EBA/GL/2021/03

10 de junho de 2021

Orientações revistas

sobre a comunicação de incidentes de caráter severo ao abrigo da 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 EBA[1]. Nos termos do artigo 16.º, n.º 3, do Regulamento EBA, 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 EBA, às quais as presentes Orientações se apliquem 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 essas Orientações se destinem maioritariamente a instituições.

Requisitos de notificação

3. Nos termos do artigo 16.°, n.º 3, do Regulamento EBA, as autoridades competentes deverão notificar a EBA sobre se dão ou tencionam dar cumprimento às presentes Orientações ou, caso contrário, indicar as razões para o não cumprimento até (07.11.2021). Na ausência de qualquer notificação até à referida data, a EBA considerará que as autoridades competentes não cumprem as Orientações. As notificações efetuam-se mediante o envio do modelo disponível no sítio Web da EBA com a referência «EBA/GL/2021/03». Estas notificações deverão ser apresentadas por pessoas devidamente autorizadas para comunicar o referido cumprimento em nome das respetivas autoridades competentes. Qualquer alteração no que respeita à situação de cumprimento deverá ser igualmente 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 de 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, conforme previsto no n.º 1 do artigo 96.º da DSP2, 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 DSP2, 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 DSP2.

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 de

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

12. As presentes Orientações aplicam-se igualmente a incidentes de caráter severo que afetem funções subcontratadas por prestadores de serviços de pagamento a terceiros.

Destinatários

13. 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 DSP2 e conforme referido no n.º 1 do artigo 4.º do Regulamento (UE) n.º 1093/2010.

14. O segundo e terceiro conjuntos 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

15. Salvo especificação em contrário, os termos utilizados e definidos na DSP2 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 têm, ou é provável que venham 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 que os serviços relacionados com pagamentos sejam totalmente acessíveis e utilizáveis pelos utilizadores de serviços de pagamento, de acordo com níveis aceitáveis predefinidos pelo prestador 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.
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

16. As presentes Orientações entram em vigor em 1 de janeiro de 2022.

Revogação

17. São revogadas as seguintes Orientações, com efeitos a partir de 1 de janeiro de 2022:

Orientações sobre a comunicação de incidentes de caráter severo, ao abrigo da Diretiva (UE) 2015/2366 (DSP2) (EBA/GL/2017/10)

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 de carácter severo 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. Quebra de segurança na rede ou nos sistemas de informação

Os prestadores de serviços de pagamento devem verificar se alguma ação maliciosa comprometeu a segurança da rede ou dos sistemas de informação relacionados com a prestação de serviços de pagamento.

iv. Interrupção do serviço

Os prestadores de serviços de pagamento devem determinar o período de tempo durante o qual é provável que o serviço se encontre indisponível para os utilizadores de serviços de pagamento ou 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.

v. 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).

vi. Encaminhamento para as instâncias superiores internas

Os prestadores de serviços de pagamento devem determinar se o incidente em causa foi, ou é provável que venha a ser, comunicado aos seus diretores executivos.

vii. 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.

viii. 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 é provável que venham 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 de os fundos terem sido recuperados ou não), ou as operações cuja adequada execução tenha sido impedida ou prejudicada de qualquer outra forma pelo incidente.

No caso de incidentes operacionais que afetem a capacidade de iniciar e/ou processar operações, os prestadores de serviços de pagamento devem comunicar apenas os incidentes com duração superior a uma hora. A duração do incidente deve ser medida desde o momento em que o incidente ocorre até ao momento em que as atividades/operações regulares são recuperadas para o nível de serviço prestado antes do incidente.

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. No caso de 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 reporte (ver anexo).

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 é provável que venham 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. Caso se trate 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.

No caso de incidentes operacionais que afetem a capacidade de iniciar e/ou processar operações, os prestadores de serviços de pagamento devem comunicar apenas os incidentes que afetem os utilizadores de serviços de pagamento com duração superior a uma hora. A duração do incidente deve ser medida desde o momento em que o incidente ocorre até ao momento em que as atividades/operações regulares são recuperadas para o nível de serviço prestado antes do incidente.

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. Quebra de segurança das redes ou dos sistemas de informação

Os prestadores de serviços de pagamento devem verificar se alguma ação maliciosa comprometeu a disponibilidade, a autenticidade, a integridade ou a confidencialidade da

rede ou dos sistemas de informação (incluindo dados) relacionados com a prestação de serviços de pagamento.

iv. Interrupção do serviço

Os prestadores de serviços de pagamento devem considerar o período de tempo em que qualquer tarefa, processo ou canal associado à prestação de serviços de pagamento está, ou é provável que venha 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 o momento em que a interrupção do serviço teve início, devem excecionalmente contabilizar a interrupção a partir do momento da sua deteção.

v. 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.

vi. *Encaminhamento para as instâncias superiores internas*

Os prestadores de serviços de pagamento devem considerar se, em resultado do impacto sobre os serviços relacionados com pagamentos, o órgão de administração, tal como definido nas Orientações da EBA relativas à gestão dos riscos associados às TIC e à segurança, foi, ou é provável que venha a ser, informado, em conformidade com a alínea d) da Orientação 60 das Orientações da EBA relativas à gestão dos riscos associados às TIC e à segurança, sobre o incidente fora do âmbito de qualquer procedimento de notificação periódico e numa base contínua durante o período de ocorrência do incidente. Além disso, os prestadores de serviços de pagamento devem considerar se foi, ou é provável que venha a ser, ativado o modo de crise em resultado do impacto do incidente nos serviços relacionados com pagamentos.

vii. *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 que o suportam e os restantes prestadores de serviços de pagamento. Em particular, os prestadores de serviços de pagamento devem avaliar se o incidente teve, ou é provável que venha a ter, repercussões noutros prestadores de serviços de pagamento, se

afetou, ou é provável que venha a afetar, o adequado funcionamento das infraestruturas do mercado financeiro e se comprometeu, ou é provável que venha 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, ou se a rede comprometida é interna ou externa ou se o prestador de serviços de pagamento deixou, ou é provável que venha a deixar, de cumprir as suas obrigações perante as infraestruturas do mercado financeiro às quais pertence.

