BANCO DE PORTUGAL
EUROSISTEMA

Instrução n.º 01/2019

BO n.º 1/2019 • 2019/01/15

Temas

Sistemas de Pagamentos :: Elementos de Informação

Índice

Texto da Instrução

Assunto: Reporte de incidentes de caráter severo

A 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), no seu artigo 96.º ("Notificação de incidentes"), consagra o dever de notificação por parte dos prestadores de serviços de pagamento (PSP), no caso da ocorrência de um incidente operacional ou de segurança de caráter severo relacionado com a prestação de serviços de pagamento.

Complementarmente, o n.º 3 do referido artigo 96.º da DSP2 determina que a Autoridade Bancária Europeia (EBA) emite Orientações relativas à classificação dos incidentes operacionais ou de segurança de caráter severo pelos PSP e de comunicação de tais incidentes à autoridade competente do Estado-Membro de origem.

Neste âmbito, a EBA emitiu as "Orientações sobre a comunicação de incidentes de caráter severo ao abrigo da DSP2" (EBA/GL/2017/10), as quais estabelecem os critérios para a classificação de incidentes operacionais ou de segurança de caráter severo e os procedimentos de comunicação desses incidentes pelos PSP às autoridades competentes. As referidas Orientações definem ainda a forma como as autoridades competentes devem avaliar a relevância dos incidentes comunicados pelos PSP e partilhar essa informação com a EBA, o Banco Central Europeu (BCE) e outras autoridades nacionais.

As supracitadas Orientações da EBA entraram em vigor em 13 de janeiro de 2018 e podem ser consultadas (na versão inglesa e portuguesa) através do seguinte link: https://www.eba.europa.eu/regulation-and-policy/payment-services-and-electronic-money/guidelines-on-major-incidents-reporting-under-psd2.

A nível nacional, o artigo 71.º do Decreto-Lei n.º 91/2018, de 12 de novembro, que transpôs a disposição relativa ao artigo 96.º da DSP2 para o ordenamento jurídico português, estabelece no seu n.º 1 que os PSP com sede em Portugal devem fazer a referida comunicação, sem demora, ao Banco de Portugal. Por seu turno, o n.º 2 do mesmo artigo determina que o Banco de Portugal deve estabelecer as normas regulamentares respeitantes à classificação, por parte dos PSP, dos referidos incidentes de caráter severo e ao conteúdo, formato, modelos e procedimentos de comunicação de tais incidentes pelos PSP.

Nestes termos, o Banco de Portugal, no uso da competência que lhe é conferida pelo artigo 14.º da sua Lei Orgânica, aprovada pela Lei n.º 5/98, de 31 de janeiro, e pelo n.º 2 do artigo 71.º do Decreto-Lei n.º 91/2018, de 12 de novembro, determina o seguinte:

I – ÂMBITO DE APLICAÇÃO E DISPOSIÇÕES GERAIS

1. Objeto

1.1. A presente instrução regulamenta o dever de comunicação, ao Banco de Portugal, dos incidentes operacionais ou de segurança de caráter severo, em cumprimento do estabelecido do artigo 71.º do Regime Jurídico dos Serviços de Pagamento da Moeda Eletrónica (RJSPME), publicado em anexo ao Decreto-Lei n.º 91/2018, de 12 de novembro, que integrou no ordenamento jurídico português a disposição do artigo 96.º da DSP2.

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

1.2. Para efeito do disposto no número anterior, a presente instrução implementa as "Orientações revistas sobre a comunicação de incidentes de caráter severo ao abrigo da DSP2" emitidas pela EBA (EBA/GL/2021/03), que estabelecem os critérios para a classificação de incidentes operacionais ou de segurança de caráter severo e os procedimentos de comunicação desses incidentes pelos PSP às autoridades competentes.

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

1.3. São objeto desta instrução os incidentes de carácter severo que afetem as funções desempenhadas pelos próprios PSP e as funções subcontratadas pelos PSP a terceiros.

Aditado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

2. Destinatários

São destinatários da presente Instrução os PSP registados e autorizados pelo Banco de Portugal, ainda que operando em outros países por intermédio do exercício do direito de estabelecimento ou da livre prestação de serviços.

3. Definições

Para efeitos da presente Instrução são aplicáveis as definições constantes no artigo 2.º do RJSPME e as seguidamente indicadas:

Incidente operacional ou de segurança: Um evento único ou uma série de eventos conexos e não previstos pelo PSP, que têm, ou é provável que venham a ter, um impacto adverso na integridade, disponibilidade, confidencialidade e/ou autenticidade 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 PSP.

