NOTIFICAÇÃO INICIAL — REGULAMENTO DORA – INCIDENTE DE CARÁCTER SEVERO RELACIONADO COM TIC

Campo de dados	Descrição	Tipo de campo
Informação relativa ao tratamento de dados pessoais		
1. Política de tratamento de dados pessoais	Consentimento do tratamento de dados pessoais.	Escolha: — Li e tomei conhecimento
Tipo de apresentação		
2. Tipo de apresentação	Indicar o tipo de notificação ou relatório de incidente apresentado[1].	Escolha: — Notificação Inicial; — Incidente de carácter severo reclassificado como sendo de carácter não severo.
Informação da entidade		
3. Informação da entidade	Indicação se a entidade financeira responsável pelo preenchimento do relatório é a mesma afetada pelo incidente[2].	Escolha: — Sim; — Não.
Informação da entidade que apresenta o relatório		
4. Nome da entidade que apresenta o relatório	Denominação legal completa da entidade que apresenta o relatório. (se a entidade que apresenta o relatório for diferente da entidade afetada pelo incidente).	Alfanumérico.
5. Código *LEI* da entidade que apresenta o relatório	Código de identificação da entidade que apresenta o relatório.[3]	Alfanumérico.
Informação da entidade afetada		
6. 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	Escolha: — Empresa de seguros ou de resseguros; — Mediador de seguros, mediador

[1] Se for selecionado a opção "Incidente de carácter severo reclassificado como sendo de carácter não severo", passa para a secção "Outras Informações".

[2] Se a entidade financeira que apresenta o relatório for a mesma que foi afetada, passa para a secção "Informação da entidade afetada".

[3] 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.

	apresentado. Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, selecionar os diferentes tipos de entidades financeiras abrangidas pelo relatório agregado.	de resseguros ou mediador de seguros a título acessório; — Sociedade gestora de fundos de pensões.
7. Nome da entidade financeira afetada	Denominação legal completa da entidade afetada.[4]	Alfanumérico.
8. Código *LEI* da entidade afetada pelo incidente	Identificador de entidade jurídica (*LEI*) da entidade financeira afetada pelo incidente de carácter severo relacionado com as TIC, atribuído em conformidade com a Organização Internacional de Normalização.[5]	Alfanumérico.
9. Nome da pessoa de contacto principal	Nome e apelido da pessoa de contacto principal da entidade financeira[6].	Alfanumérico.
10. 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[7].	Alfanumérico.
11. 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[8].	Alfanumérico.

[4] Em caso de comunicação agregada:
a) Lista de todos os nomes das entidades financeiras afetadas pelo incidente de carácter 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 carácter severo de forma agregada, conforme referido no artigo 7.º do Regulamento de Execução (UE) 2025/302, deve enumerar os nomes de todas as entidades financeiras afetadas pelo incidente, separados por ponto e vírgula.
[5] Em caso de comunicação agregada:
a) Uma lista de todos os códigos LEI das entidades financeiras afetadas pelo incidente de carácter severo relacionado com as TIC, separados por ponto e vírgula;
b) O terceiro prestador de serviços que apresenta uma notificação de incidente de carácter severo ou de forma agregada, conforme referido no artigo 7.º do Regulamento de Execução (UE) 2025/302, 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.
[6] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, o nome da pessoa de contacto principal na entidade que apresenta o relatório agregado.
[7] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, o endereço eletrónico da pessoa de contacto principal na entidade que apresenta o relatório agregado.
[8] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, 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, +351XXXXXXXXX).

12. Nome da pessoa de contacto secundária	Nome e apelido da pessoa de contacto secundária da entidade financeira.	Alfanumérico.
13. Endereço de correio eletrónico da pessoa de contacto secundária	Endereço eletrónico da pessoa de contacto secundária que pode ser utilizado pela autoridade competente para a comunicação de seguimento.	Alfanumérico.
14. 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.[9]	Alfanumérico.
Informações do grupo		
15. Informação se a entidade afetada pertence a um grupo financeiro	Indicação se a entidade financeira pertence a um grupo financeiro[10].	Escolha: — Sim; — Não.
16. Nome da empresa-mãe de topo	Nome da empresa-mãe de topo do grupo a que a entidade financeira afetada pertence, se aplicável.	Alfanumérico.
17. Código *LEI* da empresa-mãe de topo	*LEI* da empresa-mãe de topo do grupo a que a entidade financeira afetada pertence, se aplicável.	Alfanumérico
Informação relativa ao Incidente		
18. Código de referência do incidente	Código de referência do incidente atribuído pela entidade financeira. O código deverá apresentar o formato RI-CE-Ano_Mês-Numeração do reporte (ex. RI-1234-202404-01-NI)[11].	Alfanumérico.
19. Data e hora de deteção do incidente de carácter severo	Data e hora em que a entidade financeira tomou conhecimento do incidente relacionado com as TIC. No caso de incidentes recorrentes, a	AAAA-MM-DD hh:mm:ss.

