos no Regulamento Delegado (UE) 2024/1772.	Sim	Sim	Sim	Norma ISO 8601 UTC (AAAA-MM-DD hh:mm:ss)
2.4.	Descrição do incidente relacionado com as TIC	Descrição dos aspetos mais pertinentes do incidente de caráter severo relacionado com as TIC. As entidades financeiras devem fornecer uma panorâmica geral das seguintes informações, tais como possíveis causas, impactos imediatos, sistemas afetados e outras. As entidades financeiras devem incluir, sempre que tal seja conhecido ou razoavelmente previsto, se o incidente afeta terceiros prestadores de serviços ou outras entidades financeiras, o tipo de prestador de serviços ou entidade financeira, o seu nome, os respetivos códigos de identificação e o tipo de código de identificação (por exemplo, LEI ou EUID). Em relatórios subsequentes, o conteúdo do campo pode evoluir ao longo do tempo para refletir a compreensão atualizada do incidente relacionado com as TIC e descrever quaisquer outras informações pertinentes sobre o incidente relacionado com as TIC não captadas pelos campos de dados, incluindo a avaliação interna da gravidade pela entidade financeira (por exemplo, muito baixa, baixa, média, elevada, muito elevada) e uma indicação do nível e do nome das estruturas de decisão mais elevadas que estiveram envolvidas na resposta ao incidente relacionado com as TIC.	Sim	Sim	Sim	Alfanumérico
2.5.	Critérios de classificação que desencadearam a comunicação do incidente	Critérios de classificação ao abrigo do Regulamento Delegado (UE) 2024/1772 que desencadearam a determinação do incidente relacionado com as TIC como sendo de caráter severo e a subsequente notificação e comunicação. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, os critérios de classificação que desencadearam a determinação do incidente relacionado com as TIC como sendo de caráter severo para, pelo menos, uma ou mais entidades financeiras.	Sim	Sim	Sim	Escolha (múltipla): — clientes, contrapartes financeiras e operações afetadas, — impacto em termos de reputação, — duração e tempo de indisponibilidade do serviço, — distribuição geográfica, — perdas de dados, — serviços críticos afetados, — impacto. económico.
2.6.	Limiares de materialidade para o critério de classificação «Distribuição geográfica»	Estados-Membros do EEE afetados pelo incidente de caráter severo relacionado com as TIC. Ao avaliar o impacto do incidente de caráter severo relacionado com as TIC noutros Estados-Membros, as entidades financeiras devem ter em conta os artigos 4.º e 12.° do Regulamento Delegado (UE) 2024/1772.	Sim, se for atingido o limiar de «Distribuição geográfica»	Sim, se for atingido o limiar de «Distribuição geográfica»	Sim, se for atingido o limiar de «Distribuição geográfica»	Escolha (múltipla) a preencher utilizando os códigos dos países afetados de acordo com a norma ISO 3166 ALPHA-2

	Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
2.7.	Deteção do incidente de caráter severo relacionado com as TIC	Indicação da forma como o incidente de caráter severo relacionado com as TIC foi detetado.	Sim	Sim	Sim	Escolha: — segurança informática, — pessoal, — auditoria interna, — auditoria externa, — clientes, — contrapartes financeiras, — terceiro prestador de serviços, — atacante, — sistemas de monitorização, — autoridade/agência/organismo de aplicação da lei, — outros.
2.8.	Indicação sobre se o incidente tem origem num terceiro prestador ou noutra entidade financeira	Indicação sobre se o incidente de caráter severo relacionado com as TIC tem origem num terceiro prestador ou noutra entidade financeira. As entidades financeiras devem indicar se o incidente de caráter severo relacionado com as TIC tem origem num terceiro prestador ou noutra entidade financeira (incluindo entidades financeiras pertencentes ao mesmo grupo que a entidade que apresenta a comunicação), bem como o nome, o código de identificação do terceiro prestador ou da entidade financeira e o tipo desse código de identificação (por exemplo, LEI ou EUID).	Sim, se o incidente tiver origem num terceiro prestador de serviços ou noutra entidade financeira	Sim, se o incidente tiver origem num terceiro prestador de serviços ou noutra entidade financeira	Sim, se o incidente tiver origem num terceiro prestador de serviços ou noutra entidade financeira	Alfanumérico
2.9.	Ativação do plano de continuidade das atividades, se ativado	Indicação sobre se foi realizada a ativação formal das medidas de resposta para assegurar a continuidade das atividades da entidade financeira.	Sim	Sim	Sim	Booliano (Sim ou Não)
2.10.	Outras informações pertinentes	Quaisquer outras informações não abrangidas pelo modelo. As entidades financeiras que reclassificaram um incidente de caráter severo relacionado com as TIC como sendo de caráter não severo devem descrever as razões pelas quais o incidente relacionado com as TIC não cumpre, nem se prevê que cumpra, os critérios para ser considerado um incidente de caráter severo relacionado com as TIC.	Sim, se existirem outras informações não abrangidas pelo modelo	Sim, se existirem outras informações não abrangidas pelo modelo ou se o incidente de	Sim, se existirem outras informações não abrangidas pelo modelo ou	Alfanumérico

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
		ou se o incidente de caráter severo relacionado com as TIC tiver sido reclassificado como sendo de caráter não severo	caráter severo relacionado com as TIC tiver sido reclassificado como sendo de caráter não severo	se o incidente de caráter severo relacionado com as TIC tiver sido reclassificado como sendo de caráter não severo	
Conteúdo do relatório intercalar					
3.1. Código de referência do incidente fornecido pela autoridade competente	Código de referência único atribuído pela autoridade competente no momento da receção da notificação inicial para identificar inequivocamente o incidente de caráter severo relacionado com as TIC.	Não	Sim, se aplicável	Sim, se aplicável	Alfanumérico
3.2. Data e hora de ocorrência do incidente	Data e hora em que ocorreu o incidente de caráter severo relacionado com as TIC, se diferente do momento em que a entidade financeira tomou conhecimento do incidente de caráter severo relacionado com as TIC. No caso de incidentes recorrentes de caráter severo relacionados com as TIC, a data e hora em que ocorreu o último incidente de caráter severo relacionado com as TIC.	Não	Sim	Sim	Norma ISO 8601 UTC (AAAA-MM-DD hh:mm:ss)
3.3. Data e hora da recuperação dos serviços, das atividades ou das operações	Informações sobre a data e hora da recuperação dos serviços, atividades ou operações afetados pelo incidente de caráter severo relacionado com as TIC.	Não	Sim, se o campo de dados 3.16 «Tempo de indisponibilidade do serviço» tiver sido preenchido	Sim, se o campo de dados 3.16 «Tempo de indisponibilidade do serviço» tiver sido preenchido	Norma ISO 8601 UTC (AAAA-MM-DD hh:mm:ss)
3.4. Número de clientes afetados	Número de clientes afetados pelo incidente de caráter severo relacionado com as TIC que utilizam o serviço prestado pela entidade financeira. Na sua avaliação do número de clientes afetados, as entidades financeiras devem ter em conta o artigo 1.º, n.º 1, e o artigo 9.º, n.º 1, alínea b), do Regulamento Delegado (UE) 2024/1772. Uma entidade financeira que não possa determinar o número real de clientes afetados deve utilizar estimativas baseadas em dados disponíveis de períodos de referência comparáveis. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, o número total de clientes afetados em todas as entidades financeiras.	Não	Sim	Sim	Número inteiro

	Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
3.5.	Percentagem de clientes afetados	Percentagem de clientes afetados pelo incidente de caráter severo relacionado com as TIC em relação ao número total de clientes que utilizam o serviço afetado prestado pela entidade financeira. No caso de mais do que um serviço afetado, os serviços devem ser comunicados de forma agregada. Na sua avaliação, as entidades financeiras devem ter em conta o artigo 1.º, n.º 1, e o artigo 9.º, n.º 1, alínea a), do Regulamento Delegado (UE) 2024/1772. Uma entidade financeira que não possa determinar a percentagem real de clientes afetados deve utilizar estimativas baseadas em dados disponíveis de períodos de referência comparáveis. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, uma entidade financeira deve dividir a soma de todos os clientes afetados pelo número total de clientes de todas as entidades financeiras afetadas.	Não	Sim	Sim	Expresso em percentagem – qualquer valor até cinco carateres numéricos, incluindo até uma casa decimal, expresso em percentagem (por exemplo, 2,4 em vez de 2,4 %). Se o valor tiver mais de uma casa decimal, as contrapartes que comunicam as informações devem arredondar para cima
3.6.	Número de contrapartes financeiras afetadas	Número de contrapartes financeiras afetadas pelo incidente de caráter severo relacionado com as TIC que celebraram um contrato com a entidade financeira. Na sua avaliação do número de contrapartes financeiras afetadas, as entidades financeiras devem ter em conta o artigo 1.º, n.º 2, do Regulamento Delegado (UE) 2024/1772. Uma entidade financeira que não possa determinar o número real de contrapartes financeiras afetadas deve utilizar estimativas baseadas em dados disponíveis de períodos de referência comparáveis. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, o número total de contrapartes financeiras afetadas em todas as entidades financeiras.	Não	Sim	Sim	Número inteiro

	Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
3.7.	Percentagem de contrapartes financeiras afetadas	Percentagem de contrapartes financeiras afetadas pelo incidente de caráter severo relacionado com as TIC em relação ao número total de contrapartes financeiras que celebraram um contrato com a entidade financeira. Na sua avaliação da percentagem de contrapartes financeiras afetadas, as entidades financeiras devem ter em conta o artigo 1.º, n.º 1, e o artigo 9.º, n.º 1, alínea c), do Regulamento Delegado (UE) 2024/1772. Uma entidade financeira que não possa determinar a percentagem real de contrapartes financeiras afetadas deve utilizar estimativas baseadas em dados disponíveis de períodos de referência comparáveis. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, indicar a soma de todas as contrapartes financeiras afetadas dividida pelo número total de contrapartes financeiras de todas as entidades financeiras afetadas.	Não	Sim	Sim	Expresso em percentagem — qualquer valor até cinco carateres numéricos, incluindo até uma casa decimal, expresso em percentagem (por exemplo, 2,4 em vez de 2,4 %). Se o valor tiver mais de uma casa decimal, as contrapartes que comunicam as informações devem arredondar para cima
3.8.	Impacto nos clientes ou contrapartes financeiras pertinentes	Qualquer impacto identificado nos clientes ou contrapartes financeiras pertinentes a que se refere o artigo 1.º, n.º 3, e o artigo 9.º, n.º 1, alínea f), do Regulamento Delegado (UE) 2024/1772.	Não	Sim, se for atingido o limiar de «Relevância dos clientes e contrapartes financeiras»	Sim, se for atingido o limiar de «Relevância dos clientes e contrapartes financeiras»	Booliano (Sim ou Não)
3.9.	Número de operações afetadas	Número de operações afetadas pelo incidente de caráter severo relacionado com as TIC. Ao avaliarem o impacto nas operações, as entidades financeiras devem ter em conta o artigo 1.º, n.º 4, do Regulamento Delegado (UE) 2024/1772, incluindo o facto de uma parte, pelo menos, de todas as operações nacionais e transfronteiriças afetadas que contêm um montante monetário serem realizadas na União.	Não	Sim, se alguma operação tiver sido afetada pelo incidente	Sim, se alguma operação tiver sido afetada pelo incidente	Número inteiro

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	Uma entidade financeira que não possa determinar o número real de operações afetadas deve utilizar estimativas baseadas em dados disponíveis de períodos de referência comparáveis. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, indicar o número total de operações afetadas em todas as entidades financeiras.				
3.10. Percentagem de operações afetadas	Percentagem de operações afetadas em relação ao número médio diário de operações nacionais e transfronteiras realizadas pela entidade financeira relacionadas com o serviço afetado. As entidades financeiras devem ter em conta o artigo 1.º, n.º 4, e o artigo 9.º, n.º 1, alínea d), do Regulamento Delegado (UE) 2024/1772. Uma entidade financeira que não possa determinar a percentagem real de operações afetadas deve utilizar estimativas. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, uma entidade financeira deve somar o número de todas as operações afetadas e dividir a soma pelo número total de operações de todas as entidades financeiras afetadas.	Não	Sim, se alguma operação tiver sido afetada pelo incidente	Sim, se alguma operação tiver sido afetada pelo incidente	Expresso em percentagem — qualquer valor até cinco carateres numéricos, incluindo até uma casa decimal, expresso em percentagem (por exemplo, 2,4 em vez de 2,4 %). Se o valor tiver mais de uma casa decimal, as contrapartes que comunicam as informações devem arredondar para cima
3.11. Valor das operações afetadas	O valor total das operações afetadas pelo incidente de caráter severo relacionado com as TIC deve ser avaliado em conformidade com o artigo 1.º, n.º 4, e o artigo 9.º, n.º 1, alínea e), do Regulamento Delegado (UE) 2024/1772. Uma entidade financeira que não possa determinar o valor real das operações afetadas deve utilizar estimativas baseadas em dados disponíveis de períodos de referência comparáveis. Uma entidade financeira deve comunicar a quantia monetária como um valor positivo. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, o valor total das operações afetadas em todas as entidades financeiras.	Não	Sim, se algumas operações tiverem sido afetadas pelo incidente	Sim, se alguma operação tiver sido afetada pelo incidente	Monetário As entidades financeiras devem comunicar o ponto de dados em unidades utilizando uma precisão mínima equivalente a milhares de unidades (por exemplo, 2,5 em vez de 2 500 EUR)

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
3.12. Informação sobre se os números são reais ou estimados, ou se houve ou não impacto	Informações sobre se os valores comunicados nos campos de dados 3.4 a 3.11 são reais ou estimados, ou se houve ou não impacto.	Não	Sim	Sim	Escolha (múltipla): — dados reais relativos aos clientes afetados, — dados reais relativos às contrapartes financeiras afetadas, — dados reais relativos às operações afetadas, — estimativas relativas aos clientes afetados, — estimativas relativas às contrapartes financeiras afetadas, — estimativas relativas às operações afetadas, — sem impacto nos clientes, — sem impacto nas contrapartes financeiras, — sem impacto nas operações.
3.13. Impacto em termos de reputação	Informações sobre o impacto em termos de reputação resultante do incidente de caráter severo relacionado com as TIC a que se referem os artigos 2.º e 10.º do Regulamento Delegado (UE) 2024/1772. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, as categorias de impacto em termos de reputação aplicáveis a pelo menos uma entidade financeira.	Não	Sim, se for cumprido o critério «Impacto em termos de reputação»	Sim, se for cumprido o critério «Impacto em termos de reputação»	Escolha (múltipla): — o incidente de caráter severo relacionado com as TIC foi referido nos meios de comunicação social, — o incidente de caráter severo relacionado com as TIC 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, — a entidade financeira não será capaz, ou é provável que não seja capaz, de cumprir obrigações regulamentares em resultado do incidente de caráter severo relacionado com as TIC, — a entidade financeira perderá, ou é provável que perca, clientes ou contrapartes financeiras com um impacto significativo na sua atividade em resultado do incidente de caráter severo relacionado com as TIC.
3.14. Informações contextuais sobre o impacto em termos de reputação	Informações que descrevam a forma como o incidente de caráter severo relacionado com as TIC afetou ou pode afetar a reputação da entidade financeira, incluindo infrações à legislação, requisitos regulamentares não cumpridos, número de reclamações de clientes e outras.	Não	Sim, se for cumprido o critério «Impacto em termos de reputação»	Sim, se for cumprido o critério «Impacto em termos de reputação»	Alfanumérico

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	As informações contextuais devem incluir o tipo de meios de comunicação social (por exemplo, meios de comunicação tradicionais e digitais, blogues, plataformas de transmissão em contínuo) e a cobertura mediática, incluindo o alcance dos meios de comunicação social (local, nacional, internacional). A cobertura mediática neste contexto não significa alguns comentários negativos dos seguidores ou dos utilizadores das redes sociais. A entidade financeira deve também indicar se a cobertura mediática destacou riscos significativos para os seus clientes em relação ao incidente de caráter severo relacionado com as TIC, incluindo o risco de insolvência da entidade financeira ou o risco de perda de fundos. As entidades financeiras devem também indicar se forneceram aos meios de comunicação social informações que tenham servido para informar de forma fiável o público sobre o incidente de caráter severo relacionado com as TIC e as suas consequências. As entidades financeiras podem também indicar se houve informações falsas nos meios de comunicação social em relação ao incidente relacionado com as TIC, incluindo informações baseadas em desinformação deliberada propagada por autores de ameaças, ou informações relacionadas com ou que ilustrem uma desfiguração do sítio Web da entidade financeira.				
3.15. Duração do incidente	As entidades financeiras devem medir a duração do incidente de caráter severo relacionado com as TIC desde o momento em que esse incidente ocorreu até ao momento em que foi resolvido. As entidades financeiras que não possam determinar o momento em que ocorreu o incidente de caráter severo relacionado com as TIC devem medir a duração do mesmo a partir do primeiro que ocorrer, entre o momento em que a entidade financeira detetou o incidente e o momento em que a entidade financeira registou o incidente na rede ou no sistema ou noutras fontes de dados. As entidades financeiras que ainda não conhecem o momento em que o incidente de caráter severo relacionado com as TIC será resolvido devem aplicar estimativas. O valor é expresso em dias, horas e minutos. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, as entidades financeiras devem medir a duração mais longa do incidente de caráter severo relacionado com as TIC, se existirem diferenças entre entidades financeiras.	Não	Sim	Sim	DD:HH:MM