viii. *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 é provável que venha 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 os utilizadores de serviços de pagamento e/ou outros prestadores de serviços de pagamento se queixaram do impacto adverso do incidente, (ii) se o incidente afetou algum processo com visibilidade relacionado com os serviços de pagamento, sendo, por conseguinte, provável que receba ou já tenha recebido cobertura mediática (considerando não só os meios de comunicação tradicionais, como os jornais, mas também os blogues, as redes sociais, etc.), (iii) se as obrigações contratuais não foram, ou é provável que não venham a ser, cumpridas, resultando na divulgação de ações judiciais contra o prestador de serviços de pagamento, (iv) se os requisitos regulamentares não foram cumpridos, resultando na imposição de medidas de supervisão ou sanções que foram, ou é provável que venham a ser, divulgadas ao público, e (v) 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** duração do incidente > 1 hora* **ou** > 500 000 EUR **e** duração do incidente > 1 hora*	> 25 % do nível normal de operações do prestador de serviços de pagamento (em termos de número de operações) **ou** > 15 000 000 EUR
Utilizadores de serviços de pagamento afetados	> 5 000 **e**	> 50 000

	duração do incidente > 1 hora* **ou** > 10 % dos utilizadores de serviços de pagamento do prestador de serviços de pagamento **e** duração do incidente > 1 hora*	**ou** > 25 % dos utilizadores de serviços de pagamento do prestador de serviços de pagamento
Interrupção do serviço	> 2 horas	Não aplicável
Quebra de segurança na rede ou nos sistemas de informação	Sim	Não aplicável
Impacto económico	Não aplicável	> Máximo (0,1 % dos fundos próprios de nível 1**, 200 000 EUR) **ou** > 5 000 000 EUR
Encaminhamento para as instâncias superiores internas	Sim	Sim, e é provável que venha a ser ativado o 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

* O limite relativo à duração do incidente por um período superior a uma hora aplica-se apenas a incidentes operacionais que afetem a capacidade do prestador de serviços de pagamento de iniciar e/ou processar operações.

**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 valores 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 numa base contínua 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). Qualquer reclassificação do incidente de severo para não severo deve ser comunicada à autoridade competente, em conformidade com o requisito da Orientação 2.21 e sem demora injustificada.

Orientação 2: Processo de notificação

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

2.2. Os prestadores de serviços de pagamento devem utilizar o mesmo modelo de reporte no momento de submissão dos relatórios inicial, intercalar e final relativos ao mesmo incidente. Os prestadores de serviços de pagamento devem, por conseguinte, preencher um único modelo de reporte de forma incremental e atualizar, quando aplicável, as informações fornecidas nos relatórios anteriores.

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, 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, a pedido da autoridade competente do Estado-Membro de origem, fornecer todo e qualquer documento adicional que complemente as informações apresentadas no modelo de reporte. Os prestadores de serviços de pagamento devem dar seguimento a qualquer pedido adicional, por parte da autoridade competente do Estado-Membro de origem, de informação ou de esclarecimentos sobre a documentação previamente submetida.

2.5. Qualquer informação adicional contida nos documentos fornecidos pelos prestadores de serviços de pagamento à autoridade competente, quer por iniciativa do prestador de serviços de pagamento, quer a pedido da autoridade competente, em conformidade com a Orientação 2.4, deve ser refletida pelo prestador de serviços de pagamento no modelo de reporte referido na Orientação 2.1.

2.6. Os prestadores de serviços de pagamento devem garantir, em permanência, a confidencialidade e a integridade da informação trocada, bem como a sua adequada autenticação 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 um incidente operacional ou de segurança for classificado de caráter severo. As autoridades competentes devem acusar sem demora a receção do relatório inicial e atribuir um código de referência único que identifique inequivocamente o incidente. Os prestadores de serviços de pagamento devem indicar esse código de referência ao submeter uma atualização ao relatório inicial, intercalar e final

relativos ao mesmo incidente, a menos que os relatórios intercalar e final sejam submetidos conjuntamente com o relatório inicial.

2.8. Os prestadores de serviços de pagamento devem enviar o relatório inicial à autoridade competente no prazo de quatro horas a contar do momento em que o incidente operacional ou de segurança foi classificado como de caráter severo. No caso de os canais de comunicação da autoridade competente não estarem disponíveis ou operacionais nesse momento, os prestadores de serviços de pagamento devem enviar o relatório inicial assim que os mesmos se encontrem novamente disponíveis/operacionais.

2.9. Os prestadores de serviços de pagamento devem classificar o incidente em conformidade com as Orientações 1.1 e 1.4, e em tempo oportuno após a deteção do incidente, mas o mais tardar 24 horas após a sua deteção, e sem demora injustificada após a informação necessária para a classificação do incidente estar à disposição do prestador de serviços de pagamento. Caso seja necessário um prazo mais longo para classificar o incidente, os prestadores de serviços de pagamento devem explicar, no relatório inicial submetido à autoridade competente, as razões para o prolongamento do prazo.

2.10. 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 seja reclassificado como 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.

2.11. Os prestadores de serviços de pagamento devem fornecer, no relatório inicial, informação de caráter geral (secção A do modelo de reporte), descrevendo algumas das características essenciais do incidente e as suas prováveis consequências com base na informação imediatamente disponível após a sua classificação como de caráter severo. Os prestadores de serviços de pagamento devem recorrer a estimativas sempre que não se encontrem disponíveis valores reais.

Relatório intercalar

2.12. Os prestadores de serviços de pagamento devem submeter o relatório intercalar assim que as atividades regulares forem recuperadas 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 recuperadas para os mesmos níveis de serviço/condições definidos pelo prestador de serviços de pagamento, ou estipulados por entidade externa através de um acordo de nível de serviço (no que diz respeito a prazos de processamento, capacidade, requisitos de segurança, entre outras) e quando deixarem de se aplicar as

medidas de contingência. O relatório intercalar deve conter uma descrição mais pormenorizada do incidente e das suas consequências (secção B do modelo de reporte).

2.13. Caso as atividades regulares ainda não tiverem sido recuperadas, os prestadores de serviços de pagamento devem submeter um relatório intercalar à autoridade competente no prazo de três dias úteis a contar da submissão do relatório inicial.