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 vv) do artigo 2.º do RJSPME e todas as tarefas de suporte técnico necessárias à correta prestação de serviços de pagamento.

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

II – REQUISITOS DE REPORTE

4. Classificação de um incidente como de caráter severo

4.1. Os PSP devem classificar como de caráter severo os incidentes operacionais ou de segurança que preencham:

4.1.1. um ou mais critérios de "nível de impacto superior", ou

4.1.2. três ou mais critérios de "nível de impacto inferior",

conforme indicado na tabela seguinte:

Critérios	**Nível de impacto inferior**	**Nível de impacto superior**
Operações afetadas	> 10 % do nível normal de operações do PSP (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 PSP (em termos de número de operações) **ou** > 15 000 000 EUR
Utilizadores de serviços de pagamento afetados	> 5 000 **e** duração do incidente > 1 hora* **ou** > 10 % dos utilizadores de serviços de pagamento do PSP **e** duração do incidente > 1 hora*	> 50 000 **ou** > 25 % dos utilizadores de serviços de pagamento do PSP

Critérios	Nível de impacto inferior	Nível de impacto superior
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 PSP 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 PSP 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, 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.

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

5. Critérios / indicadores a considerar

5.1. Os PSP devem avaliar os incidentes operacionais ou de segurança de acordo com os critérios e respetivos indicadores subjacentes a seguir indicados:

5.1.1. Operações afetadas: os PSP 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.

5.1.2. Utilizadores de serviços de pagamentos afetados: os PSP 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.

5.1.3. Quebra de segurança na rede ou nos sistemas de informação: os PSP devem verificar se alguma ação maliciosa comprometeu a segurança da rede ou dos sistemas de informação relacionados com a prestação de serviços de pagamento.

5.1.4. Interrupção do serviço: os PSP 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 ii) do artigo 2.º do RJSPME, não poderá ser executada pelo PSP.

5.1.5. Impacto económico: os PSP 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 PSP (ou seja, aos fundos próprios de nível 1 do PSP).

5.1.6. Encaminhamento para as instâncias superiores internas: os PSP devem determinar se o incidente em causa foi, ou é provável que venha a ser, comunicado ao órgão de administração.

5.1.7. Outros PSP ou infraestruturas relevantes potencialmente afetadas: os PSP devem determinar as prováveis implicações sistémicas do incidente, nomeadamente o risco de contágio de outros PSP, infraestruturas do mercado financeiro e/ou sistemas de pagamento.

5.1.8. Impacto na reputação: os PSP devem determinar de que forma o incidente pode prejudicar a confiança dos utilizadores no próprio PSP e, de uma forma geral, no serviço em causa ou em todo o mercado.

5.2. Os PSP devem calcular o valor dos indicadores de acordo com a seguinte metodologia:

5.2.1. Operações afetadas: 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 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 PSP 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 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, considerando o exercício anterior como período de referência para efeitos de cálculo. No caso de os PSP não considerarem este número representativo (por ex., devido à sazonalidade), devem utilizar outra medida mais representativa e transmitir ao Banco de Portugal o racional subjacente a essa abordagem no campo correspondente do relatório de reporte.

5.2.2. Utilizadores de serviços de pagamentos afetados: 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 seus próprios utilizadores de serviços de pagamento. Se se tratar de um PSP que disponibilize serviços operacionais a terceiros, o mesmo deve apenas considerar os seus próprios utilizadores de serviços de pagamento (se tiver algum) e os PSP 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 PSP 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 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 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.

5.2.3. Quebra de segurança na rede ou nos sistemas de informação: os PSP 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.

5.2.4. Interrupção do serviço: 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 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 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.

5.2.5. Impacto económico: os PSP devem considerar os custos direta e indiretamente 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 materializar.

5.2.6. 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.

5.2.7. Outros PSP ou infraestruturas relevantes potencialmente afetadas: 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, o bom funcionamento 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, ou se a rede comprometida é interna ou externa ou 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.

5.2.8. 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 de comunicação social (incluindo para além dos meios 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 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, e (v) se o mesmo tipo de incidente já ocorreu anteriormente.

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

5.4. Os PSP 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 descrito no ponto 10.5 desta instrução e sem demora injustificada).

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

III – PROCESSO DE REPORTE

6. Canal de reporte

6.1. Os PSP devem comunicar ao Banco de Portugal os incidentes de caráter severo através do preenchimento de um relatório, em língua inglesa, no portal BP*net* (www.bportugal.net).

6.2. Para o efeito, os responsáveis pela submissão dos reportes ao Banco de Portugal devem aderir ao serviço "Sistemas de Pagamentos » Reporte de incidentes DSP2" disponibilizado no portal BP*net*.