[9] O número de telefone deve ser comunicado com todos os prefixos internacionais (por exemplo, +351XXXXXXXXX).
[10] Se a empresa não pertencer a um grupo financeiro, passa apara a secção "Informação relativa ao incidente".
[11] Sendo que:
RI – Reporte de Incidentes.
CE – Código Estatístico da entidade (a preencher pela entidade).
Ano – Ano atual do reporte de incidentes.
Mês – Mês atual do reporte de incidentes (a preencher pela entidade).
Numeração do reporte – Número de identificação do reporte indicado pela empresa, a iniciar na numeração "01" (a preencher pela entidade).
NI – Notificação Inicial.

relacionado com as TIC	data e hora em que foi detetado o último incidente relacionado com as TIC.	
20. Data e hora de classificação do incidente relacionado com as TIC como sendo de carácter severo	Data e hora em que o incidente relacionado com as TIC foi classificado como sendo de carácter severo de acordo com os critérios de classificação estabelecidos no Regulamento Delegado (UE) 2024/1772[12].	AAAA-MM-DD hh:mm:ss.
21. Descrição do incidente de carácter severo relacionado com as TIC	Descrição dos aspetos mais pertinentes do incidente de carácter severo relacionado com as TIC[13].	Alfanumérico.
22. 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 carácter severo e a subsequente notificação e comunicação[14].	Escolha: — 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; — Impactos económicos.
23. Limiares de materialidade para o critério de classificação "Distribuição geográfica"	Estados-Membros do EEE afetados pelo incidente de carácter severo relacionado com as TIC (se for atingido o limiar de "Distribuição geográfica")[15].	Alfanumérico.
24. Deteção do incidente de carácter severo relacionado com	Informações sobre a forma como o incidente de carácter severo relacionado com as TIC foi detetado.	Escolha: — Segurança informática; — Pessoal;

[12] https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=OJ:L_202500302.

[13] 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).

[14] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, os critérios de classificação que desencadearam a determinação do incidente relacionado com as TIC como sendo de carácter severo para, pelo menos, uma ou mais entidades financeiras.

[15] Ao avaliar o impacto do incidente de carácter severo relacionado com as TIC noutros Estados-Membros, as entidades financeiras devem ter em conta os artigos 4.º e 12.º do Regulamento Delegado (UE) 2024/1772.

as TIC		— Auditoria interna; — Auditoria externa; — Clientes; — Contrapartes financeiras; — Terceiro prestador de serviços; — Atacante; — Sistemas de monitorização; — Autoridade/agência/organismo de aplicação da lei; — Outro;
25. Indicação sobre se o incidente tem origem num terceiro prestador de serviços ou noutra entidade financeira	Indicação sobre se o incidente de carácter severo relacionado com as TIC tem origem num terceiro prestador de serviços ou noutra entidade financeira[16].	Alfanumérico.
26. 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.	Escolha: — Sim; — Não.
27. Outras informações	Quaisquer outras informações não abrangidas pelas questões anteriores[17].	Alfanumérico.

[16] Se o incidente de carácter severo teve origem num terceiro prestador de serviços, indique o nome, código *LEI* ou EUID.
[17] No caso de reclassificação de um incidente relacionado com as TIC de caráter severo para caráter não severo, especifique as justificativas para essa alteração, indicando a data e hora da reclassificação no formato AAAA-MM-DD hh:mm:ss.

RELATÓRIO INTERCALAR — REGULAMENTO DORA — INCIDENTE DE CARÁCTER SEVERO RELACIONADO COM TIC

Campo de dados	Descrição	Tipo de campo
Tipo de apresentação		
1. Tipo de apresentação	Indicar o tipo de notificação ou relatório de incidente apresentado[18].	Escolha: — Relatório Intercalar; — Incidente de carácter severo reclassificado como sendo de carácter não severo.
Informação relativa ao incidente		
2. Código de referência do incidente	Código de referência do incidente atribuído pela entidade financeira. O código deverá apresentar o formato RI-CE-Ano_Mês-Numeração do reporte (ex. RI-1234-202404-01-Rin) [19].	Alfanumérico.
3. Data e hora de ocorrência do incidente	Data e hora em que ocorreu o incidente de carácter severo relacionado com as TIC, se diferente do momento em que a entidade financeira tomou conhecimento do incidente de carácter severo relacionado com as TIC.	AAAA-MM-DD hh:mm:ss.
Critério "Clientes, contrapartes financeiras e operações afetadas"		
4. Cumprimento do critério "Clientes, contrapartes financeiras e operações afetadas"	Indicação se o incidente cumpre os requisitos do critério "Clientes, contrapartes financeiras	Escolha: — Sim; — Não.