2.14. Os prestadores de serviços de pagamento devem atualizar a informação já fornecida nas secções A e B do modelo de reporte sempre que tenham conhecimento de alterações significativas após a submissão do relatório anterior (por ex., quando o incidente sofre um agravamento ou desagravamento, quando são identificadas novas causas ou tomadas novas medidas para resolver o problema). Incluem-se nesta situação i os casos em que o incidente não tenha sido resolvido no prazo de três dias úteis, o que exige que os prestadores de serviços de pagamento submetam um relatório intercalar adicional. Não obstante, os prestadores de serviços de pagamento devem submeter um relatório intercalar adicional sempre que tal lhes seja solicitado pela autoridade competente do Estado-Membro de origem.

2.15. À semelhança do definido para o relatório inicial, sempre que não se encontrem disponíveis valores reais, os prestadores de serviços de pagamento devem recorrer a estimativas.

2.16. No caso de a atividade comercial regressar à normalidade antes de decorridas quatro horas desde que o incidente foi classificado como de caráter severo, os prestadores de serviços de pagamento devem procurar submeter simultaneamente os relatórios inicial e intercalar (ou seja, preencher as secções A e B do modelo de reporte) dentro do prazo de quatro horas.

Relatório final

2.17. Os prestadores de serviços de pagamento devem submeter 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 valores reais para substituir quaisquer potenciais estimativas.

2.18. Os prestadores de serviços de pagamento devem entregar o relatório final à autoridade competente no prazo máximo de 20 dias úteis 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 ou por não terem sido identificadas as causas do problema) 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 reporte) no prazo de quatro

horas após a classificação do incidente como de caráter severo, devem procurar fornecer, em simultâneo, a informação relacionada com os relatórios inicial, intercalar e final.

2.20. Os prestadores de serviços de pagamento devem incluir no relatório final 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 reporte) e (ii) na secção C do modelo de reporte, 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 ocorrência 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 de caráter 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, no prazo previsto para a submissão do próximo relatório. Nesta situação em particular, em vez de preencher a secção C do modelo de reporte, os prestadores de serviços de pagamento devem selecionar a opção «incidente reclassificado como não severo» e fornecer uma explicação sobre os motivos que justificam a sua reclassificação.

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; ou

ii. nas Orientações da EBA relativas à subcontratação (EBA/GL/2019/02) em relação a todos os prestadores de serviços de pagamento.

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 são adequadamente garantidas.

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 submissão 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, fornecer a informação de contacto referente ao «PSP afetado» no modelo de reporte 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. fornecer uma lista de todos os prestadores de serviços de pagamento afetados pelo incidente;

e. garantir que o terceiro avalia a materialidade do incidente relativamente a cada prestador de serviços de pagamento afetado e apenas inclui no relatório consolidado os prestadores de serviços de pagamento para quem o incidente seja classificado como de caráter severo; adicionalmente, garantir que, em caso de dúvida, o prestador de serviços de pagamento é incluído no relatório consolidado, sempre que não existam evidências que confirmem o contrário;

f. garantir que, sempre que existam campos no modelo de reporte em que não seja possível fornecer uma resposta comum (por ex., secções B2, B4 ou C3), o terceiro procede (i) ao preenchimento individual para cada prestador de serviços de pagamento afetado, identificando especificamente cada prestador a que a informação diz respeito, ou (ii) à utilização de valores cumulativos, conforme observados ou estimados para os prestadores de serviços de pagamento;

g. o terceiro mantém o prestador de serviços de pagamento informado, a todo o momento, de toda a informação relevante relativa ao incidente e de todas as interações que o mesmo possa ter com a autoridade competente, bem como do teor de tais interações, mas apenas na medida do possível, de modo a evitar 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 notificados 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, cumprindo 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.

3.6. Os prestadores de serviços de pagamento devem assegurar que, no caso de um incidente ser causado por uma disrupção nos serviços prestados por um prestador de serviços técnicos (ou uma infraestrutura) que afete vários PSP, a comunicação delegada se refere aos dados individuais do prestador de serviços de pagamento (exceto no caso de comunicação consolidada).

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 tornar relevante um incidente anteriormente não considerado como tal.

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 relevantes identificadas na sequência da aplicação da Orientação 5.1, no mínimo, no momento da receção do relatório inicial (ou, em alternativa, do relatório que espoletou a partilha da informação) e quando forem notificadas de que a atividade comercial regressou à normalidade (i.e. o relatório intercalar).

6.2. As autoridades competentes devem submeter às 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 reporte a seguir indicados (independentemente de se tratar de um relatório inicial ou intercalar):

- data e hora da classificação do incidente como de caráter severo;
- 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 recuperar 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 as 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 garantir, em permanência, a confidencialidade e a integridade da informação armazenada e trocada, bem como a sua adequada autenticação junto das 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 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, utilizando o ficheiro disponível no sítio Web da EBA.

Orientação 8: Comunicação

8.1. As autoridades competentes devem garantir, em permanência, a confidencialidade e a integridade da informação armazenada e trocada, bem como a sua adequada autenticação junto da EBA e do BCE. 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 – Modelo de reporte para prestadores de serviços de pagamento

Relatório inicial

Relatório inicial	no prazo de 4 horas após a classificação do incidente como severo		Redefinir seleções de lista suspensa
Data do relatório *(DD/MM/AAAA)*		Hora *(HH:MM)*	
Código de referência do incidente			

A – Relatório inicial					
A 1 – DISPOSIÇÕES GERAIS					
Tipo de relatório					
Tipo de relatório					
Prestador de serviços de pagamento (PSP) afetado					
Nome do PSP					
Número de identificação nacional do PSP					
Responsável do grupo, se aplicável					
País/países afetado(s) pelo incidente	☐ AT ☐ BE ☐ BG ☐ CY ☐ CZ	☐ DE ☐ DK ☐ EE ☐ ES ☐ FI	☐ FR ☐ LI ☐ GR ☐ HR ☐ HU	☐ IE ☐ IS ☐ IT ☐ LT ☐ LU	☐ LV ☐ MT ☐ NL ☐ NO ☐ PL	☐ PT ☐ RO ☐ SE ☐ SI ☐ SK
Primeira pessoa de contacto		E-mail		Telefone	
Segunda pessoa de contacto		E-mail		Telefone	
Entidade responsável pela comunicação (preencher esta secção se a entidade em causa não for o PSP afetado, em caso de delegação da comunicação)					
Nome da entidade responsável pela comunicação					
Número de identificação nacional					
Primeira pessoa de contacto		E-mail		Telefone	
Segunda pessoa de contacto		E-mail		Telefone	
A 2 – DETEÇÃO E CLASSIFICAÇÃO DE INCIDENTES					
Data e hora de deteção do incidente *(DD/MM/AAAA HH:MM)*					
Data e hora de classificação do incidente *(DD/MM/AAAA HH:MM)*					
O incidente foi detetado por		Se «Outro», especificar:			
Tipo de incidente					
Critérios que levam à elaboração do relatório de incidentes de caráter severo	☐ Operações afetadas ☐ Utilizadores de serviços de pagamento afetados ☐ Interrupção do serviço ☐ Quebra de segurança das redes ou dos sistemas informáticos ☐ Impacto económico ☐ Encaminhamento para as instâncias superiores ☐ Outros PSP ou infraestruturas relevantes potencialmente afetados ☐ Impacto na reputação				
Descrição breve e geral do incidente					
Impacto noutros Estados-Membros da UE, se aplicável					
Comunicação a outras autoridades		Se «Sim», especificar:			
Razões para a apresentação tardia do relatório inicial					

