EBA/GL/2017/10

19/12/2017

Orientações

sobre a comunicação de incidentes de caráter severo, ao abrigo da Diretiva (UE) 2015/2366 (DSP2)

1. Obrigações de cumprimento e de comunicação de informação

Natureza das presentes Orientações

1. O presente documento contém orientações emitidas ao abrigo do artigo 16.º do Regulamento (UE) n.º 1093/2010[1]. Nos termos do artigo 16.º, n.º 3, do referido Regulamento, as autoridades competentes e as instituições financeiras devem desenvolver todos os esforços para dar cumprimento às Orientações.

2. As Orientações refletem a posição da EBA sobre práticas de supervisão adequadas no âmbito do Sistema Europeu de Supervisão Financeira ou sobre o modo como a legislação da União deve ser aplicada num domínio específico. As autoridades competentes, na aceção do artigo 4.º, n.º 2, do Regulamento (UE) n.º 1093/2010, às quais as presentes Orientações se aplicam devem dar cumprimento às mesmas, incorporando-as nas suas práticas de supervisão conforme for mais adequado (por exemplo, alterando o seu enquadramento jurídico ou os seus processos de supervisão), incluindo nos casos em que as orientações são aplicáveis, em primeira instância, a instituições.

Requisitos de notificação

3. Nos termos do disposto no artigo 16.º, n.º 3, do Regulamento (UE) n.º 1093/2010, as autoridades competentes confirmam à EBA se dão ou tencionam dar cumprimento às presentes Orientações, ou, caso contrário, indicam as razões para o não cumprimento até 19/02/2018. Na ausência de qualquer notificação até à referida data, a EBA considerará que as autoridades competentes em causa não cumprem as Orientações. As notificações efetuam-se mediante o envio do modelo disponível no sítio Web da EBA para o endereço compliance@eba.europa.eu com a referência «EBA/GL/2017/10». As notificações devem ser apresentadas por pessoas devidamente autorizadas para o efeito pelas respetivas autoridades competentes. Qualquer alteração no que respeita à situação de cumprimento deve igualmente ser comunicada à EBA.

4. As notificações serão publicadas no sítio Web da EBA, em conformidade com o disposto no artigo 16.º, n.º 3.

[1] 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, 15.12.2010, p.12).

2. Objeto, âmbito de aplicação e definições

Objeto

5. As presentes Orientações derivam do mandato conferido à Autoridade Bancária Europeia (EBA) no âmbito do n.º 3 do artigo 96.º da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno (DSP2), que altera as Diretivas (UE) 2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE.

6. Em particular, as presentes Orientações definem os critérios para a classificação dos incidentes operacionais ou de segurança de caráter severo a utilizar pelos prestadores de serviços de pagamento, assim como o formato e os procedimentos que os mesmos devem seguir, nos termos do n.º 1 do artigo 96.º da supracitada diretiva, para a comunicação de tais incidentes à autoridade competente do Estado-Membro de origem.

7. Estas Orientações incidem ainda sobre a forma como as autoridades competentes devem avaliar a relevância do incidente e os pormenores constantes dos relatórios de incidente, informação que, de acordo com o n.º 2 do artigo 96.º da referida diretiva, devem partilhar com outras autoridades nacionais.

8. Adicionalmente, as presentes Orientações definem também a forma como os pormenores relevantes dos incidentes comunicados devem ser partilhados com a EBA e com o BCE, tendo em vista a promoção de uma abordagem comum e consistente pelas autoridades competentes.

Âmbito de aplicação

9. As presentes Orientações aplicam-se à classificação e comunicação de incidentes operacionais ou de segurança de caráter severo, em conformidade com o artigo 96.º da Diretiva (UE) 2015/2366.

10. Estas Orientações aplicam-se a todos os incidentes que se enquadram na definição de «incidente operacional ou de segurança de caráter severo», a qual abrange eventos externos e internos, quer sejam maliciosos ou acidentais.

11. As presentes Orientações aplicam-se igualmente aos incidentes operacionais ou de segurança de caráter severo originados fora da União (por exemplo, quando um incidente tenha origem na empresa-mãe ou numa filial estabelecida fora da União) e que afetem os serviços de pagamento prestados por um prestador de serviços de pagamento localizado na União, quer seja de forma direta (quando um serviço relacionado com pagamentos é prestado pela empresa afetada que está sediada em país fora da União) ou indireta (quando a capacidade do

prestador de serviços de pagamento continuar a desempenhar a sua atividade de pagamento é, de alguma forma, prejudicada em resultado do incidente).

Destinatários

12. O primeiro conjunto de Orientações (Secção 4) destina-se aos prestadores de serviços de pagamento, conforme definido no n.º 11 do artigo 4.º da Diretiva (UE) 2015/2366 e conforme referido no n.º 1 do artigo 4.º do Regulamento (UE) n.º 1093/2010.

13. O segundo e terceiro conjunto de Orientações (Secções 5 e 6) destinam-se às autoridades competentes definidas na alínea i) do n.º 2 do artigo 4.º do Regulamento (UE) n.º 1093/2010.

Definições

14. Salvo especificação em contrário, os termos utilizados e definidos na Diretiva (UE) 2015/2366 têm o mesmo significado nas presentes Orientações. Adicionalmente, para efeitos destas Orientações, aplicam-se as seguintes definições:

Incidente operacional ou de segurança	Um evento único ou uma série de eventos conexos e não previstos pelo prestador de serviços de pagamento, que tem, ou poderá vir a ter, um impacto adverso na integridade, disponibilidade, confidencialidade, autenticidade e/ou continuidade dos serviços relacionados com pagamentos.
Integridade	Característica que salvaguarda a exatidão e completude dos ativos (incluindo dados).
Disponibilidade	Característica que permite o acesso e a utilização dos serviços relacionados com pagamentos pelos utilizadores de serviços de pagamento.
Confidencialidade	Característica que inibe o acesso ou a divulgação de informação a indivíduos, entidades ou processos não autorizados.
Autenticidade	Característica que confirma a veracidade de uma fonte.
Continuidade	Característica necessária aos processos, tarefas e ativos de uma organização para que a prestação de serviços relacionados com pagamentos seja totalmente acessível e executada a um nível aceitável predefinido.
Serviços relacionados com pagamentos	Qualquer atividade comercial na aceção da alínea 3) do artigo 4.º da DSP2 e todas as tarefas de suporte técnico necessárias à correta prestação de serviços de pagamento.

3. Execução

Data de aplicação

15. As presentes Orientações entram em vigor em 13 de janeiro de 2018.

4. Orientações destinadas a prestadores de serviços de pagamento sobre a comunicação de incidentes operacionais ou de segurança de caráter severo à autoridade competente do Estado-Membro de origem

Orientação 1: Classificação como incidente de caráter severo

1.1. Os prestadores de serviços de pagamento devem classificar como severos os incidentes operacionais ou de segurança que preencham

a. um ou mais critérios de «nível de impacto superior», ou

b. três ou mais critérios de «nível de impacto inferior»

conforme definido na Orientação 1.4 e tendo em conta a avaliação prevista nas presentes Orientações.

1.2. Os prestadores de serviços de pagamento devem avaliar os incidentes operacionais ou de segurança de acordo com os critérios e respetivos indicadores subjacentes a seguir indicados:

i. Operações afetadas

Os prestadores de serviços de pagamento devem determinar o valor total das operações afetadas, assim como o número de pagamentos comprometidos, em termos percentuais relativamente ao nível normal de operações de pagamento executadas pelos serviços de pagamento afetados.

ii. Utilizadores de serviços de pagamento afetados

Os prestadores de serviços de pagamento devem determinar o número de utilizadores de serviços de pagamento afetados quer em termos absolutos, quer em termos percentuais, relativamente ao número total de utilizadores de serviços de pagamento.

iii. Interrupção do serviço

Os prestadores de serviços de pagamento devem determinar o período de tempo em que o serviço se encontrará provavelmente indisponível para os utilizadores de serviços de pagamento ou em que a ordem de pagamento, na aceção da alínea 13 do artigo 4.º da DSP2, não poderá ser executada pelo prestador de serviços de pagamento.

iv. Impacto económico

Os prestadores de serviços de pagamento devem determinar os custos monetários globais do incidente e ter em conta quer os valores absolutos quer, quando pertinente, a importância relativa desses custos em relação à dimensão do prestador de serviços de pagamento (ou seja, aos fundos próprios de nível 1 do prestador de serviços de pagamento).

v. Encaminhamento para as instâncias superiores internas

Os prestadores de serviços de pagamento devem determinar se o incidente em causa foi, ou provavelmente será, comunicado aos seus diretores executivos.

vi. Outros prestadores de serviços de pagamento ou infraestruturas relevantes potencialmente afetados

Os prestadores de serviços de pagamento devem determinar as prováveis implicações sistémicas do incidente, nomeadamente o risco de contágio de outros prestadores de serviços de pagamento, infraestruturas do mercado financeiro e/ou sistemas de pagamento com cartões.

vii. Impacto na reputação

Os prestadores de serviços de pagamento devem determinar de que forma o incidente pode prejudicar a confiança dos utilizadores no próprio prestador de serviços de pagamento e, de uma forma geral, no serviço em causa ou em todo o mercado.