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
3.16. Tempo de indisponibilidade do serviço	O tempo de indisponibilidade do serviço, medido a partir do momento em que o serviço fica total ou parcialmente indisponível para clientes, contrapartes financeiras ou outros utilizadores internos ou externos até ao momento em que as atividades ou operações regulares foram restabelecidas ao nível de serviço prestado antes do incidente de caráter severo relacionado com as TIC. Se o tempo de indisponibilidade do serviço causar um atraso na prestação do serviço após o restabelecimento das atividades ou operações regulares, as entidades financeiras devem medir o tempo de indisponibilidade desde o início do incidente de caráter severo relacionado com as TIC até ao momento em que a prestação do serviço em atraso for retomada. As entidades financeiras que não consigam determinar o momento em que teve início o tempo de indisponibilidade do serviço devem medir o tempo de indisponibilidade do serviço a partir do primeiro que ocorrer, entre o momento em que o incidente foi detetado e o momento em que foi registado. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, as entidades financeiras devem medir a maior duração do tempo de indisponibilidade do serviço, se existirem diferenças entre entidades financeiras.	Não	Sim, se o incidente tiver causado uma indisponibilidade do serviço	Sim, se o incidente tiver causado uma indisponibilidade do serviço	DD:HH:MM
3.17. Informações sobre se os números relativos à duração e ao tempo de indisponibilidade do serviço são reais ou estimados.	Informações sobre se os valores comunicados nos campos de dados 3.15 e 3.16 são reais ou estimados.	Não	Sim, se for cumprido o critério «Duração e tempo de indisponibilidade do serviço»	Sim, se for cumprido o critério «Duração e tempo de indisponibilidade do serviço»	Escolha: — dados reais, — estimativas, — dados reais e estimativas, — sem informação disponível.
3.18. Tipos de impacto nos Estados-Membros	Tipo de impacto nos respetivos Estados-Membros do EEE. Indicar se o incidente de caráter severo relacionado com as TIC teve impacto noutros Estados-Membros do EEE (que não o Estado-Membro da autoridade competente à qual o incidente é diretamente comunicado), em conformidade com o artigo 4.º do Regulamento Delegado (UE) 2024/1772 e, em especial, no que respeita à importância do impacto em relação a: a) Clientes e contrapartes financeiras afetados noutros Estados-Membros; ou	Não	Sim, se for atingido o limiar de «Distribuição geográfica»	Sim, se for atingido o limiar de «Distribuição geográfica»	Escolha (múltipla): — clientes, — contrapartes financeiras, — sucursal da entidade financeira, — entidades financeiras pertencentes ao grupo que exerçam atividades nos respetivos Estados-Membros, — infraestruturas do mercado financeiro, — terceiros prestadores de serviços que podem ser comuns a outras entidades financeiras.

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	b) Sucursais ou outras entidades financeiras pertencentes ao grupo que exerçam atividades noutros Estados-Membros; ou c) Infraestruturas do mercado financeiro ou terceiros prestadores de serviços, que possam afetar as entidades financeiras de outros Estados-Membros aos quais prestam serviços.				
3.19. Descrição da forma como o incidente tem impacto noutros Estados-Membros	Descrição do impacto e da gravidade do incidente de caráter severo relacionado com as TIC em cada Estado-Membro afetado, incluindo uma avaliação do impacto e da gravidade em relação a: a) clientes, b) contrapartes financeiras, c) sucursais da entidade financeira, d) outras entidades financeiras pertencentes ao grupo que exerçam atividades nos respetivos Estados-Membros; e) infraestruturas dos mercados financeiros; f) terceiros prestadores de serviços que possam ser comuns a outras entidades financeiras, conforme aplicável noutro(s) Estado(s) -Membro(s).	Não	Sim, se for atingido o limiar de «Distribuição geográfica»	Sim, se for atingido o limiar de «Distribuição geográfica»	Alfanumérico
3.20. Limiares de materialidade para o critério de classificação «Perdas de dados»	Tipo de perdas de dados decorrentes do incidente de caráter severo relacionado com as TIC, no que respeita à disponibilidade, autenticidade, integridade e confidencialidade dos dados. Na sua avaliação, as entidades financeiras devem ter em conta os artigos 5.º e 13.º do Regulamento Delegado (UE) 2024/1772. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, as perdas de dados que afetem pelo menos uma entidade financeira.	Não	Sim, se for cumprido o critério «Perdas de dados»	Sim, se for cumprido o critério «Perdas de dados»	Escolha (múltipla): — disponibilidade, — autenticidade, — integridade, — confidencialidade.
3.21. Descrição das perdas de dados	Descrição do impacto do incidente de caráter severo relacionado com as TIC na disponibilidade, autenticidade, integridade e confidencialidade dos dados críticos, em conformidade com os artigos 5.º e 13.º do Regulamento Delegado (UE) 2024/1772. Informações sobre o impacto na execução dos objetivos empresariais da entidade financeira ou no cumprimento dos requisitos regulamentares. No âmbito das informações fornecidas, as entidades financeiras devem indicar se os dados afetados são dados de clientes, dados de outras entidades (por exemplo, contrapartes financeiras) ou dados da própria entidade financeira.	Não	Sim, se for cumprido o critério «Perdas de dados»	Sim, se for cumprido o critério «Perdas de dados»	Alfanumérico

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	A entidade financeira pode também indicar o tipo de dados envolvidos no incidente — em especial, se os dados são confidenciais e qual o tipo de confidencialidade envolvida (por exemplo, sigilo comercial/empresarial, dados pessoais, sigilo profissional: sigilo bancário, segredo de seguros, sigilo dos serviços de pagamento, etc.). As informações podem também incluir possíveis riscos associados às perdas de dados, nomeadamente, se os dados afetados pelo incidente podem ser utilizados para identificar pessoas e poderiam ser utilizados pelo autor da ameaça para obter crédito ou empréstimos sem o seu consentimento, para realizar ataques de mistificação da interface (*phishing*) e para divulgar informações publicamente. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, uma descrição geral do impacto do incidente nas entidades financeiras afetadas. Caso existam diferenças no impacto, a descrição do impacto deve indicar claramente o impacto específico nas diferentes entidades financeiras.				
3.22. Critério de classificação «Serviços críticos afetados»	Informações relacionadas com o critério «Serviços críticos afetados». Na sua avaliação, as entidades financeiras devem ter em conta o artigo 6.º do Regulamento Delegado (UE) 2024/1772, incluindo informações sobre: — os serviços ou atividades afetados que exigem autorização ou registo, ou que são supervisionados pelas autoridades competentes, ou — os serviços de TIC ou as redes e os sistemas de informação que apoiam funções críticas ou importantes da entidade financeira, e — a natureza do acesso malicioso e não autorizado à rede e aos sistemas de informação da entidade financeira. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, o impacto nos serviços críticos aplicável a pelo menos uma entidade financeira.	Não	Sim	Sim	Alfanumérico