Relatório intercalar

Relatório de incidente de caráter severo

Relatório intercalar	3 dias úteis, no máximo, a contar da apresentação do relatório inicial	Redefinir seleções da lista suspensa

Data do relatório *(DD/MM/AAAA)* | Hora *(HH:MM)*

Código de referência do incidente

B – Relatório intercalar

B 1 – DISPOSIÇÕES GERAIS

Descrição mais pormenorizada do incidente:			
Qual é o problema em concreto?			
Como começou o incidente?			
Como evoluiu?			
Quais são as consequências (em especial para os utilizadores dos serviços de pagamento)?			
O incidente foi comunicado aos utilizadores dos serviços de pagamento?		Se «Sim», especificar:	
Está relacionado com um ou mais incidentes anteriores?		Se «Sim», especificar:	
Outros prestadores de serviços/terceiros foram afetados ou envolvidos?		Se «Sim», especificar:	
Foi iniciado o processo de gestão de crises (interno e/ou externo)?		Se «Sim», especificar:	
Data e hora de início do incidente (se já identificadas) *(DD/MM/AAAA HH:MM)*			
Data e hora da resolução efetiva ou prevista do incidente *(DD/MM/AAAA HH:MM)*			
Áreas funcionais afetadas	☐ Autenticação/autorização ☐ Comunicação ☐ Compensação ☐ Liquidação direta ☐ Liquidação indireta ☐ Outra	Se «Outra», especificar:	
Alterações introduzidas em relatórios anteriores			

B 2 – CLASSIFICAÇÃO DO INCIDENTE/INFORMAÇÃO SOBRE O INCIDENTE

Operações afetadas (2)	Nível de impacto Número de operações afetadas Enquanto % do número normal de operações Valor das operações afetadas em EUR Duração do incidente (aplicável apenas a incidentes operacionais) Observações:		
Utilizadores de serviços de pagamento afetados (3)	Nível de impacto Número de utilizadores de serviços de pagamento afetados Enquanto % dos utilizadores dos serviços de pagamento		
Quebra de segurança das redes ou dos sistemas informáticos		Descrever como a rede ou os sistemas informáticos foram afetados	
Interrupção do serviço	Tempo total de interrupção do serviço:	Dias: / Horas: / Minutos:	
Impacto económico	Nível de impacto Custos diretos em EUR Custos indiretos em EUR		
Encaminhamento para as instâncias superiores internas		Descrever o nível de encaminhamento interno do incidente, indicando se foi, ou é provável que seja, ativado o modo de crise (ou equivalente) e, se sim, fornecer uma descrição	
Outros PSP ou infraestruturas relevantes potencialmente afetados		Descrever de que forma este incidente pode afetar outros PSP e/ou infraestruturas	
Impacto na reputação		Descrever como o incidente pode afetar a reputação do PSP (por exemplo, cobertura mediática, divulgação de ações judiciais ou infrações à lei...)	

B 3 – DESCRIÇÃO DO INCIDENTE

Tipo de incidente			
Causa do incidente	☐ Sob investigação ☐ Ação maliciosa ☐ Falha de processo ☐ Falha desistema ☐ Erro humano ☐ Eventos externos ☐ Outra	Se «Outra», especificar:	
O incidente afetou-o diretamente, ou indiretamente através de um prestador de serviços?		Se indiretamente, indique o nome do prestador de serviços	

B 4 – IMPACTO DO INCIDENTE

Impacto global	☐ Integridade ☐ Disponibilidad	☐ Confidencialidade ☐ Autenticidade	
Canais comerciais afetados	☐ Sucursais ☐ Banca eletrónica ☐ Comércio eletrónico	☐ Banca telefónica ☐ Serviço bancário móvel ☐ ATM	☐ Ponto de venda ☐ Outro
	Se «Outro», especificar:		
Serviços de pagamento afetados	☐ Depósito de numerário numa conta de pagamento ☐ Levantamento de numerário de uma conta de pagamento ☐ Operações necessárias para a gestão de uma conta de ☐ Aquisição de instrumentos de pagamento	☐ Transferência a crédito ☐ Débito direto ☐ Pagamentos com cartão ☐ Emissão de instrumentos de pagamento	☐ Envio de fundos ☐ Serviço de ☐ Serviço de informação sobre contas

B 5 – MITIGAÇÃO DO INCIDENTE

Que ações/medidas foram tomadas até ao momento ou estão previstas para garantir a recuperação de um incidente?	
O Plano de Continuidade de Negócio e/ou o Plano de Recuperação de Desastre foram ativados?	
Se sim, quando? *(DD/MM/AAAA HH:MM)*	
Se sim, descrever	

Relatório final

Relatório de incidente de caráter severo

Selecionar o tipo de relatório:

no prazo de 20 dias úteis a contar da submissão do relatório intercalar

Descrever:
(aplicável a incidentes reclassificados como não severos)

Limpar lista de seleção múltipla

Data do relatório *(DD/MM/AAAA)*

Hora *(HH:MM)*

Código de referência do incidente

C – Relatório final

Se não tiver sido enviado nenhum relatório intercalar, preencher também a secção B