1.3. Os prestadores de serviços de pagamento devem calcular o valor dos indicadores de acordo com a seguinte metodologia:

i. Operações afetadas

Regra geral, os prestadores de serviços de pagamento devem considerar como «operações afetadas» todas as operações nacionais e transfronteiriças que tenham sido, ou possam vir a ser, direta ou indiretamente afetadas pelo incidente e, nomeadamente, as operações que não tenham sido iniciadas ou processadas, bem como as operações cujo conteúdo da mensagem de pagamento tenha sido alterado e aquelas que tenham sido ordenadas de forma fraudulenta (independentemente dos fundos terem sido recuperados ou não).

Adicionalmente, os prestadores de serviços de pagamento devem considerar como nível normal de operações de pagamento a média diária anual das operações de pagamento nacionais e transfronteiriças executadas pelos mesmos serviços de pagamento que foram afetados pelo incidente, considerando o exercício anterior como período de referência para efeitos de cálculo. Se os prestadores de serviços de pagamento não considerarem este número representativo (por ex. devido à sazonalidade), devem utilizar outra medida mais representativa e transmitir à autoridade competente o racional subjacente a essa abordagem no campo correspondente do modelo de relatório (ver Anexo 1).

ii. Utilizadores de serviços de pagamento afetados

Os prestadores de serviços de pagamento devem considerar como «utilizadores de serviços de pagamento afetados» todos os clientes (nacionais ou estrangeiros, consumidores ou empresas) que possuam um contrato com o prestador de serviços de pagamento afetado

que lhes garante o acesso ao referido serviço e que tenham sofrido ou possam vir a sofrer as consequências do incidente. Para determinar o número de utilizadores de serviços de pagamento que possam ter utilizado o serviço durante o período de ocorrência do incidente, os prestadores de serviços de pagamento devem recorrer a estimativas baseadas nos respetivos históricos de atividade.

No caso de se tratar de um grupo, cada prestador de serviços de pagamento deve apenas considerar os seus próprios utilizadores de serviços de pagamento. Se se tratar de um prestador de serviços de pagamento que disponibilize serviços operacionais a terceiros, o mesmo deve considerar apenas os seus próprios utilizadores de serviços de pagamento (se tiver algum) e os prestadores de serviços de pagamento que usufruem desses serviços operacionais devem avaliar o incidente em relação aos seus próprios utilizadores de serviços de pagamento.

Além disso, os prestadores de serviços de pagamento devem considerar como número total de utilizadores de serviços de pagamento o número agregado de utilizadores de serviços de pagamento nacionais e transfronteiriços contratualmente vinculados no momento do incidente (ou, em alternativa, o valor mais recente disponível) e com acesso ao serviço de pagamento afetado, independentemente da respetiva dimensão ou de serem considerados utilizadores ativos ou passivos dos serviços em causa.

iii. Interrupção do serviço

Os prestadores de serviços de pagamento devem considerar o período de tempo em que qualquer tarefa, processo ou canal relacionado com a prestação de serviços de pagamento está, ou pode vir a estar, interrompido e que impede i) a iniciação e/ou execução de um serviço de pagamento e/ou ii) o acesso a uma conta de pagamento. Os prestadores de serviços de pagamento devem contabilizar o tempo de interrupção do serviço a partir do início da interrupção, considerando quer o período de tempo em que a prestação de serviços de pagamento está disponível ao público, quer as horas de encerramento e os períodos de manutenção, quando relevante e aplicável. Caso os prestadores de serviços de pagamento não consigam determinar a altura em que a interrupção do serviço teve início, devem excecionalmente contabilizar a interrupção a partir do momento da sua deteção.

iv. Impacto económico

Os prestadores de serviços de pagamento devem considerar os custos direta e indiretamente relacionados com o incidente. Entre outros fatores, os prestadores de serviços de pagamento devem ter em conta os fundos ou ativos expropriados, os custos de substituição de *hardware* ou *software*, outros custos judiciais ou de resolução de conflitos, taxas por incumprimento de obrigações contratuais, sanções, responsabilidades externas e perdas de receitas. No que diz respeito aos custos indiretos, os prestadores de serviços de pagamento devem considerar apenas aqueles que já forem do conhecimento ou os que são muito prováveis de se materializar.

v. *Encaminhamento para as instâncias superiores internas*

Os prestadores de serviços de pagamento devem considerar se, em resultado do impacto nos serviços relacionados com pagamentos, o Diretor Executivo de Informação (ou cargo equivalente) foi, ou provavelmente será, informado do incidente fora do âmbito de qualquer procedimento de notificação periódico e numa base continuada durante o período de ocorrência do incidente. Além disso, os prestadores de serviços de pagamento devem considerar se foi, ou é provável que seja, ativado o modo de crise em resultado do impacto do incidente nos serviços relacionados com pagamentos.

vi. *Outros prestadores de serviços de pagamento ou infraestruturas relevantes potencialmente afetados*

Os prestadores de serviços de pagamento devem avaliar o impacto do incidente no mercado financeiro, incluindo as infraestruturas do mercado financeiro e/ou os sistemas de pagamento com cartões que as suportam e os outros prestadores de serviços de pagamento. Em particular, os prestadores de serviços de pagamento devem avaliar se o incidente teve, ou pode vir a ter, repercussões noutros prestadores de serviços de pagamento, se afetou, ou pode vir a afetar, o adequado funcionamento das infraestruturas do mercado financeiro e se comprometeu, ou pode vir a comprometer, o bom funcionamento de todo o sistema financeiro. Os prestadores de serviços de pagamento devem estar atentos a vários fatores, nomeadamente se o componente/*software* afetado é privado ou de acesso generalizado, se a rede comprometida é interna ou externa e se o prestador de serviços de pagamento deixou, ou pode vir a deixar, de cumprir as suas obrigações nas infraestruturas do mercado financeiro às quais pertence.

vii. *Impacto na reputação*

Os prestadores de serviços de pagamento devem considerar o nível de visibilidade que, tanto quanto seja do seu conhecimento, o incidente obteve, ou pode vir a obter, no mercado. Os prestadores de serviços de pagamento devem considerar, nomeadamente, a probabilidade de o incidente poder causar danos à sociedade como um bom indicador para aferição do impacto potencial do incidente na sua reputação. Os prestadores de serviços de pagamento devem ter em consideração i) se o incidente afetou algum processo com visibilidade já foi, ou se poderá ser, alvo de divulgação nos meios de comunicação social (incluindo para além dos meios tradicionais, como os jornais, também os blogues, as redes sociais, etc.), ii) se os requisitos regulamentares foram, ou podem vir, a ser incumpridos, iii) se as sanções foram, ou podem vir a ser, aplicadas ou iv) se o mesmo tipo de incidente já ocorreu anteriormente.

1.4. Os prestadores de serviços de pagamento devem avaliar o incidente, determinando, para cada critério individual, se os limites previstos no Quadro 1 foram, ou é provável que venham a ser, alcançados antes da resolução do incidente.

Quadro 1: Limites

Critérios	Nível de impacto inferior	Nível de impacto superior
Operações afetadas	> 10 % do nível normal de operações do prestador de serviços de pagamento (em termos de número de operações) **e** > 100 000 EUR	> 25 % do nível normal de operações do prestador de serviços de pagamento (em termos de número de operações) **ou** > 5 milhões EUR
Utilizadores de serviços de pagamento afetados	> 5 000 **e** > 10 % dos utilizadores de serviços de pagamento do prestador de serviços de pagamento	> 50 000 **ou** > 25 % dos utilizadores de serviços de pagamento do prestador de serviços de pagamento
Interrupção do serviço	> 2 horas	Não aplicável
Impacto económico	Não aplicável	> Máximo (0,1 % dos fundos próprios de nível 1, 200 000 EUR) **ou** > 5 milhões EUR
Encaminhamento para as instâncias superiores internas	Sim	Sim, e probabilidade de ativação do modo de crise (ou outro equivalente)
Outros prestadores de serviços de pagamento ou infraestruturas relevantes potencialmente afetados	Sim	Não aplicável
Impacto na reputação	Sim	Não aplicável

* Fundos próprios de nível 1, na aceção do artigo 25.º do Regulamento (UE) n.º 575/2013 do Parlamento Europeu e do Conselho, de 26 de junho de 2013, relativo aos requisitos prudenciais para as instituições de crédito e para as empresas de investimento e que altera o Regulamento (UE) n.º 648/2012.

1.5. Os prestadores de serviços de pagamento devem recorrer a estimativas quando não se encontrem disponíveis dados reais para sustentar a sua avaliação sobre se um determinado limite foi, ou é provável que venha a ser, alcançado antes da resolução do incidente (por ex., tal poderá acontecer durante a fase de investigação inicial).

1.6. Os prestadores de serviços de pagamento devem efetuar essa avaliação durante todo o período de ocorrência do incidente, de modo a identificar eventuais alterações de estado do incidente, quer sejam no sentido do seu agravamento (de não severo para severo) ou desagravamento (de severo para não severo).

Orientação 2: Processo de notificação

2.1. Os prestadores de serviços de pagamento devem recolher toda a informação relevante, produzir um relatório de incidentes utilizando para o efeito o modelo de relatório constante do Anexo 1 e submetê-lo à autoridade competente do Estado-Membro de origem. Os prestadores de serviços de pagamento devem preencher o modelo de relatório de acordo com as instruções fornecidas no Anexo 1.

2.2. Os prestadores de serviços de pagamento devem utilizar o mesmo modelo de relatório para informar a autoridade competente durante o período de ocorrência do incidente (i.e., para

os relatórios iniciais, intercalares e finais, conforme descrito nos parágrafos 2.7 a 2.21). Os prestadores de serviços de pagamento devem preencher o modelo de relatório de forma incremental, numa base de melhor esforço, à medida que vão tomando conhecimento de mais informação no decurso das suas investigações internas.