[18] Se for selecionado a opção "Incidente de carácter severo reclassificado como sendo de carácter não severo", passa para a secção "Outras Informações".
[19] Sendo que:
RI – Reporte de Incidentes.
CE – Código Estatístico da entidade (a preencher pela entidade).
Ano – Ano atual do reporte de incidentes.
Mês – Mês atual do reporte de incidentes (a preencher pela entidade).
Numeração do reporte – Número de identificação do reporte indicado pela empresa, a iniciar na numeração "01" (a preencher pela entidade).
Rin – Relatório Intercalar.

	e operações afetadas"[20]	
5. Número de clientes afetados	Indicação do número de clientes afetados pelo incidente de carácter severo relacionado com as TIC que utilizam o serviço prestado pela entidade financeira[21].	Número inteiro.
6. Percentagem de clientes afetados	Indicação da percentagem de clientes afetados pelo incidente de carácter severo relacionado com as TIC em relação ao número total de clientes que utilizam o serviço afetado prestado pela entidade financeira[22].	Número compreendido entre 0 e 100).
7. Número de contrapartes financeiras afetadas	Indicação do número de contrapartes financeiras afetadas pelo incidente de carácter severo relacionado com as TIC que celebraram um contrato com a entidade financeira[23].	Número inteiro.
8. Percentagem de contrapartes financeiras afetadas	Indicação da percentagem de contrapartes financeiras afetadas pelo incidente de carácter severo relacionado com as TIC em relação ao número total de contrapartes financeiras que celebraram um contrato com a entidade	Número Compreendido entre 0 e 100.

[20] Se o incidente reportado não cumprir o critério em questão, passa para a secção «Cumprimento do critério "Impacto em termos de reputação"».

[21] 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 Regulamento de Execução (UE) 2025/302, uma entidade financeira deve dividir a soma de todos os clientes afetados pelo número total de clientes de todas as entidades financeiras afetadas.

[22] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, uma entidade financeira deve dividir a soma de todos os clientes afetados pelo número total de clientes de todas as entidades financeiras afetadas.

[23] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, o número total de contrapartes financeiras afetadas em todas as entidades financeiras.

	financeira[24].	
9. Impacto nos clientes ou contrapartes financeiras pertinentes	Indicação da existência de 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	Escolha: — Sim; — Não.
10. Número de operações afetadas	Número de operações afetadas pelo incidente de carácter severo relacionado com as TIC[25].	Número inteiro.
11. Percentagem de operações afetadas	Indicação da percentagem de operações afetadas em relação ao número médio diário de operações nacionais e transfronteiras realizadas pela entidade financeira relacionadas com o serviço afetado[26].	Número compreendido entre 0 e 100.
12. Valor das operações afetadas	Indicação do valor monetário total das operações afetadas pelo incidente de carácter severo relacionado com as TIC, que deve ser avaliado em conformidade com o artigo 1.º, n.º 4, e o artigo 9.º, n.º 1, alínea e), do	Indicação do valor utilizando uma precisão mínima equivalente a milhares de unidades (por exemplo, 2,5 kEUR em vez de 2 500 EUR).

[24] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, indicar a soma de todas as contrapartes financeiras afetadas dividida pelo número total de contrapartes financeiras de todas as entidades financeiras afetadas.

[25] 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. 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 Regulamento de Execução (UE) 2025/302, indicar o número total de operações afetadas em todas as entidades financeiras.

[26] 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 Regulamento de Execução (UE) 2025/302, 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.