C 1 – DISPOSIÇÕES GERAIS

Atualização das informações do relatório inicial e do(s) relatório(s) intercalar(es)	
Alterações introduzidas em relatórios anteriores	
Qualquer outra informação relevante	
Todos os procedimentos de controlo originais se encontram ativos?	
Se «Não», identificar os controlos e indicar qual o tempo necessário para a sua restauração	
Qual a causa do problema, se já for do conhecimento?	☐ Ação maliciosa ☐ Falha de processo ☐ Falha de sistema ☐ Erro humano ☐ Eventos externos ☐ Outra
Especificar:	☐ Código malicioso ☐ Recolha de informação ☐ Intrusão ☐ Ataque de distribuição/Negação de serviço (D/DoS) ☐ Ações internas deliberadas ☐ Danos físicos externos ☐ Segurança dos conteúdos de informação ☐ Ações fraudulentas ☐ Outra ☐ Monitorização e controlo deficientes ☐ Problemas de comunicação ☐ Operações indevidas ☐ Gestão de alterações inadequada ☐ Inadequação de procedimentos internos e documentação ☐ Problemas de recuperação ☐ Outra ☐ Falha de ☐ Falha de rede ☐ Problemas com a ☐ Falha de aplicação/software ☐ Danos físicos ☐ Outra ☐ Não intencional ☐ Inação ☐ Recursos insuficientes ☐ Outra ☐ Falha de um fornecedor/prestador de serviços técnicos ☐ Força maior ☐ Outra Se «Outra», especificar:
Outras informações relevantes sobre a causa do problema	
Principais ações/medidas corretivas tomadas ou previstas para evitar que o incidente volte a ocorrer no futuro, se já for do conhecimento	

C 3 – INFORMAÇÃO ADICIONAL

O incidente foi partilhado com outros PSP para efeitos de informação?	Se «Sim», especificar:
O PSP foi alvo de alguma ação legal?	Se «Sim», especificar:
Avaliação da eficácia das medidas tomadas	Especificar:

INSTRUÇÕES DE PREENCHIMENTO DO MODELO DE REPORTE

Os prestadores de serviços de pagamento (PSP) devem preencher a secção relevante do modelo de reporte, dependendo da fase de comunicação em que se encontram: secção A (relatório inicial), secção B (relatórios intercalares) ou secção C (relatório final). Os PSP devem utilizar o mesmo modelo de reporte ao submeter os relatórios inicial, intercalar e final relativos ao mesmo incidente. Todos os campos são de preenchimento obrigatório, salvo indicação em contrário.

Cabeçalho

Relatório inicial: primeira notificação que o PSP submete à autoridade competente do Estado-Membro de origem.

Relatório intercalar: contém uma descrição mais pormenorizada do incidente e das suas consequências. Trata-se de uma atualização do relatório inicial (e, se for caso disso, de um relatório intercalar anterior) sobre o mesmo incidente.

Relatório final: último relatório que o PSP irá enviar 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 de caráter severo, sendo necessária a sua reclassificação.

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 PSP devem explicar os motivos da reclassificação.

Data e hora do relatório: data e hora exatas da submissão do relatório à autoridade competente.

Código de referência do incidente (aplicável aos relatórios intercalar e final, bem como às atualizações do relatório inicial): código de referência emitido pela autoridade competente no aquando da submissão do relatório inicial para identificar inequivocamente o incidente. Cada autoridade competente deve incluir como prefixo o código ISO de duas letras[2] do respetivo Estado-Membro.

A - Relatório inicial

A 1 - Disposições gerais

Tipo de relatório:

Individual: o relatório refere-se a um único PSP.

Consolidado: o relatório refere-se aos vários PSP no mesmo Estado-Membro afetados pelo mesmo incidente operacional ou de segurança de caráter severo, que pretendem fazer uso da opção de comunicação 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 PSP).

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 nacional do PSP: o número de identificação nacional único utilizado pela autoridade competente do Estado-Membro de origem no seu registo nacional para identificar inequivocamente o PSP.

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 DSP2.

País(es) 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), independentemente da

[2] Consultar os códigos alfa-2 dos países definidos na norma ISO-3166 em https://www.iso.org/iso-3166-country-codes.html

severidade do incidente no(s) outro(s) país(es). O país(es) 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 ser um terceiro prestador de serviço a 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 o qual podem ser enviados pedidos de esclarecimento, se necessário. Poderá ser um endereço pessoal ou empresarial.

Telefone: número de telefone através do qual podem ser solicitados eventuais pedidos de esclarecimento, se necessário. Pode ser um número de telefone 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 ser um terceiro prestador de serviço a efetuar a comunicação 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 o qual podem ser enviados pedidos de esclarecimento, se necessário. Poderá ser um endereço eletrónico pessoal ou empresarial.

Telefone: número de telefone da pessoa de contacto alternativa através do qual podem ser solicitados eventuais pedidos de esclarecimento, se necessário. Pode ser um número de telefone pessoal ou empresarial.

Entidade responsável pela comunicação: esta secção deve ser preenchida no caso de ser um terceiro a 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 nacional: número de identificação nacional único utilizado no país em que o terceiro está situado para identificar inequivocamente a entidade que comunica o incidente. Se o terceiro responsável pela comunicação for um PSP, o número de identificação nacional deve ser o número de identificação nacional único do PSP utilizado pela autoridade competente do Estado-Membro de origem no seu registo nacional.

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

E-mail: endereço eletrónico para o qual podem ser enviados pedidos de esclarecimento, se necessário. Poderá ser um endereço eletrónico pessoal ou empresarial.

Telefone: número de telefone através do qual podem ser solicitados eventuais pedidos de esclarecimento, se necessário. Pode ser um número de telefone 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 o qual podem ser enviados pedidos de esclarecimento, se necessário. Poderá ser um endereço eletrónico pessoal ou empresarial.

Telefone: número de telefone da pessoa de contacto alternativa através do qual podem ser solicitados pedidos de esclarecimento, se necessário. Pode ser um número de telefone pessoal ou empresarial.

A 2 - Deteção e classificação de incidentes

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

Data e hora de classificação do incidente: data e hora em que o incidente de segurança ou operacional foi classificado como de caráter severo.
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). Se o incidente não tiver sido detetado por nenhuma destas entidades, fornecer uma explicação no campo correspondente.
Tipo de incidente: indicar, tanto quanto seja do conhecimento e se a informação estiver disponível, se se trata de um incidente operacional ou de segurança.