2.3. Caso aplicável, os prestadores de serviços de pagamento devem ainda apresentar à autoridade competente do seu Estado-Membro de origem, uma cópia da informação fornecida (ou a fornecer) aos seus utilizadores, tal como previsto no segundo parágrafo do n.º 1 do artigo 96.º da DSP2, assim que essa informação se encontrar disponível.

2.4. Os prestadores de serviços de pagamento devem fornecer à autoridade competente do Estado-Membro de origem toda e qualquer informação adicional, caso esteja disponível e se considere pertinente para a autoridade competente, juntando a documentação de suporte ao modelo de relatório, sob a forma de um ou vários anexos.

2.5. Os prestadores de serviços de pagamento devem dar seguimento a qualquer pedido, por parte da autoridade competente do Estado-Membro de origem, adicional de informação ou de esclarecimentos sobre a documentação previamente submetida.

2.6. Os prestadores de serviços de pagamento devem garantir, em permanência, a confidencialidade e a integridade da informação trocada com a autoridade competente do Estado-Membro de origem e autenticar-se adequadamente junto da autoridade competente do Estado-Membro de origem.

Relatório inicial

2.7. Os prestadores de serviços de pagamento devem submeter um relatório inicial à autoridade competente do Estado-Membro de origem sempre que detetarem um incidente operacional ou de segurança de caráter severo.

2.8. Os prestadores de serviços de pagamento devem enviar o relatório inicial à autoridade competente no espaço de 4 horas após a deteção do incidente operacional ou de segurança de caráter severo, ou, no caso de os canais de comunicação da autoridade competente não se encontrarem disponíveis ou operacionais nesse momento, assim que se encontrem novamente disponíveis/operacionais.

2.9. Os prestadores de serviços de pagamento devem ainda submeter um relatório inicial à autoridade competente do Estado-Membro de origem, sempre que um incidente de caráter não severo se transforme num incidente de caráter severo. Neste caso específico, os prestadores de serviços de pagamento devem enviar o relatório inicial à autoridade competente imediatamente após a deteção da alteração de estado, ou, no caso de os canais de comunicação da autoridade competente não se encontrarem disponíveis ou operacionais nesse momento, assim que se encontrem novamente disponíveis/operacionais.

2.10. Os prestadores de serviços de pagamento devem incluir, nos seus relatórios iniciais, informação de caráter geral (secção A do modelo de relatório), descrevendo algumas das características essenciais do incidente e as suas prováveis consequências com base na informação imediatamente disponível após a sua deteção ou reclassificação. Os prestadores de serviços de pagamento devem recorrer a estimativas sempre que não se encontrem disponíveis dados reais. Os prestadores de serviços de pagamento devem também incluir, nos seus relatórios iniciais, a data da próxima atualização, que deverá ocorrer assim que possível e, em circunstância alguma, exceder os 3 dias úteis.

Relatório intercalar

2.11. Os prestadores de serviços de pagamento devem submeter relatórios intercalares cada vez que considerem existir uma atualização de estado relevante e, no mínimo, na data da atualização prevista no relatório anterior (independentemente de se tratar de um relatório inicial ou intercalar).

2.12. Os prestadores de serviços de pagamento devem submeter à autoridade competente um primeiro relatório intercalar com uma descrição mais detalhada do incidente e suas consequências (secção B do modelo de relatório). Adicionalmente, os prestadores de serviços de pagamento devem produzir relatórios intercalares adicionais de forma a atualizar a informação já fornecida nas secções A e B do modelo de relatório, pelo menos sempre que tenham conhecimento de informação nova relevante ou alterações significativas desde a anterior notificação (por ex., quer quando o incidente se agrava ou desagrava, quer quando são identificadas novas causas ou tomadas novas medidas de ação para resolver o problema). Não obstante, os prestadores de serviços de pagamento devem elaborar um relatório intercalar sempre que tal lhes seja solicitado pela autoridade competente do Estado-Membro de origem.

2.13. À semelhança do definido para os relatórios iniciais, sempre que não se encontrem disponíveis dados reais, os prestadores de serviços de pagamento devem recorrer a estimativas.

2.14. Os prestadores de serviços de pagamento devem também incluir, em todos os relatórios intercalares, a data da próxima atualização, que deverá ocorrer assim que possível e, em circunstância alguma, exceder os 3 dias úteis. Se o prestador de serviços de pagamento não for capaz de cumprir a data prevista para a próxima atualização, deve contactar a autoridade competente para explicar os motivos do atraso, propor um novo prazo de entrega plausível (não mais do que 3 dias úteis) e enviar um novo relatório intercalar atualizando exclusivamente a informação relativa à data prevista para a próxima atualização.

2.15. Os prestadores de serviços de pagamento devem enviar o último relatório intercalar assim que as atividades correntes forem retomadas e a atividade comercial regresse à normalidade, informando a autoridade competente deste facto. Os prestadores de serviços de pagamento devem considerar que a atividade comercial regressou à normalidade quando as atividades/operações forem repostas para os níveis de serviço/condições definidos pelo

prestador de serviços de pagamento, ou estipulados por entidade externa através de um Acordo de Nível de Serviço (SLA), no que diz respeito a prazos de processamento, capacidade, requisitos de segurança, entre outras e quando deixarem de se aplicar as medidas de contingência.

2.16. No caso da atividade comercial regressar à normalidade num espaço de tempo inferior a 4 horas a contar da deteção do incidente, os prestadores de serviços de pagamento devem procurar submeter simultaneamente o relatório inicial e o último intercalar (preenchendo as secções A e B do modelo de relatório) dentro do prazo de 4 horas.

Relatório final

2.17. Os prestadores de serviços de pagamento devem enviar um relatório final quando efetuada a análise da causa do problema (independentemente de já terem sido implementadas medidas de mitigação ou de ter sido identificada a derradeira causa do problema) e se encontrarem disponíveis dados reais para substituir quaisquer estimativas.

2.18. Os prestadores de serviços de pagamento devem entregar o relatório final à autoridade competente no prazo máximo de 2 semanas após o regresso à normalidade. Os prestadores de serviços de pagamento que necessitem de uma prorrogação do prazo (por ex., por ainda não se encontrarem disponíveis os valores reais sobre o impacto) devem contactar a autoridade competente antes de findo o prazo e fornecer uma justificação adequada para o atraso, bem como uma nova estimativa da data de entrega do relatório final.

2.19. No caso de os prestadores de serviços de pagamento conseguirem fornecer toda a informação solicitada no relatório final (secção C do modelo de relatório) no prazo de 4 horas após a deteção do incidente, devem procurar submeter, no seu relatório inicial, a informação relacionada com os relatórios inicial, último intercalar e final.

2.20. Os prestadores de serviços de pagamento devem procurar incluir nos seus relatórios finais toda a informação disponível, nomeadamente i) os valores reais do impacto em vez de estimativas (bem como qualquer outra atualização necessária nas secções A e B do modelo de relatório) e ii) a secção C do modelo de relatório, que inclui a causa do problema, se já for do conhecimento, e uma síntese das medidas adotadas ou previstas adotar para resolver o problema e evitar a sua recorrência no futuro.

2.21. Os prestadores de serviços de pagamento devem ainda enviar um relatório final quando, em resultado de uma avaliação contínua do incidente, concluírem que um incidente anteriormente comunicado já não preenche os critérios para ser considerado severo nem é expectável que os preencha antes da resolução do incidente. Neste caso, os prestadores de serviços de pagamento devem enviar o relatório final assim que esta situação for detetada e, em todo o caso, na data prevista para o próximo relatório. Nesta situação em particular, em vez de preencher a secção C do modelo de relatório, os prestadores de serviços de pagamento devem selecionar a caixa «incidente reclassificado como não severo» e explicar os motivos que justificam o seu desagravamento.

Orientação 3: Delegação e consolidação de comunicação

3.1. Sempre que tal seja autorizado pela autoridade competente, os prestadores de serviços de pagamento que pretendam delegar as suas obrigações de comunicação ao abrigo da DSP2 a um terceiro devem informar a autoridade competente do Estado-Membro de origem e assegurar o preenchimento das seguintes condições:

a. O contrato formal ou, quando aplicável, os acordos internos celebrados no âmbito de um grupo, subjacentes à delegação das obrigações de comunicação entre o prestador de serviços de pagamento e um terceiro definem de forma inequívoca as responsabilidades atribuídas a cada uma das partes. Em particular, devem referir claramente que, independentemente da possível delegação das obrigações de comunicação, o prestador de serviços de pagamento afetado continua a ser inteiramente responsável pelo cumprimento dos requisitos definidos no artigo 96.º da DSP2, assim como pelo conteúdo da informação fornecida à autoridade competente do Estado-Membro de origem.

b. A delegação da obrigação de comunicação deve cumprir os requisitos de externalização de funções operacionais importantes, conforme estabelecido

   i. no n.º 6 do artigo 19.º da DSP2 relativamente às instituições de pagamento e às instituições de moeda eletrónica, aplicável *mutatis mutandis* em conformidade com o artigo 3.º da Diretiva 2009/110/CE (Diretiva da Moeda Eletrónica); ou

   ii. nas Orientações do Comité Europeu de Supervisão Bancária (CESB) sobre a externalização em relação a instituições de crédito.

c. A informação deve ser previamente submetida à autoridade competente do Estado-Membro de origem e, em todo o caso, cumprindo todos os prazos e procedimentos estabelecidos pela autoridade competente, sempre que aplicável.

d. A confidencialidade de dados sensíveis e a qualidade, consistência, integridade e fiabilidade da informação a fornecer à autoridade competente é adequadamente garantida.