	Regulamento Delegado (UE) 2024/1772[27].	
13. 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 4 a 11 são reais ou estimados, ou se houve ou não impacto.	Escolha: — 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.
Critério "Impacto em termos de reputação"		
14. Cumprimento do critério "Impacto em termos de reputação"	Indicação se o incidente cumpre os requisitos do critério "Impacto em termos de reputação"[28].	Escolha: — Sim; — Não.
15. Impacto em termos de reputação	Indicação das informações sobre o impacto em termos de reputação resultante do incidente de carácter severo relacionado com as TIC a que se referem os artigos 2.º e 10.º do Regulamento Delegado (UE) 2024/1772[29].	Escolha: — O incidente de carácter severo relacionado com as TIC foi referido nos meios de comunicação social; — O incidente de carácter 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

[27] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, o valor total das operações afetadas em todas as entidades financeiras.
[28] Se o incidente reportado não cumprir o critério em questão, passa para a secção «Cumprimento do critério "Duração e tempo de indisponibilidade do serviço"».
[29] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, as categorias de impacto em termos de reputação aplicáveis a pelo menos uma entidade financeira.

		regulamentares em resultado do incidente de carácter 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 carácter severo relacionado com as TIC.
16. Informações contextuais sobre o impacto em termos de reputação	Indicação das informações que descrevam a forma como o incidente de carácter 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.	Alfanumérico.
Critério "Duração e tempo de indisponibilidade do serviço"		
17. Cumprimento do critério "Impacto em termos de reputação"	Indicação se o incidente cumpre os requisitos do critério "Duração e tempo de indisponibilidade do serviço"[30].	Escolha: — Sim; — Não.
18. Data e hora da recuperação dos serviços, das atividades ou das operações	Indicação da data e hora da recuperação dos serviços, das atividades ou das operações.	AAAA-MM-DD hh:mm:ss.
19. Duração do incidente	Indicação da duração do incidente de carácter severo relacionado com as TIC desde o momento em que esse incidente ocorreu até ao momento em que foi	DD:HH:MM

[30] Se o incidente reportado não cumprir o critério em questão, passa para a secção «Cumprimento do critério "Distribuição geográfica"».

	resolvido[31].	
20. Tempo de indisponibilidade do serviço	Indicação do 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 carácter severo relacionado com as TIC[32].	DD:HH:MM
21. Informações sobre se os números relativos à duração e ao tempo de indisponibilidade do serviço são reais ou estimados.	Informação sobre os valores comunicados nos campos de dados anteriores, indicando se estes são reais ou estimados.	Escolha: — Dados reais; — Estimativas; — Dados reais e estimativas; — Sem informação disponível.
Critério "Distribuição geográfica"		
22. Cumprimento do critério "Distribuição geográfica"	Indicação se o incidente cumpre os requisitos do critério "Distribuição geográfica"[33].	Escolha: — Sim; — Não.
23. Tipos de impacto nos Estados-Membros	Tipos de impacto noutros Estados-	Escolha: — Clientes; — Contrapartes financeiras;

[31] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, as entidades financeiras devem medir a duração mais longa do incidente de carácter severo relacionado com as TIC, se existirem diferenças entre entidades financeiras.

[32] Se o tempo de indisponibilidade do serviço causar um atraso na prestação do serviço após o estabelecimento das atividades ou operações regulares, as entidades financeiras devem medir o tempo de indisponibilidade desde o início do incidente de carácter 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 Regulamento de Execução (UE) 2025/302, as entidades financeiras devem medir a maior duração do tempo de indisponibilidade do serviço, se existirem diferenças entre entidades financeiras.

[33] Se o incidente reportado não cumprir o critério em questão, passa para a secção «Cumprimento do critério "Perda de dados"».

	membros[34].	— 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.
24. Descrição da forma como o incidente tem impacto noutros Estados-Membros	Descrição detalhada do impacto e da gravidade do incidente de carácter severo relacionado com as TIC em cada Estado-Membro afetado	Alfanumérico.
Critério "Perda de dados"		
25. Cumprimento do critério "Perda de dados"	Indicação se o incidente cumpre os requisitos do critério "Perda de dados"[35].	Escolha: — Sim; — Não.
26. Limiares de materialidade para o critério de classificação "Perdas de dados"	Indicação do tipo de perdas de dados decorrentes do incidente de carácter severo relacionado com as TIC, no que respeita à disponibilidade, autenticidade, integridade e confidencialidade dos dados[36].	Escolha: — Disponibilidade; — Autenticidade; — Integridade; — Confidencialidade.
27. Descrição das perdas de dados	Descrição do impacto do incidente de carácter	Alfanumérico.

[34] Indicar se o incidente de carácter 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
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.

[35] Se o incidente reportado não cumprir o critério em questão, passa para a secção «Cumprimento do critério "Serviços críticos afetados"».