> **Operacional:** incidente provocado pela inadequação ou falha de processos, pessoas, sistemas ou eventos de força maior que afetaram a integridade, disponibilidade, confidencialidade e/ou autenticidade 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 e/ou autenticidade dos serviços relacionados com pagamentos. Esta situação pode acontecer, por ex., quando o PSP experiencia uma quebra de segurança na sua rede ou sistemas de informação.

Critérios que justificam a submissão do relatório de incidentes de caráter severo: indicar qual dos critérios desencadeou o relatório de incidentes de caráter severo. Podem ser selecionados vários critérios: operações afetadas, utilizadores de serviços de pagamento afetados, interrupção do serviço, quebra de segurança da rede ou dos sistemas de informação, impacto económico, encaminhamento para as instâncias superiores internas, outros PSP ou infraestruturas relevantes potencialmente afetados e/ou impacto na reputação.
Descrição breve e geral do incidente: descrever sucintamente os aspetos mais relevantes do incidente, cobrindo as causas possíveis, os efeitos imediatos, etc.
Impacto noutros Estados-Membros da UE, se aplicável: explicar sucintamente o impacto que o incidente teve noutro Estado-Membro da UE (por ex., nos utilizadores de serviços de pagamento, nos PSP e/ou nas infraestruturas de pagamento). Fornecer uma tradução em inglês, sempre que for possível fazê-lo dentro dos prazos de comunicação aplicáveis.
Comunicação a outras autoridades: indicar se o incidente foi/será comunicado a outras autoridades ao abrigo de outras obrigações de reporte de comunicação de incidentes, se tal for do conhecimento no momento da comunicação. Em caso afirmativo, identificar as autoridades competentes.
Razões para a submissão tardia do relatório inicial: explicar as razões porque foi necessário um prazo superior a 24 horas para classificar o incidente.

B Relatório intercalar

B 1 – Disposições gerais

Descrição mais pormenorizada do incidente: descrever as principais características do incidente, abrangendo, pelo menos, informação sobre o problema em específico e o respetivo enquadramento, descrição de como o incidente se iniciou, evoluiu e as suas consequências, especialmente para os utilizadores de serviços de pagamento, etc. Fornecer também informação sobre a comunicação com os utilizadores de serviços de pagamento, se aplicável.
O incidente está relacionado com um ou mais incidentes anteriores?: indicar se o incidente está ou não relacionado com incidentes anteriores, caso essa informação esteja disponível. Se o incidente estiver relacionado com incidentes anteriores, especificar quais.
Outros prestadores de serviços/terceiros foram afetados ou envolvidos?:indicar se o incidente afetou ou envolveu outros prestadores de serviços/terceiros, caso essa informação esteja disponível. Se o incidente tiver afetado ou envolvido outros prestadores de serviços/terceiros, identificá-los e fornecer mais informação.

Foi ativado o processo de gestão de crises (interno e/ou externo)?: indicar se o processo de gestão de crises (interno e/ou externo) foi ou não ativado. Se o processo de gestão de crises tiver sido ativado, fornecer mais informação.

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

Data e hora da resolução efetiva ou prevista do incidente: 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.

Áreas funcionais afetadas: indicar a(s) fase(s) do processo de pagamento que foram afetadas pelo incidente, tais como autenticação/autorização, comunicação, compensação, liquidação direta, liquidação indireta e outras.

Autenticação/autorização: 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 e o consentimento do utilizador do serviço de pagamento (ou de uma entidade terceira atuando em seu nome) para a transferência de fundos.

Comunicação: fluxo de informação para efeitos de identificação, autenticação, notificação e informação entre os PSP que gerem as contas e os prestadores de serviços de iniciação de pagamento, prestadores de serviços de informação sobre contas, ordenantes, beneficiários e outros PSP.

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 esta 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.

Alterações introduzidas em relatórios anteriores: indicar as alterações à informação fornecida em relatórios anteriores relacionadas com o mesmo incidente (por ex., no relatório inicial ou, quando aplicável, no relatório intercalar).

B 2 – Classificação do incidente/Informação sobre o incidente

Operações afetadas: Os PSP 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 mesmos serviços de pagamento afetados pelo incidente e o valor total das operações. Os PSP devem fornecer valores concretos para estas variáveis, os quais podem ser reais ou estimativas. Regra geral, os PSP devem considerar como «operações afetadas» todas as operações nacionais e transfronteiriças que tenham sido, ou é provável que venham 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 de os fundos terem sido recuperados ou não). Adicionalmente, os PSP 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, tendo por base o ano anterior

como período de referência para efeitos de cálculo. Se os PSP 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». Se o incidente afetar operações de pagamento em moedas diferentes do euro, ao calcular os limites e ao comunicar o valor das operações afetadas, os PSP devem converter para euros o montante das operações, utilizando a taxa de câmbio de referência diária do BCE referente ao dia anterior à submissão do relatório de incidentes.

Utilizadores de serviços de pagamento afetados: Os PSP 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 PSP devem fornecer valores concretos para estas variáveis, os quais podem ser reais ou estimativas. Os PSP devem considerar como «utilizadores de serviços de pagamento afetados» todos os clientes (nacionais ou estrangeiros, consumidores ou empresas) que possuam um contrato com o PSP afetado que lhes garante o acesso ao referido serviço, e que tenham sofrido, ou é provável que venham 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 PSP 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 do seu próprio serviço 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 PSP que usufruem desses serviços operacionais devem avaliar o incidente em relação aos seus próprios utilizadores de serviços de pagamento. Além disso, os PSP 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 sua dimensão ou de serem considerados utilizadores ativos ou passivos dos serviços em causa.

Quebra de segurança nas redes ou nos sistemas de informação: Os PSP devem verificar se alguma ação maliciosa comprometeu a disponibilidade, autenticidade, integridade ou confidencialidade da rede ou dos sistemas informação (incluindo dados) relacionados com a prestação de serviços de pagamento.

Interrupção do serviço: Os PSP 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 PSP devem fornecer valores concretos para estas variáveis, os quais podem ser reais ou estimativas. Os PSP devem considerar o período de tempo em que qualquer tarefa, processo ou canal associado à prestação de serviços de pagamento está, ou é provável que venha 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 PSP devem contabilizar o tempo de interrupção do serviço a partir do início da interrupção, considerando quer o período de tempo em que a execução de serviços de pagamento está disponível ao público, quer as horas de encerramento e os períodos de manutenção, quando relevante e aplicável. Caso os PSP não consigam determinar o momento em que a interrupção do serviço teve início, devem excecionalmente contabilizar a interrupção a partir do momento da sua deteção.