3.2. Os prestadores de serviços de pagamento que desejem permitir que um terceiro designado cumpra as suas obrigações de comunicação de uma forma consolidada (nomeadamente através da apresentação de um único relatório referente a vários prestadores de serviços de pagamento afetados pelo mesmo incidente operacional ou de segurança de caráter severo) devem informar a autoridade competente do Estado-Membro de origem, incluir a informação de contacto referente ao «PSP afetado» no modelo de relatório e assegurar que as seguintes condições são preenchidas:

a. Incluir esta disposição no contrato subjacente à delegação das obrigações de comunicação.

b. Condicionar a comunicação de forma consolidada ao facto de o incidente ter sido causado por uma perturbação dos serviços prestados por um terceiro.

c. Limitar a comunicação de forma consolidada aos prestadores de serviços de pagamento estabelecidos no mesmo Estado-Membro.

d. Garantir que o terceiro avalia a materialidade do incidente relativamente a cada prestador de serviços de pagamento afetado e inclui no relatório consolidado apenas os prestadores para quem o incidente seja considerado de caráter severo. Em caso de dúvida, garantir que o prestador de serviços de pagamento é incluído no relatório consolidado sempre que não existam evidências de que não deva ser incluído.

e. Garantir que, sempre que existam campos no modelo de relatório em que não seja possível fornecer uma resposta comum (por ex., secções B 2, B 4 ou C 3), o terceiro procede i) ou ao preenchimento individual para cada prestador de serviços de pagamento afetado, identificando especificamente cada prestador a que a informação diz respeito, ii) ou à utilização de intervalos, nos campos que permitam essa opção, representando os valores mínimos e máximos observados ou estimados dos diversos prestadores de serviços de pagamento.

f. Os prestadores de serviços de pagamento devem assegurar-se de que o terceiro os mantém permanentemente a par de toda a informação relevante relativa ao incidente e de todas as interações que a mesma possa ter com a autoridade competente, bem como do teor de tais interações, mas apenas na medida em que tal não implique uma quebra de confidencialidade relativamente a informação relacionada com outros prestadores de serviços de pagamento.

3.3. Os prestadores de serviços de pagamento não devem delegar as suas obrigações de comunicação antes de informarem a autoridade competente do Estado-Membro de origem ou depois de terem sido informados de que o contrato de externalização não preenche os requisitos estabelecidos na alínea b) da Orientação 3.1.

3.4. Os prestadores de serviços de pagamento que pretendam cancelar a delegação das suas obrigações de comunicação devem comunicar a sua decisão à autoridade competente do Estado-Membro de origem, em conformidade com os prazos e procedimentos estabelecidos por esta última. Os prestadores de serviços de pagamento devem ainda informar a autoridade competente do Estado-Membro de origem sobre qualquer acontecimento relevante que afete o terceiro designado e a sua capacidade de cumprir com as obrigações de comunicação.

3.5. Os prestadores de serviços de pagamento devem cumprir as suas obrigações de comunicação sem qualquer recurso a apoio externo sempre que o terceiro designado falhe o dever de informar a autoridade competente do Estado-Membro de origem sobre um incidente operacional ou de segurança de caráter severo, em conformidade com o artigo 96.º da DSP2 e com as presentes Orientações. Os prestadores de serviços de pagamento devem ainda certificar-se de que um incidente não é comunicado duas vezes, individualmente pelo respetivo prestador de serviços de pagamento e também pelo terceiro.

Orientação 4: Política operacional e de segurança

4.1. Os prestadores de serviços de pagamento devem certificar-se de que as suas políticas operacionais e de segurança gerais definem claramente todas as responsabilidades relativas à comunicação de incidentes ao abrigo da DSP2, bem como os processos implementados para o cumprimento dos requisitos estabelecidos nas presentes Orientações.

5. Orientações dirigidas às autoridades competentes sobre os critérios de avaliação da relevância do incidente e sobre os pormenores dos relatórios de incidente a partilhar com outras autoridades nacionais

Orientação 5: Avaliação da relevância do incidente

5.1. As autoridades competentes do Estado-Membro de origem devem avaliar a relevância do incidente operacional ou de segurança de caráter severo para outras autoridades nacionais, baseando-se no seu próprio parecer especializado e utilizando os critérios a seguir enunciados como principais indicadores da importância do referido incidente:

a. As causas do incidente enquadram-se na área de competência de outra autoridade nacional.
b. As consequências do incidente têm impacto nos objetivos de outra autoridade nacional (por ex., na salvaguarda da estabilidade financeira).
c. O incidente afeta, ou pode afetar, os utilizadores de serviços de pagamento em larga escala.
d. O incidente foi, ou é provável que venha a ser, amplamente divulgado nos meios de comunicação social.

5.2. As autoridades competentes do Estado-Membro de origem devem realizar estas avaliações, numa base contínua, durante todo o período de ocorrência do incidente, tendo em vista a deteção de quaisquer alterações que possam transformar um incidente anteriormente não considerado como tal num incidente relevante.

Orientação 6: Informação a partilhar

6.1. Sem prejuízo de qualquer outra disposição legal relativa à partilha de informação sobre incidentes com outras autoridades nacionais, as autoridades competentes devem fornecer informação sobre os incidentes operacionais ou de segurança de caráter severo às autoridades nacionais identificadas na sequência da aplicação da Orientação 5.1 (nomeadamente, outras autoridades nacionais relevantes), no mínimo, no momento da receção do relatório inicial (ou, em alternativa, do relatório que despoletou a partilha da informação) e quando forem notificadas de que a atividade comercial regressou à normalidade (i.e. último relatório intercalar).

6.2. As autoridades competentes devem submeter a outras autoridades nacionais relevantes toda a informação necessária que lhes permita obter uma visão clara dos acontecimentos e das potenciais consequências. Para tal, devem fornecer, no mínimo, a informação preenchida pelo prestador de serviços de pagamento nos campos do modelo de relatório a seguir indicados (independentemente de se tratar de um relatório inicial ou intercalar):

- data e hora de deteção do incidente;
- data e hora de início do incidente;
- data e hora da resolução efetiva ou prevista do incidente;
- breve descrição do incidente (incluindo informação não sensível da descrição pormenorizada);
- breve descrição das medidas efetivamente tomadas ou previstas para repor as condições existentes antes do incidente;
- descrição de como o incidente pode afetar outros prestadores de serviços de pagamento e/ou infraestruturas;
- descrição da divulgação efetuada pelos meios de comunicação social (se for o caso);
- causa do incidente.

6.3. As autoridades competentes devem proceder a uma adequada anonimização, na medida do necessário, e omitir qualquer informação que possa estar sujeita a restrições de confidencialidade ou de propriedade intelectual, antes de partilhar qualquer informação relacionada com o incidente com outras autoridades nacionais relevantes. Não obstante, as autoridades competentes devem fornecer às autoridades nacionais relevantes o nome e a morada do prestador de serviços de pagamento que efetuou a comunicação, sempre que as referidas autoridades nacionais possam garantir a confidencialidade da informação fornecida.

6.4. As autoridades competentes devem, a todo o momento, garantir a confidencialidade e a integridade da informação armazenada e trocada com outras autoridades nacionais relevantes, bem como autenticar-se adequadamente junto de outras autoridades nacionais relevantes. Em particular, as autoridades competentes devem tratar toda a informação recebida ao abrigo das presentes Orientações de acordo com as obrigações de sigilo profissional previstas na DSP2, sem prejuízo da legislação aplicável a nível Europeu e da legislação ou regulamentação nacional.

6. Orientações dirigidas às autoridades competentes sobre os critérios de avaliação da relevância dos pormenores dos relatórios de incidente a partilhar com a EBA e o BCE e sobre o formato e os procedimentos de comunicação dos mesmos

Orientação 7: Informação a partilhar

7.1. As autoridades competentes devem sempre fornecer à EBA e ao BCE todos os relatórios recebidos dos (ou em nome dos) prestadores de serviços de pagamento afetados por um incidente operacional ou de segurança de caráter severo (i.e. relatórios iniciais, intercalares e finais).

Orientação 8: Comunicação

8.1. As autoridades competentes devem, a todo o momento, garantir a confidencialidade e a integridade da informação armazenada e trocada com a EBA e com o BCE, e ainda autenticar-se adequadamente junto destas instituições. Em particular, as autoridades competentes devem tratar toda a informação recebida ao abrigo das presentes orientações de acordo com as obrigações de sigilo profissional previstas na DSP2, sem prejuízo da legislação aplicável a nível Europeu e da regulamentação nacional.

8.2. Para evitar atrasos na transmissão à EBA ou ao BCE da informação relativa a incidentes e ajudar a minimizar os riscos de perturbação operacional, as autoridades competentes devem dispor de adequados meios de comunicação.