[36] 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 Regulamento de Execução (UE) 2025/302, as perdas de dados que afetem pelo menos uma entidade financeira.

	severo relacionado com as TIC na disponibilidade, autenticidade, integridade e confidencialidade dos dados críticos[37].	
Critério "Serviços críticos afetados"		
28. Cumprimento do critério "Serviços críticos afetados"	Indicação se o incidente cumpre os requisitos do critério "Serviços críticos afetados"[38].	Escolha: — Sim; — Não.
29. Critério de classificação "Serviços críticos afetados"	Informações detalhadas sobre os serviços ou atividades críticos afetados[39].	Alfanumérico.
30. Tipo do incidente	Classificação dos incidentes por tipo.	Escolha: — Relacionado com a cibersegurança; — Falha do processo; — Avaria do sistema; — Acontecimento externo; — Relacionado com pagamentos; — Outro.
31. Ameaças e técnicas utilizadas pelo agente de ameaça	Indicação das ameaças e técnicas utilizadas pelo autor da ameaça.	Escolha: — Engenharia social [incluindo mistificação da interface (*phishing*)]; — Negação de serviço ; — Usurpação de identidade; — Encriptação de dados para impacto (*ransomware*);

[37] Em conformidade com 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 Regulamento de Execução (UE) 2025/302, 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.

[38] Se o incidente reportado não cumprir o critério em questão, passa para a secção «Comunicação e medidas temporárias para recuperar do incidente."»

[39] 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 afetadas 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 Regulamento de Execução (UE) 2025/302, o impacto nos serviços críticos aplicável a pelo menos uma entidade financeira.

		— Desvio de recursos; — Exfiltração e manipulação de dados, incluindo usurpação de identidade; — Destruição de dados; — Desfiguração (*defacement*), — Ataque à cadeia de abastecimento; — Outro.
32. 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[40].	Alfanumérico.
33. Componentes afetados da infraestrutura de apoio aos processos operacionais	Indicação 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 carácter severo relacionado com as TIC.[40]	Escolha: — Sim; — Não; — Informação não disponível.
34. Informações sobre os componentes afetados da infraestrutura de apoio aos processos operacionais	Descrição detalhada do incidente de carácter severo relacionado com as TIC nos componentes da infraestrutura que apoiam os processos operacionais, incluindo *hardware* e *software*.[40]	Alfanumérico
35. Impacto nos interesses financeiros dos clientes	Informações sobre se o incidente de carácter severo relacionado com as TIC afetou os interesses financeiros	Escolha: — Sim; — Não; — Informação não disponível.

[40] Sugere-se a consulta dos pontos 3.27 e 3.29 do Anexo II Regulamento de Execução (UE) 2025/302 de 23 de outubro de 2024 para orientação sobre a definição e identificação dos processos operacionais críticos a considerar no contexto de incidentes de carácter severo relacionados com as TIC.

	dos clientes.	
Comunicação e medidas temporárias para recuperar do incidente		
36. Comunicação a outras autoridades	Especificação de outras autoridades que tenham sido informadas sobre o incidente de carácter severo relacionado com as TIC.	Escolha: — Polícia/serviços de aplicação da lei; — CSIRT; — Comissão Nacional de Proteção de Dados (CNPD); — Centro Nacional de Cibersegurança (CNCS); — Nenhuma; — Outra.
37. Ações/medidas temporárias tomadas ou previstas para recuperar do incidente	Indicação sobre se a entidade financeira aplicou (ou tenciona aplicar) quaisquer medidas temporárias que tenham sido tomadas (ou estejam previstas) para recuperar do incidente de carácter severo relacionado com as TIC.	Escolha: — Sim; — Não.
38. Descrição de quaisquer ações e medidas temporárias tomadas ou previstas para recuperar do incidente	Descrição de quaisquer ações e medidas temporárias tomadas ou previstas para recuperar do incidente[41].	Alfanumérico.
39. Outras informações	Quaisquer outras informações não abrangidas pelas questões anteriores[42].	Alfanumérico.

[41] 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.
[42] No caso de reclassificação de um incidente relacionado com as TIC de caráter severo para caráter não severo, especifique as justificativas para essa alteração, indicando a data e hora da reclassificação no formato AAAA-MM-DD hh:mm:ss.