Impacto económico: Os PSP 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 PSP devem fornecer valores concretos para estas variáveis, os quais podem ser reais ou estimativas. Os PSP devem considerar quer os custos diretos, quer os indiretos relacionados com o incidente. Entre outros fatores, os PSP 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 PSP devem considerar apenas aqueles que já forem do conhecimento ou os que são muito

prováveis de se vir materializar. Se os custos forem expressos em moedas diferentes do euro, ao calcular o limite e ao comunicar o valor do impacto económico, os PSP devem converter para euros o montante dos custos, utilizando a taxa de câmbio de referência diária do BCE referente ao dia anterior à submissão do relatório de incidentes.

Custos diretos: Custos, expressos em euros, diretamente resultantes do incidente, incluindo os custos necessários para a resolução do incidente (por ex., fundos ou ativos expropriados, custos de substituição de *hardware* e *software*, taxas por incumprimento de obrigações contratuais).

Custos indiretos: custos, expressos em euros, indiretamente resultantes do incidente (por ex., custos de ressarcimento/compensação do cliente, potenciais custos legais).

Encaminhamento para as instâncias superiores internas: Os PSP devem considerar se, em resultado do impacto nos serviços relacionados com pagamentos, o órgão de administração, tal como definido nas Orientações da EBA relativas à gestão dos riscos associados às TIC e à segurança, foi, ou é provável que venha a ser, informado, em conformidade com a alínea d) da Orientação 60 das Orientações da EBA relativas à gestão dos riscos associados às TIC e à segurança, sobre o incidente fora do âmbito de qualquer procedimento de notificação periódico e numa base contínua durante o período de ocorrência do incidente. Além disso, os PSP devem considerar se foi, ou é provável que venha a ser, ativado o modo de crise em resultado do impacto do incidente nos serviços relacionados com pagamentos.

Outros PSP ou infraestruturas relevantes potencialmente afetados: Os PSP devem avaliar o impacto do incidente no mercado financeiro, incluindo as infraestruturas do mercado financeiro e/ou os sistemas de pagamento que o suportam e os restantes PSP. Em particular, os PSP devem avaliar se o incidente teve, ou é provável que venha a ter, repercussões noutros PSP, se afetou, ou é provável que venha a afetar, o adequado funcionamento das infraestruturas do mercado financeiro e se comprometeu, ou é provável que venha a comprometer, a solidez de todo o sistema financeiro. Os PSP 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 é provável que venha a deixar, de cumprir as suas obrigações perante as infraestruturas do mercado financeiro às quais pertence.

Impacto na reputação: Os PSP devem considerar o nível de visibilidade que, tanto quanto seja do seu conhecimento, o incidente obteve, ou é provável que venha a obter, no mercado. Os PSP 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 PSP devem ter em consideração i) se os utilizadores de serviços de pagamento e/ou outros PSP se queixaram do impacto adverso do incidente, ii) se o incidente afetou algum processo com visibilidade relacionado com os serviços de pagamento sendo, por conseguinte, provável que receba, ou já tenha recebido, cobertura mediática (considerando não só os meios tradicionais, como os jornais, mas também os blogues, as redes sociais, etc.); no entanto, neste contexto, a cobertura mediática não significa apenas alguns comentários negativos por parte dos seguidores, devendo existir um relatório válido ou um número significativo de comentários/alertas negativos), iii) se as obrigações contratuais não foram ou, é provável que não venham a ser, cumpridas, resultando na divulgação de ações judiciais contra o PSP, iv) se os requisitos regulamentares não foram cumpridos, resultando na imposição de medidas de supervisão ou sanções que foram, ou é provável que venham a ser, divulgadas ao público ou v) se o mesmo tipo de incidente já ocorreu anteriormente.

B **3 – Descrição do incidente**

Tipo de incidente: operacional ou de segurança. No campo correspondente do relatório inicial, são fornecidas mais explicações.

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

Sob investigação: selecionar esta opção se a causa for desconhecida no momento.

Ação maliciosa: ações que visem intencionalmente o PSP. Estas abrangem código malicioso, recolha de informação, intrusão, ataque distribuído/negação de serviço (D/DoS), ações internas deliberadas, danos físicos externos deliberados, ataques à segurança de conteúdos de informação, ações fraudulentas e outras. Para mais informações, consultar a secção C2 deste modelo de reporte.

Falha de processo: a causa do incidente resulta da fraca 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, redes, infraestruturas e bases de dados que suportam a atividade de pagamento.

Erro humano: o incidente foi causado pelo erro inadvertido de uma pessoa, tendo afetado parte de um procedimento de pagamento (por ex. carregamento incorreto 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).

Eventos externos: a causa está associada a acontecimentos que, de um modo geral, não estão sob o controlo direto da organização (por ex., desastres naturais ou falha de um prestador de serviços técnicos).

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 direta ou indiretamente através de um prestador de serviços?: indicar se o incidente visou diretamente o PSP ou se o afeta indiretamente através de terceiros, se essa informação estiver disponível. Em caso de impacto indireto, indicar o(s) nome(s) do(s) prestador(es) de serviços.

B 4 – Impacto do incidente

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

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

Disponibilidade: característica que permite que os serviços relacionados com pagamentos sejam totalmente acessíveis e utilizáveis pelos utilizadores de serviços de pagamento, de acordo com níveis aceitáveis e predefinidos.

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.

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. Todos os estabelecimentos situados no mesmo Estado-Membro, de um PSP com sede 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.

ATM: dispositivo eletromecânico que permite 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.

Comércio eletrónico: operação de pagamento que é iniciada num ponto de venda virtual (por ex., pagamentos iniciados através da internet utilizando transferências a crédito, cartões de pagamento, transferências de moeda eletrónica entre contas de moeda eletrónica).

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 vinculado por contrato 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.

Transferência a crédito: serviço de pagamento prestado pelo PSP 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.

Débito 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 PSP do beneficiário ou ao PSP do próprio ordenante.

Pagamento 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 vinculado por contrato prestado por um PSP 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 de pagamento 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 de pagamento *on-line* 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 PSP.

B 5 – Mitigação do incidente

Que ações/medidas foram tomadas até ao momento ou estão previstas para garantir a recuperação do incidente?: Fornecer informação mais detalhada sobre as medidas tomadas ou previstas para resolver temporariamente o incidente.