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
3.23. Tipo do incidente	Classificação dos incidentes por tipo.	Não	Sim	Sim	Escolha (múltipla): — relacionado com a cibersegurança, — falha do processo, — avaria do sistema, — acontecimento externo, — relacionado com pagamentos, — outro (especifique).
3.24. Outros tipos de incidentes	Outros tipos de incidentes relacionados com as TIC: as entidades financeiras que selecionaram «outro» tipo de incidentes no campo de dados 3.23 devem especificar o tipo de incidente relacionado com as TIC.	Não	Sim, se for selecionado «outro» tipo de incidentes no campo de dados 3.23	Sim, se for selecionado «outro» tipo de incidentes no campo de dados 3.23	Alfanumérico
3.25. Ameaças e técnicas utilizadas pelo autor da ameaça	Indicar as ameaças e técnicas utilizadas pelo autor da ameaça, incluindo: a) Engenharia social, incluindo mistificação da interface (*phishing*); b) Negação de serviço; c) Usurpação de identidade; d) Encriptação de dados para impacto, incluindo *software* de sequestro; e) Desvio de recursos; f) Exfiltração e manipulação de dados, excluindo usurpação de identidade; g) Destruição de dados; h) Desfiguração; i) Ataque à cadeia de abastecimento; j) Outra (especifique).	Não	Sim, se o tipo de incidente relacionado com as TIC for «relacionado com a cibersegurança» no campo 3.23	Sim, se o tipo de incidente relacionado com as TIC for «relacionado com a cibersegurança» no campo 3.23	Escolha (múltipla): — engenharia social [incluindo mistificação da interface (*phishing*)], — negação de serviço, — usurpação de identidade, — encriptação de dados para impacto, incluindo *software* de sequestro, — desvio de recursos, — exfiltração e manipulação de dados, incluindo usurpação de identidade, — destruição de dados, — desfiguração, — ataque à cadeia de abastecimento, — outro (especifique).
3.26. Outros tipos de técnicas	Outros tipos de técnicas As entidades financeiras que selecionaram «outro» tipo de técnicas no campo de dados 3.25 devem especificar o tipo de técnica.	Não	Sim, se for selecionado «outro» tipo de técnicas no campo de dados 3.25	Sim, se for selecionado «outro» tipo de técnicas no campo de dados 3.25	Alfanumérico

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
3.27. Informações sobre as áreas funcionais e os processos operacionais afetados	Indicação das áreas funcionais e dos processos operacionais afetados pelo incidente, incluindo produtos e serviços. As áreas funcionais devem incluir, entre outros: a) Comercialização e desenvolvimento empresarial; b) Serviço ao cliente; c) Gestão dos produtos; d) Cumprimento dos requisitos regulamentares; e) Gestão dos riscos; f) Finanças e contabilidade; g) Recursos humanos e serviços gerais; h) Tecnologias da informação. Os processos operacionais devem incluir, entre outros: — informação sobre contas, — serviços atuariais, — aquisição de operações de pagamento, — autenticação/autorização, — autoridade, — integração de autoridades/clientes, — administração de prestações, — gestão do pagamento de prestações, — políticas de compra e venda de pacotes de seguros entre seguradoras, — pagamentos com cartão, — gestão de tesouraria, — depósito ou levantamento de numerário, — gestão de sinistros; — seguro de processamento de sinistros, — compensação, — conglomerados de empréstimos a empresas, — seguros coletivos, — transferência de créditos, — custódia e guarda de ativos, — integração de clientes, — integração de dados, — processamento de dados, — débitos diretos, — seguros de exportação, — finalização de operações, — colocação de instrumentos financeiros, — contabilidade do fundo,	Não	Sim	Sim	Alfanumérico

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	— moeda estrangeira, — consultoria em matéria de investimento, — gestão de investimentos, — emissão de instrumentos de pagamento, — gestão de empréstimos, — processo de pagamento de seguros de vida, — envio de fundos, — cálculo de ativos líquidos, — ordens, — iniciação de pagamentos, — subscrição de apólices, — gestão de carteiras, — cobrança de prémios, — receção/transmissão/execução, — resseguro, — liquidação, — controlo de operações. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, as áreas funcionais e processos operacionais afetados em pelo menos uma entidade financeira.				
3.28. Componentes afetados da infraestrutura de apoio aos processos operacionais	Informações sobre se os componentes da infraestrutura (servidores, sistemas operativos, *software*, servidores de aplicações, *software* intermédio, componentes de rede, outros) que apoiam os processos operacionais foram afetados pelo incidente de caráter severo relacionado com as TIC.	Não	Sim	Sim	Escolha: — Sim, — Não, — informação não disponível.
3.29. Informações sobre os componentes afetados da infraestrutura de apoio aos processos operacionais	Descrição do impacto do incidente de caráter severo relacionado com as TIC nos componentes da infraestrutura que apoiam os processos operacionais, incluindo *hardware* e *software*. O *hardware* inclui servidores, computadores, centros de dados, comutadores, encaminhadores, plataformas. O *software* inclui sistemas operativos, aplicações, bases de dados, ferramentas de segurança, componentes de rede e outros, a especificar. As descrições devem descrever ou designar os componentes ou sistemas da infraestrutura afetados e, se disponível: a) Informações sobre a versão; b) Infraestrutura interna/parcialmente subcontratada/totalmente subcontratada – nome do terceiro prestador;	Não	Sim, se o incidente tiver afetado componentes da infraestrutura que apoiam processos operacionais	Sim, se o incidente tiver afetado componentes da infraestrutura que apoiam processos operacionais	Alfanumérico

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	c) Se a infraestrutura é utilizada ou partilhada para múltiplas funções operacionais; d) Disposições pertinentes em matéria de resiliência/continuidade/recuperação/possibilidade de substituição em vigor.				
3.30. Impacto nos interesses financeiros dos clientes	Informações sobre se o incidente de caráter severo relacionado com as TIC afetou os interesses financeiros dos clientes.	Não	Sim	Sim	Escolha: — Sim, — Não, — informação não disponível.
3.31. Comunicação a outras autoridades	Especificação das autoridades que foram informadas sobre o incidente de caráter severo relacionado com as TIC. Tendo em conta as diferenças resultantes da legislação nacional dos Estados-Membros, o conceito de autoridades responsáveis pela aplicação da lei deve ser entendido pelas entidades financeiras de modo a incluir as autoridades públicas habilitadas a instaurar ações penais contra a cibercriminalidade, incluindo a polícia, os serviços responsáveis pela aplicação da lei e os magistrados do Ministério Público.	Não	Sim	Sim	Escolha (múltipla): — polícia/serviços de aplicação da lei, — CSIRT, — Autoridade de Proteção de Dados, — Agência Nacional de Cibersegurança, — Nenhuma, — Outras (especifique).
3.32. Especificação de «outras» autoridades	Especificação dos «outros» tipos de autoridades informadas sobre o incidente de caráter severo relacionado com as TIC. Se selecionado no campo de dados 3.31 «Outras», a descrição deve incluir informações mais pormenorizadas sobre a autoridade à qual a entidade financeira apresentou informações sobre o incidente de caráter severo relacionado com as TIC.	Não	Sim, se «outro» tipo de autoridades tiver sido informado pela entidade financeira sobre o incidente de caráter severo relacionado com as TIC	Sim, se «outro» tipo de autoridades tiver sido informado pela entidade financeira sobre o incidente de caráter severo relacionado com as TIC	Alfanumérico
3.33. Ações/medidas temporárias tomadas ou previstas para recuperar do incidente	Indicação sobre se a entidade financeira aplicou (ou tenciona aplicar) quaisquer medidas temporárias que foram tomadas (ou estão previstas) para recuperar do incidente de caráter severo relacionado com as TIC.	Não	Sim	Sim	Booliano (Sim ou Não)