RELATÓRIO FINAL — REGULAMENTO DORA — INCIDENTE DE CARÁCTER SEVERO RELACIONADO COM TIC

Campo de dados	Descrição	Tipo de campo
Tipo de apresentação		
1. Tipo de apresentação	Indicar o tipo de notificação ou relatório de incidente apresentado[43].	Escolha: — Relatório Final; — Incidente de carácter severo reclassificado como sendo de carácter não severo.
Informação relativa ao incidente		
2. Código de referência do incidente	Código de referência do incidente atribuído pela entidade financeira. O código deverá apresentar o formato RI-CE-Ano_Mês-Numeração do reporte (ex. RI-1234-202404-01-RF)[44].	Alfanumérico.
3. Classificação de alto nível das causas profundas do incidente	Classificação das causas do incidente de carácter severo relacionado com as TIC no âmbito dos tipos de incidentes.	Escolhas: — Ações maliciosas; — Falha do processo; — Avaria/falha do sistema; — Erro humano; — Acontecimento externo.
4. Classificação pormenorizada das causas do incidente – Ações maliciosas	Classificação pormenorizada das causas do incidente de carácter 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	Escolhas: — Ações internas deliberadas; — Danos físicos deliberados/ manipulação/ roubo; — Ações fraudulentas.

[43] Se for selecionado a opção "Incidente de carácter severo reclassificado como sendo de carácter não severo", passa para a secção "Outras Informações".
[44] Sendo que:
RI – Reporte de Incidentes.
CE – Código Estatístico da entidade (a preencher pela entidade).
Ano – Ano atual do reporte de incidentes.
Mês – Mês atual do reporte de incidentes (a preencher pela entidade).
Numeração do reporte – Número de identificação do reporte indicado pela empresa, a iniciar na numeração "01" (a preencher pela entidade).
RF – Relatório Final.

	dados n.º 2: **Ações maliciosas.**	
5. Classificação pormenorizada das causas do incidente – Falha do processo	Classificação pormenorizada das causas do incidente de carácter 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 n.º 2: **Falha do processo.**	Escolha: — Acompanhamento insuficiente ou falha do acompanhamento e controlo; — Funções e responsabilidades insuficientes/pouco claras; — Falha do processo de gestão dos riscos associados às TIC; — Insuficiência ou falha das operações de TIC e das operações de segurança das TIC; — Insuficiência ou falha da gestão de projetos de TIC; — Inadequação das políticas, procedimentos e documentação internos; — Aquisição, desenvolvimento e manutenção inadequados dos sistemas de TIC; — Outro.
6. Classificação adicional das causas profundas do incidente – Falha do processo	Classificação adicional das causas profundas do incidente de carácter severo relacionado com as TIC no âmbito do tipo de incidente, incluindo as seguintes categorias de classificação adicionais relacionadas com a categoria pormenorizada que devem ser comunicadas no âmbito do campo n.º 4: **Falha do processo**[45].	Escolha: — 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

[45] A classificação adicional é aplicável às categorias do ponto 5 nos casos em que representam um detalhe mais rigoroso das causas dos incidentes. Consultar o ponto 4.3 do Anexo II do Regulamento de Execução (EU) 2025/302, de 23 de outubro de 2024.

		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*.
7. Classificação pormenorizada das causas do incidente – Avaria/falha no sistema	Classificação pormenorizada das causas do incidente de carácter 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 n.º 2: **Avaria/falha no sistema**.	Escolha; — Capacidade e desempenho do *hardware*; — Manutenção do *hardware*; — Obsolescência/envelhecimento do *hardware*; — Compatibilidade/configuração do *software*; — Desempenho do *software*; — Configuração da rede; — Danos físicos; — Outro.
8. Classificação pormenorizada das causas do incidente – Erro humano	Classificação pormenorizada das causas do incidente de carácter 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 n.º 2: **Erro humano**.	Escolha: — Omissão; — Erro; — Competências e conhecimento; — Recursos humanos inadequados; — Falha de comunicação; — Outro.
9. Classificação pormenorizada das causas do incidente – Acontecimento externo	Classificação pormenorizada das causas do incidente de carácter 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 n.º 2: **Acontecimento**	Escolha: — Catástrofes naturais/força maior; — Falhas de terceiros; — Outro.

	externo.	
10. Informações sobre as causas profundas do incidente	Descrição da sequência dos acontecimentos que conduziram ao incidente de carácter 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 carácter severo relacionado com as TIC.	Alfanumérico.
11 Resumo da resolução do incidente	Informações adicionais sobre as ações/medidas tomadas/previstas para resolver permanentemente o incidente de carácter severo relacionado com as TIC e para evitar que esse incidente volte a ocorrer. Ensinamentos retirados do incidente de carácter severo relacionado com as TIC.	Alfanumérico
12. Data e hora em que foi abordada a causa principal do incidente	Data e hora em que a causa principal do incidente foi abordada.	AAAA-MM-DD hh:mm:ss
13. Data e hora da resolução do incidente	Data e hora em que o incidente foi resolvido.	AAAA-MM-DD hh:mm:ss
14. Informação sobre se a data de resolução permanente dos incidentes difere da data de execução inicialmente prevista	Descrição das razões pelas quais a data de resolução permanente do incidente de carácter severo relacionados com as TIC é diferente da data de resolução inicialmente prevista, quando aplicável.	Alfanumérico
Critério "Impacto económico"		
15. Cumprimento do critério "Impacto económico"	Indicação se o incidente cumpre os requisitos do critério "Impacto económico"[46].	Escolha: — Sim; — Não.