7. Modelo de reporte

7.1. Os PSP devem recolher toda a informação relevante, preencher o relatório de incidentes, de acordo com as instruções fornecidas no manual técnico que se encontra no Portal BPnet e utilizando para o efeito o modelo também disponível no Portal BPnet, e submetê-lo ao Banco de Portugal, enquanto autoridade competente do Estado-Membro de origem.

7.2. Os PSP devem preencher os relatórios iniciais, intercalares e finais relativos ao mesmo incidente de forma incremental, e atualizar, quando aplicável, as informações fornecidas nos relatórios anteriores.

7.3. Caso aplicável, os PSP devem ainda remeter ao Banco de Portugal, através do e-mail sp.psd2@bportugal.pt, uma cópia da informação fornecida (ou a fornecer) aos seus utilizadores, como previsto na alínea b) do n.º 1 do artigo 71.º do RJSPME, assim que essa informação se encontrar disponível.

7.4. Os PSP devem, a pedido do Banco de Portugal, fornecer todo e qualquer documento adicional que complemente as informações apresentadas no relatório, sob a forma de um ou vários anexos remetidos para o e-mail sp.psd2@bportugal.pt.

7.5. Os PSP devem dar resposta a qualquer pedido de informação adicional ou de esclarecimentos sobre a documentação submetida, efetuado pelo Banco de Portugal.

7.6. Qualquer informação adicional contida nos documentos fornecidos pelos PSP ao Banco de Portugal, quer por iniciativa do PSP, quer a pedido do Banco de Portugal, em conformidade com o ponto anterior desta instrução, deve ser refletida pelo PSP no respetivo relatório de incidente.

7.7. Os PSP devem garantir, em permanência, a confidencialidade e a integridade da informação trocada, bem como a sua adequada autenticação junto do Banco de Portugal.

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

8. Reporte inicial

8.1. Os PSP devem submeter um relatório inicial ao Banco de Portugal sempre que um incidente operacional ou de segurança for classificado como de caráter severo. O Banco de Portugal deve acusar sem demora a receção do relatório inicial e atribuir um código de referência único que identifique inequivocamente o incidente. Os PSP 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.

8.2. Os PSP devem enviar o relatório inicial ao Banco de Portugal no prazo de 4 horas a partir do momento em que o incidente operacional ou de segurança foi classificado como de caráter severo, ou, no caso da BPnet não se encontrar disponível ou operacional nesse momento, assim que se encontre novamente disponível/operacional.

8.3. Os PSP devem classificar o incidente em conformidade com o exposto no ponto 4 desta Instrução, 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 PSP. Caso seja necessário um prazo mais longo para classificar o incidente, os PSP devem explicar, no relatório inicial submetido ao Banco de Portugal, as razões para o prolongamento do prazo.

8.4. Os PSP devem ainda submeter um relatório inicial ao Banco de Portugal sempre que um incidente de caráter não severo seja reclassificado como de caráter severo. Neste caso específico, os PSP devem enviar o relatório inicial ao Banco de Portugal imediatamente após a deteção da alteração de estado, ou, no caso da BPnet não se encontrar disponível ou operacional nesse momento, assim que se encontre novamente disponível/operacional.

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

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

9. Reporte intercalar

9.1. Os PSP devem submeter o relatório intercalar assim que as atividades regulares forem recuperadas e a atividade comercial regresse à normalidade, informando o Banco de Portugal deste facto. Os PSP devem considerar que a atividade comercial regressou à normalidade quando as atividades/operações forem recuperadas para os mesmos níveis de serviço/condições definidos pelo PSP, 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 relatório).

9.2. Caso as atividades regulares ainda não tiverem sido recuperadas, os PSP devem submeter um relatório intercalar ao Banco de Portugal no prazo de 3 dias úteis a contar da submissão do relatório inicial.

9.3. Os PSP devem atualizar a informação já fornecida nas secções A e B do relatório 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 os casos em que o incidente não tenha sido resolvido no prazo de 3 dias úteis, o que exige que os PSP submetam um relatório intercalar adicional. Não obstante, os PSP devem submeter um relatório intercalar adicional sempre que tal lhes seja solicitado pelo Banco de Portugal.

9.4. À semelhança do definido para o relatório inicial, sempre que não se encontrem disponíveis valores reais, os PSP devem recorrer a estimativas.

9.5. No caso de a atividade comercial regressar à normalidade antes de decorridas 4 horas desde que o incidente foi classificado como de caráter severo, os PSP devem procurar submeter simultaneamente os relatórios inicial e intercalar (preenchendo as secções A e B do relatório) dentro desse prazo de 4 horas.