Anexo 1 – Modelos de relatório para prestadores de serviços de pagamento

CLASSIFICATION: RESTRICTED

Major Incident Report

☐ Initial report	within 4 hours after detection
☐ Intermediate report	maximum of 3 business days from previous report
☐ Last intermediate report	
☐ Final report	within 2 weeks after closing the incident
☐ Incident reclassified as non-major — Please explain:	

Report date	DD/MM/YYYY	Time	HH:MM
Incident identification number, if applicable (for interim and final reports)			

A - Initial report

A 1 - GENERAL DETAILS

Type of report					
Type of report	☐ Individual	☐ Consolidated			
Affected payment service provider (PSP)					
PSP name					
PSP unique identification number, if relevant					
PSP authorisation number					
Head of group, if applicable					
Home country					
Country/countries affected by the incident					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	
Reporting entity (complete this section if the reporting entity is not the affected PSP in case of delegated reporting)					
Name of the reporting entity					
Unique identification number, if relevant					
Authorisation number, if applicable					
Primary contact person		Email		Telephone	
Secondary contact person		Email		Telephone	

A 2 - INCIDENT DETECTION and INITIAL CLASSIFICATION

Date and time of detection of the incident	DD/MM/YYYY, HH:MM		
The incident was detected by (1)		If Other, please explain:	
Please provide a short and general description of the incident (should you deem the incident to have an impact in other EU Member States(s), and if feasible within the applicable reporting deadlines, please provide a translation in English)			
What is the estimated time for the next update?	DD/MM/YYYY, HH:MM		

B - Intermediate report

B 1 - GENERAL DETAILS

Please provide a more DETAILED description of the incident. e.g. information on: - What is the specific issue? - How it happened - How did it develop - Was it related to a previous incident? - Consequences (in particular for payment service users) - Background of the incident detection - Areas affected - Actions taken so far - Service providers/ third party affected or involved - Crisis management started (internal and/or external (Central Bank Crisis management)) - PSP internal classification of the incident	
Date and time of beginning of the incident (if already identified)	DD/MM/YYYY, HH:MM
Incident status	☐ Diagnostics ☐ Recovery ☐ Repair ☐ Restoration
Date and time when the incident was restored or is expected to be restored	DD/MM/YYYY, HH:MM

B 2 - INCIDENT CLASSIFICATION & INFORMATION ON THE INCIDENT

Overall impact	☐ Integrity ☐ Confidentiality ☐ Continuity ☐ Availability ☐ Authenticity
Transactions affected [2]	Number of transactions affected — ☐ Actual figure ☐ Estimation As a % of regular number of transactions — ☐ Actual figure ☐ Estimation Value of transactions affected in EUR — ☐ Actual figure ☐ Estimation Comments:
Payment service users affected [3]	Number of payment service users affected — ☐ Actual figure ☐ Estimation As a %-of total payment service users — ☐ Actual figure ☐ Estimation
Service downtime[4]	Total service downtime: DD:HH:MM — ☐ Actual figure ☐ Estimation
Economic impact [5]	Direct costs in EUR — ☐ Actual figure ☐ Estimation Indirect costs in EUR — ☐ Actual figure ☐ Estimation
High level of internal escalation	☐ YES ☐ YES, AND CRISIS MODE (OR EQUIVALENT) IS LIKELY TO BE CALLED UPON ☐ NO Describe the level of internal escalation of the incident, indicating if it has triggered or is likely to trigger a crisis mode (or equivalent) and if so, please describe
Other PSPs or relevant infrastructures potentially affected	☐ YES ☐ NO Describe how this incident could affect other PSPs and/or infrastructures
Reputational impact	☐ YES ☐ NO Describe how the incident could affect the reputation of the PSP (e.g. media coverage, potential legal or regulatory infringement, etc.)

B 3 - INCIDENT DESCRIPTION

Type of Incident	☐ Operational ☐ Security
Cause of incident	☐ Under investigation ☐ External attack ☐ Internal attack Type of attack: ☐ Distributed/Denial of Service (D/DoS) ☐ Infection of internal systems ☐ Targeted intrusion ☐ Other If Other, specify ☐ External events ☐ Human error ☐ Process failure ☐ System failure ☐ Other If Other, specify
Was the incident affecting you directly, or indirectly through a service provider?	☐ Directly ☐ Indirectly If indirectly, please provide the service provider's name

B 4 - INCIDENT IMPACT

Building(s) affected (Address), if applicable	
Commercial channels affected	☐ Branches ☐ Telephone banking ☐ Point of sale ☐ E-banking ☐ Mobile banking ☐ Other ☐ ATMs If Other, specify:
Payment services affected	☐ Cash placement on a payment account ☐ Credit transfers ☐ Money remittance ☐ Cash withdrawal from a payment account ☐ Direct debits ☐ Payment initiation services ☐ Operations required for operating a payment account ☐ Card payments ☐ Account information services ☐ Acquiring of payment instruments ☐ Issuing of payment instruments ☐ Other If Other, specify:
Functional areas affected	☐ Authentication/authorisation ☐ Clearing ☐ Indirect settlement ☐ Communication ☐ Direct settlement ☐ Other If Other, specify:
Systems and components affected	☐ Application/software ☐ Hardware ☐ Database ☐ Network/infrastructure ☐ Other If Other, specify:
Staff affected	☐ YES ☐ NO Describe how the incident could affect the staff of the PSP/service provider (e.g. staff not being able to reach the office to support customers, etc.)

B 5 - INCIDENT MITIGATION

Which actions/measures have been taken so far or are planned to recover from the incident?	
Has the Business Continuity Plan and/or Disaster Recovery Plan been activated? If so, when? If so, please describe	☐ YES ☐ NO DD/MM/YYYY, HH:MM
Has the PSP cancelled or weakened some controls because of the incident? If so, please explain	☐ YES ☐ NO

C - Final report	
If no intermediate report has been sent, please also complete section B	
C 1 - GENERAL DETAILS	
Please update the information from the intermediate report (summary): - additional actions/measures taken to recover from the incident - final remediation actions taken - root cause analysis - lessons learnt - addittional actions - any other relevant information	
Date and time of closing the incident	DD/MM/YYYY, HH:MM
If the PSP had to cancel or weaken some controls because of the incident, are the original controls back in place?	☐ YES ☐ NO
If so, please explain	
C 2 - ROOT CAUSE ANALYSIS AND FOLLOW-UP	
What was the root cause (if already known)? (possible to attach a file with detailed information)	
Main corrective actions/measures taken or planned to prevent the incident from happening again in the future, if already known	
C 3 - ADDITIONAL INFORMATION	
Has the incident been shared with other PSPs for information purposes?	☐ YES ☐ NO
If so, please provide details	
Has any legal action been taken against the PSP?	☐ YES ☐ NO
If so, please provide details	

Notes:

(1) Pull-down menu: payment service user; internal organisation; external organisation; none of the above

(2) Pull-down menu: > 10% of regular level of transactions and > EUR 100,000; > 25% of regular level of transactions or > EUR 5 milion; none of the above

(3) Pull-down menu: > 5,000 and > 10% payment service users; > 50,000 or > 25% payment service users; none of the above

(4) Pull-down menu: > 2 hours; < 2 hours

(5) Pull-down menu: > Max (0,1% Tier 1 capital, EUR 200,000) or > EUR 5 million; none of the above

CONSOLIDATED REPORT - LIST OF PSPs		
PSP Name	**PSP Unique Identification Number**	**PSP Authorisation number**

INSTRUÇÕES PARA O PREENCHIMENTO DOS MODELOS DE RELATÒRIO

Os prestadores de serviços de pagamento (PSPs) devem preencher a secção relevante do modelo de relatório, dependendo da fase de comunicação em que se encontram: secção A (relatório inicial), secção B (relatórios intercalares) ou secção C (relatório final). Todos os campos são de preenchimento obrigatório, salvo indicação em contrário.

Cabeçalho

Relatório inicial: primeira notificação que o PSP submete à autoridade do Estado-Membro de origem.
Relatório intercalar: atualização de um relatório anterior (inicial ou intercalar) sobre o mesmo incidente.
Último relatório intercalar: este relatório informa a autoridade competente do Estado-Membro de origem que as atividades correntes foram retomadas e que a atividade comercial regressou à normalidade, não sendo submetidos mais relatórios intercalares.
Relatório final: último relatório que o PSP irá envia sobre o incidente, tendo em conta que i) já foi efetuada uma análise da causa do problema e as estimativas podem ser substituídas por valores reais ou que ii) o incidente já não é considerado severo.
Incidente reclassificado como não severo: o incidente já não preenche os critérios para ser considerado de caráter severo e não é expectável que os preencha antes da sua resolução. Nesta situação, os PSPs devem explicar os motivos do desagravamento.
Data e hora do relatório: data e hora exatas da submissão do relatório à autoridade competente.
Número de identificação do incidente, se aplicável (para os relatórios intercalares e final): número de referência atribuído pela autoridade competente na altura da submissão do relatório inicial, com vista a identificar inequivocamente o incidente, se aplicável (i.e. se a autoridade competente atribuir tal referência).

A – Relatório inicial

A 1 – Disposições gerais

Tipo de relatório:

Individual: o relatório refere-se a um único PSP.
Consolidado: o relatório é referente aos vários PSPs que fazem uso da opção de comunicação de forma consolidada. Os campos relativos a «PSP afetado» devem ser deixados em branco (à exceção do campo «País/países afetado(s) pelo incidente») e deve ser fornecida uma lista dos PSP incluídos no relatório através do preenchimento da tabela correspondente (Relatório consolidado – Lista de PSPs).

PSP afetado: refere-se ao PSP que está a experienciar o incidente.