[46] Se o incidente reportado não cumprir o critério em questão, passa para a secção "Incidentes de carácter não severo."

16. Limiar de materialidade para o critério de classificação "Impacto económico"	Informações pormenorizadas sobre os limiares eventualmente atingidos pelo incidente de carácter severo relacionado com as TIC em relação ao critério "Impacto económico"[47].	Alfanumérico.
17. Montante dos custos diretos e indiretos	Indicação do montante total dos custos e perdas brutos diretos e indiretos incorridos pela entidade financeira decorrentes do incidente de carácter severo relacionado com as TIC[48].	Indicação do valor e da unidade monetária utilizando uma precisão mínima equivalente a milhares de unidades.
18. Montante das recuperações financeiras	Indicação do montante total das recuperações financeiras[49].	Indicação do valor e da unidade monetária utilizando uma precisão mínima equivalente a milhares de unidades.
Incidentes de carácter não severo recorrentes		
19. Informações sobre	Informações sobre se a	Escolha:

[47] Referido nos artigos 7.º e 14.º do Regulamento Delegado (UE) 2024/1772. Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, 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.

[48] 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 carácter severo relacionado com as TIC;
ii) provisões ou reservas contabilizadas na conta de resultados contra perdas prováveis relacionadas com o incidente de carácter severo relacionado com as TIC;
iii) perdas pendentes, sob a forma de perdas decorrentes do incidente de carácter 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 carácter 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.

[49] Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, as entidades financeiras devem ter em conta o montante total das recuperações financeiras em todas as entidades financeiras.

se os incidentes de carácter não severo são recorrentes	entidade financeira identificou mais do que um incidente de carácter não severo relacionado com as TIC que, pela sua natureza recorrente[50], é considerado, em conjunto, um incidente de carácter severo na aceção do artigo 8. º, n. º 2, do Regulamento Delegado (UE) 2024/1772[51].	— Sim; —Não.
20. Incidentes recorrentes de carácter não severo.	Indicação do número total de ocorrências destes incidentes de carácter não severo relacionados com as TIC.	Alfanumérico.
21. 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.	AAAA-MM-DD hh:mm:ss
22. Outras informações	Quaisquer outras informações não abrangidas pelas questões anteriores[52].	Alfanumérico.

[50] Consideram-se "incidentes recorrentes" aqueles que, apesar de individualmente classificados como não severos, quando analisados em conjunto, atingem os critérios de severidade estabelecidos pela regulamentação.
[51] Se a entidade financeira não identificou mais do que um incidente de carácter não severo relacionado com as TIC, passa para o fim do formulário.
[52] No caso de reclassificação de um incidente relacionado com as TIC de caráter severo para caráter não severo, especifique as justificativas para essa alteração, indicando a data e hora da reclassificação no formato AAAA-MM-DD hh:mm:ss.

NOTIFICAÇÃO DE CIBERAMEAÇAS SIGNIFICATIVAS — REGULAMENTO DORA

Campo de dados	Descrição	Tipo de campo
Informação relativa ao tratamento de dados pessoais		
1. Política de tratamento de dados pessoais	Consentimento do tratamento de dados pessoais.	Escolha: — Li e tomei conhecimento
Informação da entidade		
2. Informação da entidade	Indicação se a entidade financeira responsável pelo preenchimento do relatório é a mesma afetada pelo incidente[53].	Escolha: — Sim; — Não.
3. Nome da entidade que apresenta a notificação	Denominação legal completa da entidade que apresenta a notificação (se a entidade que apresenta a notificação for diferente da entidade afetada pelo incidente).	Alfanumérico.
4. Código *LEI* da entidade que apresenta a notificação	Código de identificação da entidade que apresenta a notificação.[54]	Alfanumérico.
Informação da entidade afetada		
5. Nome da entidade financeira afetada	Denominação legal completa da entidade afetada (se a entidade que apresenta a notificação for igual à entidade afetada pelo incidente).[55]	Alfanumérico.
6. Código Estatístico	Código estatístico utilizado para efeitos de reporte à ASF.	Número inteiro.
8. Código *LEI* da entidade afetada	Identificador de entidade jurídica (*LEI*) da entidade financeira afetada	Alfanumérico.