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
3.34. Descrição de quaisquer ações e medidas temporárias tomadas ou previstas para recuperar do incidente	As informações devem descrever as medidas imediatas tomadas, incluindo o isolamento do incidente a nível da rede, os procedimentos operacionais ativados, as portas USB bloqueadas, o local de recuperação de catástrofes ativado e quaisquer outros controlos de segurança adicionais temporariamente aplicados. As entidades financeiras devem indicar a data e a hora da aplicação das medidas temporárias e a data prevista de regresso ao local principal. No que respeita a quaisquer medidas temporárias que não foram aplicadas, mas que ainda estejam planeadas, indicação da data prevista para a sua aplicação. Se não tiverem sido tomadas quaisquer ações/medidas temporárias, indicar o motivo.	Não	Sim, se tiverem sido tomadas ou estiverem previstas ações/ medidas temporárias (campo de dados 3.33)	Sim, se tiverem sido tomadas ou estiverem previstas ações/ medidas temporárias (campo de dados 3.33)	Alfanumérico
3.35. Indicadores de exposição a riscos	Informações relacionadas com o incidente de caráter severo relacionado com as TIC que possam ajudar a identificar atividades maliciosas numa rede ou num sistema de informação (indicadores de exposição a riscos), se for caso disso. O campo aplica-se apenas às entidades financeiras abrangidas pelo âmbito de aplicação da Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho ([1]) e às entidades financeiras identificadas como entidades essenciais ou importantes nos termos das regras nacionais de transposição do artigo 3.º da Diretiva (UE) 2022/2555, se for caso disso. Os indicadores de exposição a riscos fornecidos pela entidade financeira devem incluir as seguintes categorias de dados: a) Endereços IP; b) Endereços URL; c) Domínios; d) Dispersão dos ficheiros; e) Dados sobre o *software* malicioso (nome do *software* malicioso, nomes de ficheiros e respetiva localização, chaves de registo específicas associadas a atividades de *software* malicioso); f) Dados relativos à atividade da rede (portas, protocolos, endereços, encaminhadores, agentes de utilizador, cabeçalhos, registos específicos ou padrões distintivos no tráfego de rede); g) Dados de mensagens de correio eletrónico (remetente, destinatário, assunto, cabeçalho, conteúdo);	Não	Sim, se no campo de dados 3.23 tiver sido selecionado o tipo de incidente relacionado com a cibersegurança	Sim, se no campo de dados 3.23 tiver sido selecionado o tipo de incidente relacionado com a cibersegurança	Alfanumérico

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	h) Pedidos de DNS e configurações do registo; i) Atividades da conta de utilizador (início de sessão, atividade de conta de utilizador privilegiada, aumento de privilégios); j) Tráfego na base de dados (ler/escrever), pedidos para o mesmo ficheiro. Na prática, este tipo de informação pode incluir dados relativos, nomeadamente, a indicadores que descrevem padrões de tráfego de rede correspondentes a ataques conhecidos/comunicações *botnet*, endereços IP de máquinas infetadas com *software* malicioso (*bots*), dados relativos a servidores de «comando e controlo» utilizados por *software* malicioso (geralmente domínios ou endereços IP) e URL relativos a sítios de *phishing* ou sítios Web observados que alojam *software* malicioso ou *kits* de exploração.				
Conteúdo do relatório final					
4.1. Classificação de alto nível das causas profundas do incidente	Classificação de alto nível das causas profundas do incidente de caráter severo relacionado com as TIC no âmbito dos tipos de incidentes, incluindo as seguintes categorias de alto nível: a) Ações maliciosas; b) Falha do processo; c) Avaria/falha do sistema; d) Erro humano; e) Acontecimento externo.	Não	Não	Sim	Escolha (múltipla): — ações maliciosas, — falha do processo, — avaria/falha do sistema, — erro humano, — acontecimento externo.
4.2. Classificação pormenorizada das causas profundas do incidente	Classificação pormenorizada das causas profundas do incidente de caráter severo relacionado com as TIC no âmbito dos tipos de incidentes, incluindo as seguintes categorias pormenorizadas relacionadas com as categorias de alto nível comunicadas no campo de dados 4.1: 1. **Ações maliciosas** (se selecionado, escolher uma ou mais das seguintes opções): a) Ações internas deliberadas; b) Danos físicos deliberados/manipulação/roubo; c) Ações fraudulentas. 2. **Falha do processo** (se selecionado, escolher uma ou mais das seguintes opções): a) Acompanhamento insuficiente ou falha do acompanhamento e controlo;	Não	Não	Sim	Escolha (múltipla): — ações maliciosas: Ações internas deliberadas, — ações maliciosas: danos físicos deliberados/manipulação/roubo, — ações maliciosas: ações fraudulentas, — falha do processo: Acompanhamento insuficiente ou falha do acompanhamento e controlo, — falha do processo: **f**unções e responsabilidades insuficientes/pouco claras, — falha do processo: Falha do processo de gestão dos riscos associados às TIC, — falha do processo: Insuficiência ou falha das operações de TIC e das operações de segurança das TIC,

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	b) Funções e responsabilidades insuficientes/pouco claras; c) Falha do processo de gestão dos riscos associados às TIC; d) Insuficiência ou falha das operações de TIC e das operações de segurança das TIC; e) Insuficiência ou falha da gestão de projetos de TIC; f) Políticas, procedimentos e documentação internos inadequados; g) Aquisição, desenvolvimento ou manutenção de sistemas de TIC inadequados; h) Outra (especifique). 3. **Avaria/falha do sistema** (se selecionado, escolher uma ou mais das seguintes opções): a) Capacidade e desempenho do *hardware*: incidentes de caráter severo relacionados com as TIC causados por recursos de *hardware* que se revelem inadequados em termos de capacidade ou desempenho para cumprir os requisitos legislativos aplicáveis; b) Manutenção do *hardware*: incidentes de caráter severo relacionados com as TIC resultantes de manutenção inadequada ou insuficiente de componentes de *hardware*, com exceção da «obsolescência/envelhecimento do *hardware*»; c) Obsolescência/envelhecimento do *hardware*: este tipo de causa profunda envolve incidentes de caráter severo relacionados com as TIC resultantes de componentes de *hardware* obsoletos ou desatualizados; d) Compatibilidade/configuração do *software*: incidentes de caráter severo relacionados com as TIC causados por componentes de *software* incompatíveis com outro *software* ou com a configuração dos sistemas, incluindo incidentes de caráter severo relacionados com as TIC resultantes de conflitos de *software*, configurações incorretas ou parâmetros mal configurados que afetem a funcionalidade global do sistema; e) Desempenho do *software*: incidentes de caráter severo relacionados com as TIC resultantes de componentes de *software* que apresentem um desempenho insuficiente ou ineficiências, por outros motivos que não os especificados em «Compatibilidade/configuração do *software*», incluindo incidentes de caráter severo relacionados com as TIC causados por tempos de resposta lentos, consumo excessivo de recursos ou execução ineficiente de pesquisas com impacto no desempenho do *software* ou do sistema;				— falha do processo: Insuficiência ou falha da gestão de projetos de TIC, — falha do processo: inadequação das políticas, procedimentos e documentação internos, — falha do processo: aquisição, desenvolvimento e manutenção inadequados dos sistemas de TIC, — falha do processo: outra (especifique), — avaria do sistema: capacidade e desempenho do *hardware*, — avaria do sistema: manutenção do *hardware*, — avaria do sistema: obsolescência/envelhecimento do *hardware*, — avaria do sistema: compatibilidade/configuração do *software*, — avaria do sistema: desempenho do *software*, — avaria do sistema: configuração da rede, — avaria do sistema: danos físicos, — avaria do sistema: outra (especifique), — erro humano: omissão, — erro humano: erro, — erro humano: competências e conhecimento, — erro humano: recursos humanos inadequados, — erro humano: falha de comunicação, — erro humano: outra (especifique), — acontecimento externo: Catástrofes naturais/força maior, — acontecimento externo: Falhas de terceiros, — acontecimento externo: Outra (especifique).

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	f) Configuração da rede: incidentes de caráter severo relacionados com as TIC resultantes de configurações de rede ou infraestruturas incorretas ou mal configuradas, incluindo incidentes de caráter severo relacionados com as TIC causados por erros de configuração da rede, problemas de encaminhamento, configurações incorretas de *firewall* ou outros problemas relacionados com a rede que afetem a conectividade ou a comunicação; g) Danos físicos: incidentes de caráter severo relacionados com as TIC causados por danos físicos na infraestrutura de TIC que conduzem a falhas do sistema; h) Outra (especifique). 4. **Erro humano** (se selecionado, escolher uma ou mais das seguintes opções): a) Omissão (não intencional); b) Erro; c) Competências e conhecimento: incidentes de caráter severo relacionados com as TIC resultantes da falta de conhecimentos especializados ou de proficiência na utilização de sistemas ou processos de TIC, que podem ser causados por formação inadequada, conhecimentos insuficientes ou lacunas de competências necessárias para executar tarefas específicas ou dar resposta a desafios técnicos; d) Recursos humanos inadequados: incidentes de caráter severo relacionados com as TIC causados pela falta de recursos necessários, incluindo *hardware*, *software*, infraestruturas ou pessoal, e incluindo situações em que a insuficiência de recursos conduza a ineficiências operacionais, falhas do sistema ou incapacidade de satisfazer os requisitos das empresas; e) Falha de comunicação; f) Outra (especifique). 5. **Acontecimento externo** (se selecionado, escolher uma ou mais das seguintes opções): a) Catástrofes naturais/força maior; b) Falhas de terceiros;				