Nome do PSP: nome completo do PSP sujeito ao procedimento de comunicação, conforme indicado no registo oficial nacional aplicável ao PSP.
Número de identificação único do PSP, se relevante: número de identificação único utilizado em cada Estado-Membro para identificar o PSP, o qual deve ser fornecido pelo PSP se o campo «número de autorização do PSP» não se encontrar preenchido.
Número de autorização do PSP: número de autorização atribuído pelo Estado-Membro de origem.
Responsável do grupo: indicar o nome da entidade responsável no caso de se tratar de um grupo de entidades conforme definido no n.º 40 do artigo 4.º da Diretiva (UE) 2015/2366 do Parlamento Europeu e do Conselho, de 25 de novembro de 2015, relativa aos serviços de pagamento no mercado interno (DSP2), que altera as Diretivas (UE)

2002/65/CE, 2009/110/CE e 2013/36/UE e o Regulamento (UE) n.º 1093/2010, e que revoga a Diretiva 2007/64/CE.

Estado-membro de origem: Estado-Membro em que a sede estatutária do PSP está situada; ou, no caso do PSP não ter, nos termos do direito nacional, uma sede estatutária, o Estado-Membro em que a sua sede está situada.

País/países afetado(s) pelo incidente: país ou países onde o impacto do incidente se materializou (por ex., várias sucursais de um PSP localizadas em diferentes países). O país/países afetado(s) pode(m) ou não ser o(s) mesmo(s) que o Estado-Membro de origem.

Primeira pessoa de contacto: nome e apelido da pessoa responsável pela comunicação do incidente ou, no caso de um terceiro efetuar a comunicação em nome do PSP afetado, o nome e apelido da pessoa responsável pela gestão de incidentes/departamento de risco ou outra área equivalente do PSP afetado.

E-mail: endereço eletrónico para envio de pedidos de esclarecimentos adicionais, quando necessário, o qual pode ser um endereço pessoal ou empresarial.

Telefone: número de telefone para solicitação de pedidos de esclarecimentos adicionais, quando necessário, o qual pode ser um número pessoal ou empresarial.

Segunda pessoa de contacto: nome e apelido de uma pessoa alternativa que possa ser contactada pela autoridade competente para obter informação sobre um incidente quando a primeira pessoa de contacto não se encontrar disponível. No caso de um terceiro comunicar em nome do PSP afetado, o nome e o apelido de uma pessoa alternativa responsável pela gestão de incidentes/departamento de risco ou outra área equivalente do PSP afetado.

E-mail: endereço eletrónico da pessoa de contacto alternativa para envio de pedidos de esclarecimentos adicionais, quando necessário, o qual pode ser um endereço pessoal ou empresarial.

Telefone: número de telefone da pessoa de contacto alternativa para solicitação de pedidos de esclarecimentos adicionais, quando necessário, o qual pode ser um número pessoal ou empresarial.

Entidade responsável pela comunicação: esta secção deve ser preenchida no caso de um terceiro cumprir as obrigações de comunicação em nome do PSP afetado.

Nome da entidade responsável pela comunicação: nome completo da entidade que comunica o incidente, tal como indicado no registo comercial nacional aplicável.

Número de identificação único, se relevante: número de identificação único relevante utilizado no país onde se encontra situada o terceiro, destinado a identificar a entidade que comunica o incidente. Esta informação deve ser fornecida pela entidade que comunica caso o campo «Número de autorização» não se encontre preenchido.

Número de autorização, se aplicável: número de autorização do terceiro no país onde se encontra situado, quando aplicável.

Primeira pessoa de contacto: nome e apelido da pessoa responsável pela comunicação do incidente.

E-mail: endereço eletrónico para envio de pedidos de esclarecimentos adicionais, quando necessário, o qual pode ser um endereço pessoal ou empresarial.

Telefone: número de telefone para solicitação de pedidos de esclarecimentos adicionais, quando necessário, o qual pode ser um número pessoal ou empresarial.

Segunda pessoa de contacto: nome e apelido de uma pessoa alternativa, ao serviço da entidade que comunica o incidente, que pode ser contactada pela autoridade competente quando a primeira pessoa de contacto não se encontrar disponível.

E-mail: endereço eletrónico da pessoa de contacto alternativa para envio de pedidos de esclarecimentos adicionais, quando necessário, o qual pode ser um endereço pessoal ou empresarial.

Telefone: número de telefone da pessoa de contacto alternativa para solicitação de pedidos de esclarecimentos adicionais, quando necessário, o qual pode ser um número pessoal ou empresarial.

A 2 – Deteção de incidentes e classificação inicial

Data e hora de deteção do incidente: data e hora em que o incidente foi identificado pela primeira vez.

Incidente detetado por: indicar se o incidente foi detetado por um utilizador do serviço de pagamento, por uma área interna do PSP (por ex., função de auditoria interna) ou por uma entidade externa (por ex., um prestador de serviço externo). Se o incidente não tiver sido detetado por nenhuma destas entidades, fornecer uma explicação no campo correspondente.

Descrição breve e geral do incidente: descrever sucintamente os problemas mais relevantes do incidente, cobrindo as causas possíveis, os efeitos imediatos, etc.

Qual a hora estimada para a próxima atualização?: indicar a data e hora estimadas para a submissão da próxima atualização (relatório intercalar ou final).

B – Relatório intercalar

B 1 – Disposições gerais

Descrição mais pormenorizada do incidente: descrever as principais características do incidente, abrangendo pelo menos os pontos incluídos no questionário (que problema em concreto está o PSP a enfrentar, como começou e como evoluiu, possível ligação a um incidente anterior, consequências, sobretudo para os utilizadores de serviços de pagamento, etc.).

Data e hora de início do incidente: data e hora em que o incidente começou, se for do conhecimento.

Fase do incidente:

Diagnóstico: as características do incidente acabam de ser identificadas.

Reparação: os elementos afetados estão a ser reconfigurados.

Recuperação: os elementos afetados estão a ser restaurados para o último estado de recuperação possível.

Restauração: os serviços relacionados com pagamentos já voltaram a ser prestados.

Data e hora em que o incidente foi restaurado ou em que se prevê que venha a ser restaurado: indicar a data e a hora em que o incidente ficou, ou se espera que venha a ficar, controlado e em que a atividade comercial regressou, ou se espera que regresse, à normalidade.

B 2 – Classificação do incidente/Informação sobre o incidente

Impacto global: indicar as dimensões afetadas pelo incidente. Possibilidade de resposta múltipla.

Integridade: característica que salvaguarda a exatidão e completude dos ativos (incluindo dados).

Disponibilidade: característica que permite o acesso e a utilização dos serviços relacionados com pagamentos pelos utilizadores de serviços de pagamento.

Confidencialidade: característica que inibe o acesso ou a divulgação da informação a indivíduos, entidades ou processos não autorizados.

Autenticidade: característica que confirma a veracidade de uma fonte.

Continuidade: característica necessária aos processos, tarefas e ativos de uma organização para que a prestação de serviços relacionados com pagamentos seja totalmente acessível e executada a um nível aceitável predefinido.

Operações afetadas: Os PSPs devem indicar que limites foram, ou é provável que venham a ser, alcançados pelo incidente, se for o caso, e os valores associados: número de operações afetadas, percentagem de operações afetadas em relação ao número de operações de pagamento executadas pelos serviços de pagamento afetados pelo incidente e o valor total das operações. Os PSPs devem fornecer valores concretos para estas variáveis, os quais podem ser reais ou estimativas. As entidades que comunicam em nome de vários PSPs (i.e. comunicação de forma consolidada) podem fornecer, em alternativa, intervalos de valores representando o mínimo e o máximo observados ou estimados, dentro do grupo de PSPs incluídos no relatório, separados por um hífen. Regra geral, os PSPs devem considerar como «operações afetadas» todas as operações nacionais e transfronteiriças que tenham sido ou possam vir a ser, direta ou indiretamente, afetadas pelo incidente e, nomeadamente, as operações que não tenham sido iniciadas ou processadas, bem como as operações cujo conteúdo da mensagem de pagamento tenha sido alterado e aquelas que tenham sido executadas de forma fraudulenta (independentemente dos fundos afetados terem sido recuperados ou não). Neste contexto, os PSPs devem considerar como nível normal de operações de pagamento a média diária anual das operações de pagamento nacionais e transfronteiriças executadas pelos mesmos serviços de pagamento que foram afetados pelo incidente, considerando o exercício anterior como período de referência para efeitos de cálculo. Se os PSPs não considerarem este número representativo (por ex., devido à sazonalidade), devem utilizar outra medida mais representativa e comunicar à autoridade competente o racional subjacente a essa abordagem no campo «Observações».

Utilizadores de serviços de pagamento afetados: Os PSPs devem indicar que limites foram, ou é provável que venham a ser, alcançados pelo incidente, se for o caso, e os valores associados: número total de utilizadores de serviços de pagamento que foram afetados e percentagem de utilizadores de serviços de pagamento afetados em relação ao número total de utilizadores de serviços de pagamento. Os PSPs devem fornecer valores concretos para estas variáveis, os quais podem ser reais ou estimativas. As entidades que comunicam em nome de vários PSPs (comunicação de forma consolidada) podem fornecer, em alternativa, intervalos de valores representando o mínimo e o máximo observados ou estimados, dentro do grupo de PSPs incluídos no relatório, separados por um hífen. Os PSPs devem considerar como «utilizadores de serviços de pagamento afetados» todos os clientes (nacionais ou estrangeiros, consumidores ou empresas) que possuam um contrato com o prestador de serviços de pagamento afetado que lhes garante o acesso ao referido serviço, e que tenham sofrido, ou possam vir a sofrer, as consequências do incidente. Para determinar o número de utilizadores de serviços de pagamento que possam ter utilizado o serviço durante o período de ocorrência do incidente, os PSPs devem recorrer a estimativas baseadas nos respetivos históricos de atividade. No caso de se tratar de um grupo, cada PSP deve apenas considerar os utilizadores dos seus próprios serviços de pagamento. Se se tratar de um PSP que disponibilize serviços operacionais a terceiros, o mesmo deve considerar apenas os seus utilizadores de serviços de pagamento (se tiver algum). Da mesma forma, os PSPs que usufruem desses serviços operacionais devem avaliar o incidente em relação aos seus próprios utilizadores de serviços de pagamento. Além disso, os PSPs devem considerar, como número total de utilizadores de serviços de pagamento, o número agregado de utilizadores de serviços de pagamento nacionais e transfronteiriços contratualmente vinculados aos mesmos no momento do incidente (ou, em alternativa, o número mais recente disponível) e com acesso ao serviço de pagamento afetado, independentemente da respetiva dimensão ou de serem considerados utilizadores ativos ou passivos dos serviços em causa.