[53] Se a entidade financeira que apresenta o relatório for a mesma que foi afetada, passa para a secção "Informação da entidade afetada".

[54] 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.

[55] Em caso de comunicação agregada:
a) Lista de todos os nomes das entidades financeiras afetadas pelo incidente de carácter 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 carácter severo de forma agregada, conforme referido no artigo 7.º do Regulamento de Execução (UE) 2025/302, deve enumerar os nomes de todas as entidades financeiras afetadas pelo incidente, separados por ponto e vírgula.

pelo incidente	pelo incidente de carácter severo relacionado com as TIC, atribuído em conformidade com a Organização Internacional de Normalização.[56]	
9. Tipo de entidade financeira afetada	Tipo de entidade a que se refere o artigo 2.º, n.º 1, alíneas a) a t), do Regulamento (UE) 2022/2554, relativamente à qual a notificação é apresentada. Em caso de comunicação agregada a que se refere o artigo 7.º do Regulamento de Execução (UE) 2025/302, selecionar os diferentes tipos de entidades financeiras abrangidas pela notificação agregada.	Escolha: — Empresa de seguros ou de resseguros; — Mediador de seguros, mediador de resseguros ou mediador de seguros a título acessório; — Sociedade gestora de fundos de pensões.
Informações de contacto		
9. Nome da pessoa de contacto principal	Nome e apelido da pessoa de contacto principal da entidade financeira.	Alfanumérico.
10. 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.	Alfanumérico.
11. 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.[57]	Alfanumérico.
12. Nome da pessoa de contacto secundária	Nome e apelido da pessoa de contacto secundária da entidade financeira.	Alfanumérico.
13. Endereço de correio eletrónico da pessoa de contacto	Endereço eletrónico da pessoa de contacto secundária que pode ser utilizado pela autoridade competente para a comunicação de	Alfanumérico.

[56] Em caso de comunicação agregada:
a) Uma lista de todos os códigos LEI das entidades financeiras afetadas pelo incidente de carácter severo relacionado com as TIC, separados por ponto e vírgula;
b) O terceiro prestador de serviços que apresenta uma notificação de incidente de carácter severo ou de forma agregada, conforme referido no artigo 7.º do Regulamento de Execução (UE) 2025/302, 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.
[57] O número de telefone deve ser comunicado com todos os prefixos internacionais (por exemplo, +351XXXXXXXXX).

secundária	seguimento.	
14. 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.[58]	Alfanumérico.
Informação sobre a ciberameaça significativa		
15. Data e hora de deteção da ciberameaça	Data e hora em que a entidade financeira tomou conhecimento da ciberameaça significativa e quaisquer outros carimbos temporais pertinentes relacionados com a ciberameaça significativa[59].	Alfanumérico.
16. Descrição da ciberameaça significativa	Descrição dos aspetos mais pertinentes da ciberameaça significativa[60].	Alfanumérico.
17. 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.	Alfanumérico.
18. Critérios de classificação de potenciais incidentes	Os critérios de classificação que poderiam ter desencadeado um relatório sobre um incidente de carácter severo se a ciberameaça se tivesse materializado.	Escolha: — 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.
19. Estado da ciberameaça	Informações sobre o estado da ciberameaça para a entidade financeira e se houve alterações na	Escolha: —Ativo; — Inativo.

[58] O número de telefone deve ser comunicado com todos os prefixos internacionais (por exemplo, +351XXXXXXXXX).
[59] Deve ser seguido o seguinte formato: "Tipo de timestamp – AAAA-MM-DD hh:mm:ss". Se for reportado mais do que um timestamp, estes devem ser separados com ponto e virgula.
[60] 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.

	atividade de ameaça[61].	
20. 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.	Alfanumérico.
21. Notificação a outras partes interessadas	Informações sobre a notificação da ciberameaça significativa a outras entidades financeiras ou autoridades competentes, detalhando quais.	Alfanumérico.
22. Indicadores de exposição a riscos	Informações relacionadas com a ciberameaça que possam auxiliar na identificação de atividades maliciosas em redes ou sistemas de informação (indicadores de exposição a riscos), quando aplicável.	Alfanumérico.
23. Outras informações pertinentes	Indicação de quaisquer outras informações pertinentes sobre a ciberameaça significativa que não foi descrita nos restantes campos de dados.	Alfanumérico.

[61] 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.