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	c) Outra (especifique). As entidades financeiras devem ter em conta que, no caso de incidentes recorrentes de caráter severo relacionados com as TIC, é tida em conta a causa profunda específica aparente do incidente e não as categorias gerais incluídas neste campo.				
4.3. Classificação adicional das causas profundas do incidente	Classificação adicional das causas profundas do incidente de caráter severo relacionado com as TIC no âmbito do tipo de incidente, incluindo as seguintes categorias de classificação adicionais relacionadas com as categorias pormenorizadas que devem ser comunicadas no campo de dados 4.2. O campo é obrigatório para o relatório final, se no campo de dados 4.2 forem comunicadas categorias específicas que exigem maior granularidade. Ponto 2, alínea a), **Acompanhamento insuficiente ou falha do acompanhamento e controlo:** a) Acompanhamento da adesão às políticas; b) Acompanhamento de terceiros prestadores de serviços; c) Acompanhamento e verificação da correção das vulnerabilidades; d) Gestão da identidade e do acesso; e) Encriptação e criptografia; f) Registo de dados. Ponto 2, alínea c), **Falha do processo de gestão dos riscos associados às TIC:** a) Falha na especificação de níveis exatos de tolerância ao risco; b) Avaliações insuficientes da vulnerabilidade e das ameaças; c) Medidas inadequadas de tratamento dos riscos; d) Má gestão dos riscos residuais associados às TIC. Ponto 2, alínea d), **Insuficiência ou falha das operações de TIC e das operações de segurança das TIC:** a) Gestão das vulnerabilidades e correções informáticas; b) Gestão das alterações; c) Gestão da capacidade e do desempenho; d) Gestão de ativos de TIC e classificação da informação;	Não	Não	Sim	Escolha (múltipla): — acompanhamento da adesão às políticas, — acompanhamento de terceiros prestadores de serviços, — acompanhamento e verificação da correção das vulnerabilidades, — gestão da identidade e do acesso, — encriptação e criptografia, — registo de dados, — falha na especificação de níveis exatos de tolerância ao risco, — avaliações insuficientes da vulnerabilidade e das ameaças, — medidas inadequadas de tratamento dos riscos, — má gestão dos riscos residuais associados às TIC, — gestão das vulnerabilidades e correções informáticas, — gestão das alterações, — gestão da capacidade e do desempenho, — gestão de ativos de TIC e classificação da informação, — salvaguarda e restauro, — tratamento de erros, — aquisição, desenvolvimento e manutenção inadequados dos sistemas de TIC, — insuficiências ou falhas nos testes de *software*.

Campo de dados		Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
		e) Salvaguarda e restauro; f) Tratamento de erros. Ponto 2, alínea g), **Aquisição, desenvolvimento e manutenção inadequados dos sistemas de TIC:** a) Aquisição, desenvolvimento e manutenção inadequados dos sistemas de TIC; b) Insuficiências ou falhas nos ensaios de *software*.				
4.4.	Outros tipos de causas profundas	As entidades financeiras que selecionaram «outro» tipo de causa profunda no campo de dados 4.2 devem especificar outros tipos de causas profundas.	Não	Não	Sim, se for selecionado «outro» tipo de causas profundas no campo de dados 4.2	Alfanumérico
4.5.	Informações sobre as causas profundas do incidente	Descrição da sequência dos acontecimentos que conduziram ao incidente de caráter severo relacionado com as TIC e descrição da forma como o incidente tem uma causa profunda aparente semelhante, caso esse incidente seja classificado como incidente recorrente, incluindo uma descrição concisa de todas as razões subjacentes e dos principais fatores que contribuíram para a ocorrência do incidente de caráter severo relacionado com as TIC. Em caso de ações maliciosas, descrição do *modus operandi* da ação maliciosa, incluindo as táticas, técnicas e procedimentos utilizados, bem como o vetor de entrada do incidente de caráter severo relacionado com as TIC, incluindo uma descrição das investigações e análises que conduziram à identificação das causas profundas, se aplicável.	Não	Não	Sim	Alfanumérico
4.6.	Resolução do incidente	Informações adicionais sobre as ações/medidas tomadas/previstas para resolver permanentemente o incidente de caráter severo relacionado com as TIC e para evitar que esse incidente volte a ocorrer. Ensinamentos retirados do incidente de caráter severo relacionado com as TIC.	Não	Não	Sim	Alfanumérico

Campo de dados		Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
		A descrição deve incluir os seguintes pontos: 1. **Descrição das medidas de resolução** a) Medidas tomadas para resolver permanentemente o incidente de caráter severo relacionado com as TIC (excluindo quaisquer medidas temporárias); b) Para cada medida tomada, indicar o potencial envolvimento de um terceiro prestador de serviços e da entidade financeira; c) Indicar se os procedimentos foram adaptados na sequência do incidente de caráter severo relacionado com as TIC; d) Indicar quaisquer controlos adicionais que tenham sido aplicados ou que estejam previstos, com o respetivo calendário de aplicação. Potenciais problemas identificados no que respeita à solidez dos sistemas informáticos afetados ou em termos dos procedimentos ou controlos em vigor, se aplicável. As entidades financeiras devem indicar claramente de que forma as medidas corretivas previstas abordarão as causas profundas identificadas e quando se prevê que o incidente de caráter severo relacionado com as TIC seja resolvido de forma permanente. 2. **Ensinamentos retirados** As entidades financeiras devem descrever as conclusões da análise pós-incidente.				
4.7.	Data e hora em que foi abordada a causa profunda do incidente	Data e hora em que foi abordada a causa profunda do incidente.	Não	Não	Sim	Norma ISO 8601 UTC (AAAA-MM-DD hh:mm:ss)
4.8.	Data e hora em que o incidente foi resolvido	Data e hora em que o incidente foi resolvido.	Não	Não	Sim	Norma ISO 8601 UTC (AAAA-MM-DD hh:mm:ss)

	Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
4.9.	Informação sobre se a data de resolução permanente dos incidentes difere da data de execução inicialmente prevista	Descrições das razões pelas quais a data de resolução permanente dos incidentes de caráter severo relacionados com as TIC é diferente da data de execução inicialmente prevista, quando aplicável.	Não	Não	Sim	Alfanumérico
4.10.	Avaliação do risco para as funções críticas para efeitos de resolução	Avaliação para determinar se o incidente de caráter severo relacionado com as TIC representa um risco para funções críticas na aceção do artigo 2.º, n.º 1, ponto 35, da Diretiva 2014/59/UE do Parlamento Europeu e do Conselho ([2]). As entidades a que se refere o artigo 1.º, n.º 1, da Diretiva 2014/59/UE devem indicar se o incidente representa um risco para as funções críticas na aceção do artigo 2.º, n.º 1, ponto 35, da Diretiva 2014/59/UE, comunicado no modelo Z07.01 do Regulamento de Execução (UE) 2018/1624 da Comissão ([3]) e afetado à entidade específica no modelo Z07.02.	Não	Não	Sim, se o incidente representar um risco para as funções críticas das entidades financeiras nos termos do artigo 2.º, n.º 1, ponto 35, da Diretiva 2014/59/UE	Alfanumérico
4.11.	Informações pertinentes para as autoridades de resolução	Descrição sobre se o incidente de caráter severo relacionado com as TIC afetou a resolubilidade da entidade ou do grupo e, em caso afirmativo, de que forma. As entidades a que se refere o artigo 1.º, n.º 1, da Diretiva 2014/59/UE devem fornecer informações sobre se o incidente de caráter severo relacionado com as TIC afetou a resolubilidade da entidade ou do grupo e, em caso afirmativo, de que forma. Essas entidades devem também indicar se o incidente de caráter severo relacionado com as TIC afeta a solvência ou a liquidez da entidade financeira e a potencial quantificação do impacto. Essas entidades devem também fornecer informações sobre o impacto na continuidade operacional, o impacto na resolubilidade da entidade, qualquer impacto adicional nos custos e perdas decorrentes do incidente de caráter severo relacionado com as TIC, incluindo na posição de capital da entidade financeira, e se os acordos contratuais sobre a utilização de serviços de TIC continuam a ser sólidos e plenamente aplicáveis em caso de resolução da entidade.	Não	Não	Sim, se o incidente tiver afetado a resolubilidade da entidade ou do grupo	Alfanumérico

	Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
4.12.	Limiar de materialidade para o critério de classificação «Impacto económico»	Informações pormenorizadas sobre os limiares eventualmente atingidos pelo incidente de caráter severo relacionado com as TIC em relação ao critério «Impacto económico» referido nos artigos 7.º e 14.º do Regulamento Delegado (UE) 2024/1772.	Não	Não	Sim	Alfanumérico
4.13.	Montante dos custos e perdas brutos diretos e indiretos	Montante total dos custos e perdas brutos diretos e indiretos incorridos pela entidade financeira decorrentes do incidente de caráter severo relacionado com as TIC, incluindo: a) O montante dos fundos ou ativos financeiros expropriados pelos quais a entidade financeira é responsável; b) O montante dos custos de substituição ou relocalização de *software*, *hardware* ou infraestrutura; c) O montante dos custos de pessoal, incluindo os custos associados à substituição ou relocalização de pessoal, à contratação de pessoal adicional, à remuneração das horas extraordinárias e à recuperação de competências perdidas ou diminuídas do pessoal; d) O montante das taxas por incumprimento de obrigações contratuais; e) O montante dos custos de reparação e indemnização dos clientes; f) O montante das perdas devidas à perda de receitas; g) O montante dos custos associados à comunicação interna e externa; h) O montante dos custos de consultoria, incluindo custos associados a aconselhamento jurídico, a serviços forenses e a serviços de correção; i) O montante de outros custos e perdas, incluindo: i) encargos diretos, incluindo imparidades e custos de liquidação, registados na conta de resultados e depreciações devidas ao incidente de caráter severo relacionado com as TIC, ii) provisões ou reservas contabilizadas na conta de resultados contra perdas prováveis relacionadas com o incidente de caráter severo relacionado com as TIC,	Não	Não	Sim	Monetário

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	iii) perdas pendentes, sob a forma de perdas decorrentes do incidente de caráter severo relacionado com as TIC, que se encontram temporariamente registadas em contas transitórias ou provisórias e não estão ainda refletidas nos resultados, que se prevê venham a ser incluídas num prazo compatível com a dimensão e a duração do elemento pendente, iv) receitas não cobradas significativas, relativas a obrigações contratuais perante terceiros, incluindo a decisão de compensar um cliente na sequência do incidente de caráter severo relacionado com as TIC, não através de um reembolso ou pagamento direto, mas sim através de um ajustamento das receitas, dispensando ou reduzindo taxas contratuais durante um determinado período futuro, v) perdas temporárias, quando abrangem mais do que um exercício financeiro e dão origem a riscos jurídicos. Na sua avaliação, as entidades financeiras devem ter em conta o artigo 7.º, n.ºs 1 e 2, do Regulamento Delegado (UE) 2024/1772. As entidades financeiras não devem incluir neste valor qualquer tipo de recuperações financeiras. As entidades financeiras devem comunicar a quantia monetária como um valor positivo. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, as entidades financeiras devem ter em conta o montante total dos custos e perdas em todas as entidades financeiras. As entidades financeiras devem comunicar o ponto de dados em unidades utilizando uma precisão mínima equivalente a milhares de unidades.				
4.14. Montante das recuperações financeiras	Montante total das recuperações financeiras. As recuperações financeiras devem estar relacionadas com a perda inicial causada pelo incidente, independentemente do momento em que são recebidos os fundos ou entradas de benefícios económicos.	Não	Não	Sim	Monetário As entidades financeiras devem comunicar o ponto de dados em unidades utilizando uma precisão mínima equivalente a milhares de unidades

Campo de dados	Descrição	Obrigatório para a notificação inicial	Obrigatório para o relatório intercalar	Obrigatório para o relatório final	Tipo de campo
	As entidades financeiras devem comunicar a quantia monetária como um valor positivo. Em caso de comunicação agregada a que se refere o artigo 7.º do presente regulamento, as entidades financeiras devem ter em conta o montante total das recuperações financeiras em todas as entidades financeiras.				
4.15. Informações sobre se os incidentes de caráter não severo são recorrentes	Informações sobre se mais do que um incidente de caráter não severo relacionado com as TIC foram recorrentes e se, em conjunto, são considerados um incidente de caráter severo na aceção do artigo 8.º, n.º 2, do Regulamento Delegado (UE) 2024/1772. As entidades financeiras devem indicar se os incidentes de caráter não severo relacionados com as TIC foram recorrentes e se, em conjunto, são considerados como um incidente de caráter severo relacionado com as TIC. As entidades financeiras devem também indicar o número de ocorrências destes incidentes de caráter não severo relacionados com as TIC.	Não	Não	Sim, se o incidente de caráter severo incluir mais do que um incidente de caráter não severo recorrente	Alfanumérico
4.16. Data e hora de ocorrência de incidentes recorrentes	Quando as entidades financeiras comunicam incidentes recorrentes relacionados com as TIC, a data e hora em que ocorreu o primeiro incidente relacionado com as TIC.	Não	Não	Sim, em caso de incidentes recorrentes	Norma ISO 8601 UTC (AAAA-MM-DD hh:mm:ss)

(1) 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).

(2) Diretiva 2014/59/UE do Parlamento Europeu e do Conselho, de 15 de maio de 2014, que estabelece um enquadramento para a recuperação e a resolução de instituições de crédito e de empresas de investimento e que altera a Diretiva 82/891/CEE do Conselho, e as Diretivas 2001/24/CE, 2002/47/CE, 2004/25/CE, 2005/56/CE, 2007/36/CE, 2011/35/UE, 2012/30/UE e 2013/36/UE e os Regulamentos (UE) n.º 1093/2010 e (UE) n.º 648/2012 do Parlamento Europeu e do Conselho (JO L 173 de 12.6.2014, p. 190, ELI: http://data.europa.eu/eli/dir/2014/59/oj).

(3) Regulamento de Execução (UE) 2018/1624 da Comissão, de 23 de outubro de 2018, que estabelece normas técnicas de execução no que respeita aos procedimentos e aos formulários e modelos normalizados para a apresentação de informações para efeitos dos planos de resolução de instituições de crédito e de empresas de investimento nos termos da Diretiva 2014/59/UE do Parlamento Europeu e do Conselho e revoga o Regulamento de Execução (UE) 2016/1066 da Comissão (JO L 277 de 7.11.2018, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2018/1624/oj).

ANEXO III

MODELOS PARA A NOTIFICAÇÃO DE CIBERAMEAÇAS SIGNIFICATIVAS

Número do campo	Campo de dados	
1	Nome da entidade que apresenta a notificação	
2	Código de identificação da entidade que apresenta a notificação	
3	Tipo de entidade financeira que apresenta a notificação	
4	Nome da entidade financeira	
5	Código LEI da entidade financeira	
6	Nome da pessoa de contacto principal	
7	Endereço de correio eletrónico da pessoa de contacto principal	
8	Telefone da pessoa de contacto principal	
9	Nome da pessoa de contacto secundária	
10	Endereço de correio eletrónico da pessoa de contacto secundária	
11	Telefone da pessoa de contacto secundária	
12	Data e hora de deteção da ciberameaça	
13	Descrição da ciberameaça significativa	
14	Informação sobre o potencial impacto	
15	Critérios de classificação de incidentes potenciais	
16	Estado da ciberameaça	
17	Medidas tomadas para evitar a materialização	
18	Notificação a outras partes interessadas	
19	Indicadores de exposição a riscos	
20	Outras informações pertinentes	

ELI: http://data.europa.eu/eli/reg_impl/2025/302/oj

ANEXO IV

GLOSSÁRIO DE DADOS E INSTRUÇÕES PARA A NOTIFICAÇÃO DE CIBERAMEAÇAS SIGNIFICATIVAS

Campo de dados	Descrição	Campo obrigatório	Tipo de campo
1. Nome da entidade que apresenta a notificação	Denominação legal completa da entidade que apresenta a notificação.	Sim	Alfanumérico
2. Código de identificação da entidade que apresenta a notificação	Código de identificação da entidade que apresenta a notificação. Quando a notificação/o relatório for apresentada/o por uma entidade financeira, o código de identificação deve ser um identificador de entidade jurídica (LEI), que é um código único de 20 carateres alfanuméricos, com base na norma ISO 17442-1:2020. Quando um terceiro prestador de serviços apresenta um relatório em nome de uma entidade financeira pode utilizar um código de identificação conforme especificado nas normas técnicas de execução adotadas nos termos do artigo 28.º, n.º 9, do Regulamento (UE) 2022/2554.	Sim	Alfanumérico
3. Tipo de entidade financeira que apresenta o relatório	Tipo da entidade a que se refere o artigo 2.º, n.º 1, alíneas a) a t), do Regulamento (UE) 2022/2554, que apresenta o relatório.	Sim, se o relatório não for apresentado diretamente pela entidade financeira afetada	Escolha (escolha múltipla): — instituição de crédito, — instituição de pagamento, — instituição de pagamento isenta, — prestador de serviços de informação sobre contas, — instituição de moeda eletrónica, — instituição de moeda eletrónica isenta, — empresa de investimento, — prestador de serviços de criptoativos, — emitente de criptofichas referenciadas a ativos, — central de valores mobiliários, — contraparte central, — plataforma de negociação, — repositório de transações, — gestor de fundos de investimento alternativos, — sociedade gestora, — prestador de serviços de comunicação de dados,