Interrupção do serviço: Os PSPs devem indicar se o limite foi, ou é provável que venha a ser alcançado pelo incidente, bem como o valor associado: tempo total de interrupção do serviço. Os PSPs devem fornecer valores concretos para estas variáveis, os quais podem ser reais ou estimativas. As entidades que comunicam em nome de vários PSPs (i.e. comunicação de forma consolidada) podem fornecer, em alternativa, intervalos de valores representando o mínimo e o máximo observados ou estimados, dentro do grupo de PSP incluídos no relatório, separados por um hífen. Os PSP devem considerar o período de tempo em que qualquer tarefa, processo ou canal associado à prestação de serviços de pagamento está, ou possa vir a estar, interrompido e que impede i) a iniciação e/ou execução de um serviço de pagamento e/ou ii) o acesso a uma conta de pagamento. Os PSPs devem contabilizar o tempo de interrupção do serviço a partir do início da interrupção, considerando quer o período de tempo em que a prestação de serviços de pagamento está disponível ao público, quer as horas de encerramento e os períodos de manutenção, quando relevante e aplicável. Caso os PSPs não consigam determinar a altura em que a interrupção do serviço teve início, devem excecionalmente contabilizar a interrupção a partir do momento da sua deteção.

Impacto económico: Os PSPs devem indicar se o limite foi, ou é provável que venha a ser, alcançado pelo incidente, bem como os valores associados: custos diretos e indiretos. Os PSPs devem fornecer valores concretos para estas variáveis, os quais podem ser reais ou estimativas. As entidades que comunicam em nome de vários PSPs (i.e. comunicação de forma consolidada) podem fornecer, em alternativa, intervalos de valores representando o mínimo e o máximo observados ou estimados, dentro do grupo de PSP incluídos no relatório, separados por um hífen. Os PSPs devem considerar quer os custos diretos, quer os indiretos relacionados com o incidente. Entre outros fatores, os PSPs devem ter em conta os fundos ou ativos expropriados, os custos de substituição de *hardware* ou *software*, outros custos judiciais ou de resolução de conflitos, taxas por incumprimento de obrigações contratuais, sanções, responsabilidades externas e perdas de receitas. No que diz respeito aos custos indiretos, os PSPs devem considerar apenas aqueles que já forem do conhecimento ou os que são muito prováveis de se materializar.

> **Custos diretos:** custo, expresso em euros, diretamente resultante do incidente, incluindo os fundos necessários para retificar o incidente (por ex. fundos ou ativos expropriados, custos de substituição de *hardware* ou *software*, taxas por incumprimento de obrigações contratuais).
>
> **Custos indiretos:** custo, expresso em euros, indiretamente resultante do incidente (por ex. custos de ressarcimento/compensação do cliente, perdas de receitas devido a oportunidades de negócio perdidas, potenciais custos legais).

Encaminhamento para as instâncias superiores internas: Os PSPs devem considerar se, tendo em conta o impacto do incidente nos serviços relacionados com pagamentos, o Diretor Executivo de Informação (ou cargo equivalente) foi, ou será provavelmente, informado do incidente fora do âmbito de qualquer procedimento de notificação periódico e numa base continuada durante o período de ocorrência do incidente. No caso de existir delegação de comunicação, o encaminhamento do processo deve ocorrer ao nível do terceiro. Adicionalmente, os PSPs devem considerar se foi, ou é provável que seja, ativado o modo de crise em resultado do impacto do incidente nos serviços relacionados com pagamentos.

Outros PSPs ou infraestruturas relevantes potencialmente afetados: Os PSPs devem avaliar o impacto do incidente no mercado financeiro, incluindo as infraestruturas do mercado financeiro e/ou os sistemas de pagamento com cartões que as suportam e os outros prestadores de serviços de pagamento. Em particular, os PSPs devem avaliar se o incidente teve, ou pode vir a ter, repercussões noutros PSPs, se afetou, ou pode vir a afetar, o adequado funcionamento das infraestruturas do mercado financeiro e se comprometeu, ou pode vir a comprometer, a solidez

de todo o sistema financeiro. Os PSPs devem estar atentos a vários fatores, nomeadamente se o componente/*software* afetado é privado ou de acesso generalizado, se a rede comprometida é interna ou externa e se o PSP deixou, ou pode vir a deixar, de cumprir as suas obrigações nas infraestruturas do mercado financeiro às quais pertence.

Impacto na reputação: Os PSPs devem considerar o nível de visibilidade que, tanto quanto seja do seu conhecimento, o incidente obteve, ou pode vir a obter, no mercado. Os PSPs devem considerar, nomeadamente, a probabilidade de o incidente poder causar danos à sociedade como um bom indicador para aferição do impacto potencial do incidente na sua reputação. Os PSPs devem ainda ter em consideração i) se o incidente afetou algum processo com visibilidade ou se já foi, ou poderá vir a ser, alvo de divulgação nos meios de comunicação social (incluindo para além dos meios tradicionais, como os jornais, também os blogues, as redes sociais, etc.), ii) se os requisitos regulamentares foram ou podem vir a ser ignorados, iii) as sanções foram ou podem vir a ser aplicadas ou iv) se o mesmo tipo de incidente já ocorreu anteriormente.

B 3 – Descrição do incidente

Tipo de incidente: indicar, quando possível, se representa um incidente operacional ou de segurança.

Operacional: incidente provocado pela inadequação ou falha de processos, por pessoas, sistemas ou eventos de força maior que afetaram a integridade, disponibilidade, confidencialidade, autenticidade e/ou continuidade dos serviços relacionados com pagamentos.

Segurança: ato não autorizado de acesso, utilização, divulgação, perturbação, alteração ou destruição dos ativos do PSP, afetando a integridade, disponibilidade, confidencialidade, autenticidade e/ou continuidade dos serviços relacionados com pagamentos. Esta situação pode acontecer em resultado, por exemplo, de um ataque cibernético ao PSP, de uma conceção ou implementação inadequadas das políticas de segurança ou de uma inadequada segurança física.

Causa do incidente: indicar a causa do incidente ou, se a mesma ainda não for do conhecimento, a causa mais provável. Possibilidade de resposta múltipla.

Sob investigação: a causa ainda não foi determinada.

Ataque externo: a causa tem origem externa, tendo sido intencionalmente dirigida ao PSP (por ex., ataques de *malware*).

Ataque interno: a causa tem origem interna, tendo sido intencionalmente dirigida ao PSP (por ex., fraude interna).

Tipo de ataque:

Distribuído/Negação de Serviço (D/DoS): tentativa de tornar indisponível um serviço em linha através de uma sobrecarga de tráfego com múltiplas origens.

Infeção dos sistemas internos: ato nocivo que ataca os sistemas informáticos para roubar espaço no disco rígido ou tempo de CPU, aceder a informação privada, corromper dados, enviar mensagens de *spam* aos contactos, etc.

Intrusão direcionada: ato não autorizado de espionagem, interceção e roubo de informação através do ciberespaço.

Outro: qualquer outro tipo de ataque que o PSP possa ter sofrido, diretamente ou através de outro prestador de serviço. Esta caixa deve ser selecionada, nomeadamente, se tiver ocorrido um ataque dirigido ao processo de autorização e autenticação. O campo de texto livre deve ser preenchido com informação mais detalhada.

Eventos externos: a causa está associada à ocorrência de eventos geralmente fora do controlo da organização (por ex. desastres naturais, questões legais, questões comerciais e relações de dependência de serviço).

Erro humano: o incidente foi causado pelo erro inadvertido de uma pessoa, tendo afetado parte de um procedimento de pagamento (por ex. errado carregamento dos ficheiros no sistema de pagamentos) ou estando relacionado de alguma forma com o mesmo (por ex. um corte acidental de energia que interrompa a atividade de pagamento).

Falha de processo: a causa do incidente resulta da má conceção ou execução do processo de pagamento, dos controlos do processo e/ou dos processos de suporte (por ex. processo de alteração/migração, testes, configuração, capacidade, monitorização).

Falha de sistema: a causa do incidente está associada à inadequação da conceção, da execução, dos componentes, das especificações, da integração ou da complexidade dos sistemas que suportam a atividade de pagamento.

Outra: nenhuma das causas acima indicadas está na origem do incidente. O campo de texto livre deve ser preenchido com informação mais detalhada.

O incidente afetou o PSP diretamente ou indiretamente através de um prestador de serviços?: um incidente pode atingir um PSP diretamente ou indiretamente através de um terceiro. Em caso de impacto indireto, indicar o(s) nome(s) do(s) prestador(es) de serviços.