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

10. Reporte final

10.1. Os PSP 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.

10.2. Os PSP devem entregar o relatório final ao Banco de Portugal no prazo máximo de 20 dias úteis após o regresso à normalidade. Os PSP 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 o Banco de Portugal 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.

10.3. No caso dos PSP conseguirem fornecer toda a informação solicitada no relatório final (secção C do relatório) no prazo de 4 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.

10.4. Os PSP 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 relatório) e (ii) na secção C do relatório, 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.

10.5. Os PSP 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 PSP 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 relatório, os PSP devem selecionar a opção "incidente reclassificado como não severo" e fornecer uma explicação sobre os motivos que justificam a sua reclassificação.

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

11. Delegação do reporte

11.1. Sempre que tal seja autorizado pelo Banco de Portugal, os PSP que pretendam delegar as suas obrigações de comunicação de incidentes de caráter severo ao abrigo do artigo 71.º do RJSPME a um terceiro devem informar o Banco de Portugal 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 PSP 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 PSP afetado continua a ser inteiramente responsável pelo cumprimento dos requisitos definidos no artigo 71.º do RJSPME, assim como pelo conteúdo da informação fornecida ao Banco de Portugal.

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

   i. no artigo 71.º do RJSPME relativamente às instituições de pagamento e às instituições de moeda eletrónica, aplicável, com as necessárias adaptações, em conformidade com o artigo 3.º da Diretiva 2009/110/CE do Parlamento Europeu e do Conselho, de 16 de setembro de 2009, relativa ao acesso à atividade das instituições de moeda eletrónica, ao seu exercício e à sua supervisão prudencial (Diretiva da Moeda Eletrónica); ou

   ii. nas Orientações da EBA relativas à subcontratação (EBA/GL/2019/02) em relação todos os PSP.

c) A informação deve ser previamente submetida ao Banco de Portugal e, em todo o caso, cumprindo todos os prazos e procedimentos estabelecidos pelo Banco de Portugal.

d) A confidencialidade de dados sensíveis e a qualidade, consistência, integridade e fiabilidade da informação a fornecer ao Banco de Portugal são adequadamente garantidas.

11.2. Os PSP não devem delegar as suas obrigações de comunicação depois de terem sido notificados de que o contrato de externalização não preenche os requisitos estabelecidos na alínea b) do número 11.1.

11.3. Os PSP que pretendam cancelar a delegação das suas obrigações de comunicação devem comunicar a sua decisão ao Banco de Portugal no prazo de 15 dias úteis antes da data pretendida para o cancelamento.

11.4. Os PSP devem informar o Banco de Portugal sobre qualquer acontecimento relevante que afete o terceiro designado e a sua capacidade de cumprir com as obrigações de comunicação.

11.5. Os PSP devem cumprir as suas obrigações de comunicação sem qualquer recurso a apoio externo sempre que o terceiro designado falhe o dever de informar o Banco de Portugal sobre um incidente operacional ou de segurança de caráter severo, em conformidade com o disposto no artigo 71º do RJSPME e da presente Instrução.

11.6. Os PSP devem certificar-se de que um incidente não é comunicado duas vezes, individualmente pelo respetivo PSP e também pelo terceiro.

11.7. Os PSP 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 PSP (exceto no caso de comunicação consolidada).

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

12. Reporte consolidado

Os PSP 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 PSP afetados pelo mesmo incidente operacional ou de segurança de caráter severo) devem informar o Banco de Portugal, fornecer a informação de contacto referente ao "PSP afetado" no relatório e assegurar que as seguintes condições são preenchidas:

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

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

12.3. Limitar a comunicação de forma consolidada aos PSP estabelecidos em Portugal;

12.4. Fornecer uma lista de todos os PSP afetados pelo incidente;

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

12.6. Garantir que, sempre que existam campos no relatório 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 PSP afetado, identificando especificamente cada PSP a que a informação diz respeito, ou; (ii) à utilização de valores cumulativos, conforme observados ou estimados para os PSP.

12.7. O terceiro mantém o PSP informado, a todo o momento, de toda a informação relevante relativa ao incidente e de todas as interações que o mesmo possa ter com o Banco de Portugal, 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 PSP.

Texto alterado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

13. Política operacional e de segurança

Os PSP 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 do artigo 71º do RJSPME e da presente Instrução.

Aditado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.

IV – DISPOSIÇÕES FINAIS

14. Entrada em vigor

A presente instrução entra em vigor no dia da sua publicação.

Renumerado pela Instrução n.º 20/2021, publicada no BO n.º 12/2021, de 15 de dezembro.