O Plano de Continuidade de Negócio e/ou o Plano de Recuperação de Desastre foram ativados?: Indicar se tal aconteceu e, em caso afirmativo, fornecer os detalhes mais relevantes sobre a situação (i.e., quando foram ativados e em que consistiram esses planos).

C – Relatório final

C 1 – Disposições gerais

Atualização das informações do relatório inicial e do(s) relatório(s) intercalar(es) (resumo): fornecer informações adicionais sobre o incidente, incluindo as alterações específicas feitas às informações fornecidas com o relatório intercalar. Incluir também quaisquer outras informações relevantes.

Todos os procedimentos de controlo originais se encontram ativos?: Indicar se, em algum momento, o PSP teve ou não de cancelar ou reduzir alguns controlos durante o incidente. Em caso afirmativo, indicar se todos os controlos já se encontram ativos e, se tal não tiver acontecido, especificar no campo de texto livre quais os controlos que ainda não foram ativados e o tempo que será necessário para a sua restauração.

C 2 – Análise da causa do problema e acompanhamento

Qual a causa do problema, se já for do conhecimento?: Indicar o que esteve na origem do incidente ou, se tal ainda não for do conhecimento, indicar a causa mais provável. Possibilidade de resposta múltipla. (Ter em conta que a causa deve ser diferenciada do impacto do incidente)

- **Ação maliciosa:** ações externas ou internas que visem intencionalmente o PSP. Estas causas estão divididas pelas seguintes categorias:
  - **Código malicioso:** por ex., um vírus, *worm*, *Trojan*, *spyware*.
  - **Recolha de informação:** por ex., digitalização, interceção, engenharia social.
  - **Intrusão:** por ex., comprometimento de conta privilegiada, comprometimento de conta não privilegiada, comprometimento de aplicação, *bot*.
  - **Ataque distribuído/negação de serviço (D/DoS):** tentativa de tornar indisponível um serviço *on-line* através de uma sobrecarga de tráfego com múltiplas origens.
  - **Ações internas deliberadas:** por ex., sabotagem, roubo.
  - **Danos físicos externos deliberados:** por ex., sabotagem, ataque físico às instalações/centros de dados.
  - **Segurança dos conteúdos de informação:** acesso não autorizado à informação, alteração não autorizada da informação.
  - **Ações fraudulentas:** utilização não autorizada de recursos e de direitos de autor, disfarce, *phishing*.
  - **Outra (especificar):** nenhuma das causas acima indicadas está na origem do incidente. O campo de texto livre deve ser preenchido com informação mais detalhada.
- **Falha de processo:** a causa do incidente resulta da fraca 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). Estas causas estão divididas pelas seguintes categorias:
  - **Monitorização e controlo deficientes:** por ex., em relação a operações em execução, datas de expiração de certificados, datas de expiração de licenças, datas de expiração de atualizações de segurança, valores máximos de contravalores definidos, níveis de preenchimento de bases de dados, gestão de direitos de utilizadores, princípio de controlo duplo.

Problemas de comunicação: por ex., entre participantes de mercado ou dentro da organização.

Operações indevidas: por ex., sem exigência de certificados, *cache* cheia.

Gestão de alterações inadequada: por ex., erros de configuração não identificados, implementação incluindo atualizações, problemas de manutenção, erros inesperados.

Inadequação de procedimentos internos e documentação: por exemplo, falta de transparência no que respeita às funcionalidades, processos e ocorrências de avarias, ausência de documentação.

Problemas de recuperação: por ex., gestão de contingências, redundância inadequada.

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

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, redes, infraestruturas e bases de dados que suportam a atividade de pagamento. Estas causas estão divididas pelas seguintes categorias:

Falha de *hardware*: falha do equipamento físico tecnológico que executa processos e/ou armazena os dados necessários que permitem aos PSP levar a cabo operações relacionadas com pagamentos (por ex., falha ao nível dos discos rígidos, dos centros de dados ou de outras infraestruturas).

Falha de rede: falha das redes de telecomunicações, públicas ou privadas, que permitem a troca de dados e de informação (por ex., através da internet) durante o processo de pagamento.

Problemas com a base de dados: problemas com a estrutura de dados que armazena informação pessoal e relacionada com pagamentos necessária para executar operações de pagamento.

Falha de aplicação/*software*: falhas dos programas, sistemas operativos, etc. que apoiam a prestação dos serviços de pagamento pelo PSP (por ex., mau funcionamento, funcionalidades desconhecidas).

Danos físicos: por ex., danos não intencionais causados por condições inadequadas, obras de construção.

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

Erro humano: o incidente foi causado pelo erro inadvertido de uma pessoa, tendo afetado parte de um procedimento de pagamento (por ex. carregamento incorreto 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). Estas causas estão divididas pelas seguintes categorias:

Não intencional: por ex., erros, omissões, falta de experiência e de conhecimentos.

Inação: por ex., devido à falta de competências, conhecimentos, experiência e sensibilização.

Recursos insuficientes: por ex., falta de recursos humanos e de disponibilidade de pessoal.

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

Evento externo: a causa está associada a acontecimentos que, de um modo geral, não estão sob o controlo da organização. Estas causas estão divididas pelas seguintes categorias:

Falha de um fornecedor/prestador de serviços técnicos: por ex., falha de energia, quebra do serviço de internet, problemas legais, problemas comerciais, dependências de serviços.

Força maior: por ex., falha de energia, incêndio, causas naturais como terramotos, inundações, precipitação forte, vento intenso.

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

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

Outras informações relevantes sobre a causa do problema: fornecer quaisquer detalhes adicionais sobre a causa do problema, incluindo as conclusões preliminares retiradas da análise da causa do problema.

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 futura ocorrência do incidente.

C 3 – Informação adicional

O incidente foi partilhado com outros PSP para efeitos de informação?: Identificar os PSP que foram contactados, formal ou informalmente, para dar informações 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, até ao momento do preenchimento do relatório final, o PSP foi alvo de qualquer ação legal (por ex., se foi a tribunal ou se perdeu a sua licença) em resultado do incidente.

Avaliação da eficácia das medidas tomadas: incluir, quando disponível, uma autoavaliação da eficácia das medidas tomadas durante a duração do incidente, incluindo quaisquer lições retiradas do incidente.