B 4 – Impacto do incidente

Edifício(s) afetado(s) (morada), se aplicável: se um edifício fisico tiver sido afetado, indicar a morada do mesmo.

Canais comerciais afetados: indicar o canal ou os canais de interação com os utilizadores de serviços de pagamento que foram afetados pelo incidente. Possibilidade de resposta múltipla.

Sucursal: um estabelecimento distinto da sede social que faz parte de um PSP, desprovido de personalidade jurídica e que executa diretamente algumas ou a totalidade das operações inerentes à atividade de um PSP. Os estabelecimentos de um PSP com sede num Estado-Membro, situados noutro Estado-Membro, são considerados como uma única sucursal.

Banca eletrónica: utilização de computadores para executar operações financeiras através da internet.

Banca telefónica: utilização de telefones para executar operações financeiras.

Serviço bancário móvel: utilização de uma aplicação bancária específica num *smartphone* ou dispositivo similar para executar operações financeiras.

ATMs: dispositivos eletromecânicos que permitem aos utilizadores de serviços de pagamento levantar numerário das suas contas e/ou aceder a outros serviços.

Ponto de venda: instalação física do comerciante onde é iniciada a operação de pagamento.

Outro: o canal comercial afetado não é nenhum dos acima referidos. O campo de texto livre deve ser preenchido com informação mais detalhada.

Serviços de pagamento afetados: indicar os serviços de pagamento que não estão a funcionar corretamente devido ao incidente. Possibilidade de resposta múltipla.

Depósito de numerário numa conta de pagamento: entrega de numerário a um PSP para crédito numa conta de pagamento.

Levantamento de numerário de uma conta de pagamento: pedido recebido por um PSP de um dos seus utilizadores de serviços de pagamento para disponibilização de numerário e débito da sua conta de pagamento pelo mesmo montante.

Operações necessárias para a gestão de uma conta de pagamento: ações necessárias para ativar, desativar e/ou manter uma conta de pagamento (por ex., abertura, bloqueio).

Aceitação de operações de pagamento: serviço de pagamento prestado por um PSP vinculado por contrato a um beneficiário para aceitar e processar operações de pagamento que resultam numa transferência de fundos para o beneficiário.

Transferências a crédito: serviço de pagamento prestado pelo prestador de serviços de pagamento que detém a conta de pagamento do ordenante que consiste em creditar, com base em instruções deste, a conta de pagamento de um beneficiário no montante correspondente a uma operação de pagamento ou uma série de operações de pagamento a partir da conta de pagamento do ordenante.

Débitos direto: serviço de pagamento que consiste em debitar a conta de pagamento de um ordenante, sendo a operação de pagamento iniciada pelo beneficiário com base no consentimento dado pelo ordenante ao beneficiário, ao prestador de serviços de pagamento do beneficiário ou ao prestador de serviços de pagamento do próprio ordenante.

Pagamentos com cartão: serviço de pagamento baseado numa infraestrutura de sistemas de pagamento com cartão e sujeito a regras comerciais que permitem a realização de operações de pagamento por meio de qualquer cartão, telecomunicação, dispositivo digital ou informático, ou *software*, se tal resultar numa operação baseada em cartão de débito ou crédito. As operações de pagamento baseadas em cartão excluem as operações baseadas noutros tipos de serviços de pagamento.

Emissão de instrumentos de pagamento: serviço de pagamento prestado por um PSP vinculado por contrato para fornecer um instrumento de pagamento a um ordenante a fim de iniciar e processar as operações de pagamento do ordenante.

Envio de fundos: serviço de pagamento em que são recebidos fundos de um ordenante, sem que sejam criadas contas de pagamento em nome do ordenante ou do beneficiário, com a finalidade exclusiva de transferir um montante correspondente para um beneficiário ou para outro PSP que atue por conta do beneficiário, e/ou em que esses fundos são recebidos por conta do beneficiário e lhe são disponibilizados.

Serviço de iniciação de pagamento: serviço que inicia uma ordem de pagamento a pedido do utilizador do serviço de pagamento relativamente a uma conta de pagamento detida noutro PSP.

Serviço de informação sobre contas: serviço em linha que consiste em prestar informações consolidadas sobre uma ou mais contas de pagamento tituladas pelo utilizador de serviços de pagamento junto de outro ou outros PSPs.

Outro: o serviço de pagamento afetado não é nenhum dos acima referidos. O campo de texto livre deve ser preenchido com informação mais detalhada.

Áreas funcionais afetadas: indicar a(s) fase(s) do processo de pagamento que foi/foram afetada(s) pelo incidente. Possibilidade de resposta múltipla.

Autenticação: procedimento que permite ao PSP verificar a identidade de um utilizador de serviços de pagamento ou a validade da utilização de um instrumento de pagamento específico, incluindo a utilização das credenciais de segurança personalizadas do utilizador.

Autorização: o consentimento do utilizador do serviço de pagamento (ou de uma entidade terceira agindo em seu nome) para a transferência de fundos ou valores mobiliários.

Comunicação: fluxo de informação para efeitos de identificação, autenticação, notificação e informação entre os PSPs que gerem as contas e os prestadores de serviços de iniciação de pagamento, prestadores de serviços de informação sobre contas, ordenantes, beneficiários e outros PSPs.
Compensação: processo de transmissão, reconciliação e, em certos casos, de confirmação de ordens de transferência antes da liquidação, incluindo potencialmente a compensação de ordens e a definição das posições finais para liquidação.
Liquidação direta: conclusão de uma operação ou do seu processamento, com o objetivo de garantir o cumprimento das obrigações dos participantes através da transferência de fundos, sempre que esta ação seja executada pelo próprio PSP afetado.
Liquidação indireta: conclusão de uma operação ou do seu processamento, com o objetivo de garantir o cumprimento das obrigações dos participantes através da transferência de fundos, sempre que estar ação seja executada por outro PSP em nome do PSP afetado.
Outra: a área funcional afetada não é nenhuma das acima referidas. O campo de texto livre deve ser preenchido com informação mais detalhada.

Sistemas e componentes afetados: indicar que parte(s) da infraestrutura tecnológica do PSP foi/foram afetada(s) pelo incidente. Possibilidade de resposta múltipla.

Aplicação/*software*: programas, sistemas operativos ou outros que suportam a prestação de serviços de pagamento pelo PSP.
Base de dados: estrutura de dados que armazena informação pessoal e de pagamento necessária para executar operações de pagamento.
***Hardware*:** equipamento físico tecnológico que executa processos e/ou armazena os dados necessários pelos PSP para continuarem a desenvolver as suas atividades relacionadas com pagamentos.
Rede/infraestrutura: redes de telecomunicações, públicas ou privadas, que permitem a troca de dados e de informação durante o processo de pagamento (por ex., internet).
Outros: o sistema e o componente afetado não é nenhum dos acima referidos. O campo de texto livre deve ser preenchido com informação mais detalhada.

Pessoal afetado: indicar se o incidente teve ou não algum efeito no pessoal do PSP e, em caso afirmativo, fornecer informação mais detalhada no campo de texto livre.

B 5 – Mitigação do incidente

Que ações/medidas foram tomadas até ao momento ou estão previstas para garantir a recuperação de um incidente?: fornecer informação mais detalhada sobre as medidas tomadas ou previstas para resolver temporariamente o incidente.
Os Planos de Continuidade de Negócio e/ou os Planos de Recuperação de Desastre foram ativados?: indicar sim ou não e, caso afirmativo, fornecer os detalhes mais relevantes sobre a situação (i.e., quando foram ativados e em que consistiram esses planos).
O PSP cancelou ou reduziu algum procedimento de controlo devido ao incidente?: indicar se o PSP teve de alterar algum procedimento de controlo (por ex., deixar de utilizar o princípio dos «quatro olhos») para resolver o incidente e, em caso afirmativo, indicar os motivos que estiveram na origem de tal redução ou cancelamento.

C – Relatório final

C 1 – Disposições gerais

Atualização da informação do relatório intercalar (resumo): fornecer informação adicional sobre as medidas tomadas para assegurar a recuperação do incidente e evitar a recorrência do mesmo, análise da causa do problema, lições retiradas, etc.

Data e hora de resolução do incidente: indicar a data e a hora em que o incidente foi considerado fechado.

Foram retomados os procedimentos de controlo originais?: no caso de o PSP ter cancelado ou reduzido algum procedimento de controlo devido ao incidente, indicar se os mesmos já estão ativos e fornecer informação adicional no campo de texto livre.

C 2 – Análise da causa do problema e acompanhamento

Qual a causa do problema, se já for do conhecimento?: explicar o que esteve na origem do problema ou, se tal ainda for desconhecido, referir as conclusões preliminares retiradas da análise da causa do problema efetuada. Os PSPs podem anexar um ficheiro com informação mais detalhada, sempre que o considerem necessário.

Principais ações/medidas corretivas tomadas ou previstas para evitar que o incidente volte a ocorrer no futuro, se já for do conhecimento: descrever as principais medidas tomadas ou previstas para evitar a recorrência do incidente no futuro.

C 3 – Informação adicional

O incidente foi partilhado com outros PSPs para efeitos de informação?: identificar os PSPs que foram contactados, formal ou informalmente, sobre o incidente, fornecendo detalhes sobre os mesmos, sobre a informação partilhada e sobre os motivos que levaram à partilha dessa informação.

O PSP foi alvo de alguma ação legal?: indicar se, no momento do preenchimento do relatório final, o PSP foi alvo de qualquer ação legal (por ex., foi levado a tribunal ou perdeu a sua licença) em resultado do incidente.