Campo de dados		Descrição	Campo obrigatório	Tipo de campo
				— empresa de seguros e de resseguros, — mediador de seguros, mediador de resseguros e mediador de seguros a título acessório, — instituição de realização de planos de pensões profissionais, — agência de notação de risco, — administrador de índices de referência críticos, — prestador de serviços de financiamento colaborativo, — repositório de titularizações.
4.	Nome da entidade financeira	Denominação legal completa da entidade financeira que notifica a ciberameaça significativa.	Sim, se a entidade financeira for diferente da entidade que apresenta a notificação	Alfanumérico
5.	Código LEI da entidade financeira	Identificador de entidade jurídica (LEI) da entidade financeira que notifica a ciberameaça significativa, atribuído em conformidade com a Organização Internacional de Normalização.	Sim, se a entidade financeira que notifica a ciberameaça significativa for diferente da entidade que apresenta o relatório	Código único de 20 carateres alfanuméricos, com base na norma ISO 17442-1:2020
6.	Nome da pessoa de contacto principal	Nome e apelido da pessoa de contacto principal da entidade financeira.	Sim	Alfanumérico
7.	Endereço de correio eletrónico da pessoa de contacto principal	Endereço eletrónico da pessoa de contacto principal que pode ser utilizado pela autoridade competente para a comunicação de seguimento.	Sim	Alfanumérico
8.	Telefone da pessoa de contacto principal	Número de telefone da pessoa de contacto principal que pode ser utilizado pela autoridade competente para a comunicação de seguimento. O número de telefone deve ser comunicado com todos os prefixos internacionais (por exemplo, +33XXXXXXXXX).	Sim	Alfanumérico
9.	Nome da pessoa de contacto secundária	Nome e apelido da pessoa de contacto secundária da entidade financeira ou de uma entidade que apresenta a notificação em nome da entidade financeira, se for caso disso.	Sim, se o nome e o apelido da pessoa de contacto secundária da entidade financeira ou de uma entidade que apresenta a notificação em nome da entidade financeira estiver disponível	Alfanumérico

Campo de dados	Descrição	Campo obrigatório	Tipo de campo
10. Endereço de correio eletrónico da pessoa de contacto secundária	Endereço de correio eletrónico da pessoa de contacto secundária ou um endereço de correio eletrónico funcional da equipa que pode ser utilizado pela autoridade competente para a comunicação de seguimento, se for caso disso.	Sim, se o endereço de correio eletrónico da pessoa de contacto secundária ou um endereço de correio eletrónico funcional da equipa que pode ser utilizado pela autoridade competente para a comunicação de seguimento estiver disponível	Alfanumérico
11. Telefone da pessoa de contacto secundária	Número de telefone da pessoa de contacto secundária que pode ser utilizado pela autoridade competente para a comunicação de seguimento, se for caso disso. O número de telefone deve ser comunicado com todos os prefixos internacionais (por exemplo, +33XXXXXXXXX).	Sim, se o número de telefone da pessoa de contacto secundária que pode ser utilizado pela autoridade competente para a comunicação de seguimento estiver disponível.	Alfanumérico
12. Data e hora de deteção da ciberameaça	Data e hora em que a entidade financeira tomou conhecimento da ciberameaça significativa.	Sim	Norma ISO 8601 UTC (AAAA-MM-DD hh: mm:ss)
13. Descrição da ciberameaça significativa	Descrição dos aspetos mais pertinentes da ciberameaça significativa. As entidades financeiras devem fornecer: a) Uma panorâmica geral dos aspetos mais pertinentes da ciberameaça significativa; b) Os riscos conexos daí decorrentes, incluindo as potenciais vulnerabilidades dos sistemas da entidade financeira que possam ser exploradas; c) Informações sobre a probabilidade de materialização da ciberameaça significativa; e d) Informações acerca da fonte de informações sobre a ciberameaça.	Sim	Alfanumérico
14. Informação sobre o potencial impacto	Informação sobre o potencial impacto da ciberameaça na entidade financeira, nos seus clientes ou contrapartes financeiras, caso a ciberameaça se tenha materializado	Sim	Alfanumérico
15. Critérios de classificação de incidentes potenciais	Os critérios de classificação que poderiam ter desencadeado um relatório sobre um incidente de caráter severo se a ciberameaça se tivesse materializado.	Sim	Escolha (múltipla): — clientes, contrapartes financeiras e operações afetadas, — impacto em termos de reputação, — duração e tempo de indisponibilidade do serviço, — distribuição geográfica, — perdas de dados, — serviços críticos afetados, — impacto económico.

Campo de dados		Descrição	Campo obrigatório	Tipo de campo
16.	Estado da ciberameaça	Informações sobre o estado da ciberameaça para a entidade financeira e se houve alterações na atividade de ameaça. Se a ciberameaça tiver deixado de comunicar com os sistemas de informação da entidade financeira, o estado pode ser assinalado como inativo. Se a entidade financeira tiver informações de que a ameaça permanece ativa contra outras partes ou o sistema financeiro no seu conjunto, o estado deve ser assinalado como ativo.	Sim	Escolha: — ativo, — inativo.
17.	Medidas tomadas para evitar a materialização	Informações de alto nível sobre as medidas tomadas pela entidade financeira para impedir a materialização das ciberameaças significativas, se aplicável.	Sim	Alfanumérico
18.	Notificação a outras partes interessadas	Informações sobre a notificação da ciberameaça a outras entidades financeiras ou autoridades.	Sim, se outras entidades financeiras ou autoridades tiverem sido informadas sobre a ciberameaça	Alfanumérico
19.	Indicadores de exposição a riscos	Informações relacionadas com a ciberameaça que possam ajudar a identificar atividades maliciosas numa rede ou num sistema de informação (indicadores de exposição a riscos), se for caso disso. Os indicadores da exposição a riscos fornecidos pela entidade financeira podem incluir, entre outros, as seguintes categorias de dados: a) Endereços IP; b) Endereços URL; c) Domínios; d) Dispersão dos ficheiros; e) Dados sobre o *software* malicioso (nome do *software* malicioso, nomes de ficheiros e respetiva localização, chaves de registo específicas associadas a atividades de *software* malicioso); f) Dados relativos à atividade da rede (portas, protocolos, endereços, encaminhadores, agentes de utilizador, cabeçalhos, registos específicos ou padrões distintivos no tráfego de rede); g) Dados de mensagens de correio eletrónico (remetente, destinatário, assunto, cabeçalho, conteúdo); h) Pedidos de DNS e configurações do registo; i) Atividades da conta de utilizador (início de sessão, atividade de conta de utilizador privilegiada, aumento de privilégios); j) Tráfego na base de dados (ler/escrever), pedidos para o mesmo ficheiro. Este tipo de informação pode incluir dados relativos a indicadores que descrevem padrões de tráfego de rede correspondentes a ataques conhecidos/comunicações *botnet*, endereços IP de máquinas infetadas com *software* malicioso (*bots*), dados relativos a servidores de «comando e controlo» utilizados por *software* malicioso (geralmente domínios ou endereços IP) e URL relativos a sítios de *phishing* ou sítios Web observados que alojam *software* malicioso ou *kits* de exploração.	Sim, se estiverem disponíveis informações sobre indicadores de exposição a riscos relacionados com a ciberameaça	Alfanumérico
20.	Outras informações pertinentes	Quaisquer outras informações pertinentes sobre a ciberameaça significativa.	Sim, se aplicável e se existirem outras informações disponíveis, não abrangidas pelo modelo	Alfanumérico