BANCO DE PORTUGAL
EUROSISTEMA

Instrução n.º 21/2019

BO n.º 11/2019 Suplemento • 2019/11/25

Temas
Supervisão :: Elementos de Informação

Índice

Texto da Instrução

Assunto: Reporte de Incidentes de Cibersegurança

Atualmente, as entidades supervisionadas pelo Banco de Portugal devem reportar quaisquer situações com impacto no equilíbrio financeiro, nomeadamente eventos com potencial impacto negativo nos resultados ou capital próprio, incluindo incidentes de índole operacional. Num contexto de importância crescente do risco operacional associado às tecnologias de informação e comunicação, o Banco de Portugal considera que os incidentes de cibersegurança podem comprometer os sistemas e dados das entidades.

A presente Instrução tem como objeto regulamentar o reporte de incidentes de cibersegurança em entidades supervisionadas pelo Banco de Portugal e em instituições de crédito significativas com sede em Portugal supervisionadas pelo Banco Central Europeu (BCE).

No que respeita à comunicação ao BCE, por decisão interna e notificada às instituições de crédito significativas visadas, o BCE — nos termos dos artigos 10, n.º 1, alínea a) e 26, n.º 8 do Regulamento (UE) n.º 1024/2013 do Conselho, de 15 de outubro de 2013, que confere ao BCE atribuições específicas nas políticas relativas à supervisão prudencial das instituições de crédito — estabeleceu um reporte de incidentes de cibersegurança significativos ou severos suscetível de abranger as instituições de crédito em Portugal classificadas como significativas à luz do Regulamento (UE) n.º 468/2014 do BCE, de 16 de abril de 2014, que define o quadro de cooperação no âmbito do Mecanismo Único de Supervisão (MUS).

Adicionalmente, por decisão interna do Conselho de Supervisão do BCE, foi prevista a possibilidade de reporte indireto de incidentes de cibersegurança ao BCE, caso existisse uma sobreposição com disposições legais nacionais que implicasse uma duplicação de esforços.

Concomitantemente, algumas instituições de crédito em Portugal, incluindo instituições significativas, são também classificadas como Operadores de Serviços Essenciais (OSE) e devem notificar o Centro Nacional de Cibersegurança (CNCS) dos incidentes com impacto relevante na continuidade dos serviços essenciais, nos termos do artigo 17.º, da Lei n.º 46/2018, de 13 de agosto, que transpõe a Diretiva (UE) 2016/1148, do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União Europeia (i.e., Diretiva SRI – Segurança das Redes e Sistemas de Informação).

Na sequência do enquadramento supramencionado, entende-se necessário harmonizar os processos de reporte e agilizar a comunicação das entidades através de um ponto único de contacto que reencaminhará, se necessário e sem demora, a informação ao BCE e ao CNCS, consoante o âmbito e a natureza do incidente.

Ressalva-se que, atendendo ao 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), a Autoridade Bancária Europeia (EBA) publicou as "Orientações sobre a comunicação de incidentes de caráter severo ao abrigo da DSP2" (EBA/GL/2017/10), com data de entrada em vigor a 13 de janeiro de 2018. Para dar cumprimento a estas orientações, o Banco de Portugal emitiu a Carta Circular n.º CC/2018/00000015, de 26 de fevereiro de 2018, tendo o entendimento aí expresso sido substituído pela Instrução do Banco de Portugal n.º 1/2019, de 15 de Janeiro de 2019, que regulamenta o dever de reporte ao Banco de Portugal de incidentes de carácter severo relacionados com a prestação de serviços de pagamento ao abrigo da DSP2. Esta Instrução, aplicável aos Prestadores de Serviços de Pagamento registados e autorizados pelo Banco de Portugal, mantém-se em vigor, pelo que os respetivos incidentes devem continuar a ser reportados através de modelo de reporte e canal estabelecidos para o efeito.

Adicionalmente, a presente Instrução não prejudica o dever de comunicação pelas instituições à Comissão Nacional de Proteção de Dados (CNPD) de qualquer violação da proteção de dados em consequência do incidente de cibersegurança e suscetível de resultar num risco para os direitos e liberdades das pessoas singulares, em cumprimento do Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados (i.e., RGPD - Regulamento Geral de Proteção de Dados).

Assim, o Banco de Portugal, no uso das competências que lhe são conferidas pelo artigo 17.º da sua Lei Orgânica, aprovada pela Lei n.º 5/98, de 31 de janeiro, bem como pelos artigos 14.º, alíneas g) e h), 93.º, n.º 1, 115.º-T, 116.º-Z, 121.º-A, 133.º, 134.º e 196.º, n.º 1, todos do Regime Geral das Instituições de Crédito e Sociedades Financeiras (RGICSF), aprovado pelo Decreto-Lei n.º 298/92, de 31 de dezembro, bem como pelo artigo 60.º, n.º 3 do Decreto-Lei n.º 91/2018, de 12 de novembro, que aprova o novo Regime Jurídico dos Serviços de Pagamento e da Moeda Eletrónica (RJSPME), e em linha com a decisão interna do BCE acima referida, aprova a seguinte Instrução:

Artigo 1.º

Objeto e âmbito

1 – A presente Instrução regulamenta o dever de comunicação ao Banco de Portugal de incidentes de cibersegurança classificados como significativos ou severos.

2 – São considerados incidentes de cibersegurança todos os eventos de segurança de informação com probabilidade elevada de comprometer operações de negócio e/ou ameaçar a segurança da informação, designadamente eventos que:

a) impliquem um efeito adverso na segurança dos sistemas, aplicações ou redes;
b) comprometam a informação que estes sistemas, aplicações e redes processam, armazenam ou partilham;

c) infrinjam as políticas de segurança de informação e uso dos sistemas, aplicações ou redes das entidades.

3 – O dever de comunicação enunciado no número anterior deve ser cumprido pelas seguintes instituições, desde que exerçam a sua atividade em Portugal:

a) Instituições de Crédito;
b) Caixa Central de Crédito Agrícola Mútuo e Caixas de Crédito Agrícola Mútuo;
c) Empresas de Investimento;
d) Instituições de pagamento e instituições de moeda eletrónica;
e) Sucursais de instituições de crédito com sede no estrangeiro.

4 – Encontram-se abrangidas na alínea a) do número anterior as instituições de crédito classificadas como significativas nos termos do Regulamento (UE) n.º 1024/2013 do Conselho, de 15 de outubro de 2013, as quais devem reportar os incidentes significativos e severos ao Banco de Portugal, que encaminhará o reporte estabelecido para o efeito, de forma imediata e automática, ao BCE.

Artigo 2.º

Âmbito da informação a comunicar

1 – As instituições referidas nas alíneas a) a d) do número 3 do artigo anterior devem comunicar, em base consolidada, ao Banco de Portugal, no prazo de até 2 horas após a deteção do incidente, todos os incidentes de cibersegurança significativos ou severos ocorridos, ou que produzam efeitos, nas entidades incluídas no perímetro de supervisão, independentemente do local onde estas últimas prestam a sua atividade.

2 – As instituições referidas na alínea e) do número 3 do artigo anterior devem comunicar ao Banco de Portugal, em base individual, a ocorrência de incidentes de cibersegurança significativos ou severos que afetem, ou possam vir a afetar, a sua atividade exercida em território nacional.

Artigo 3.º

Classificação de incidentes de cibersegurança

1 – As entidades abrangidas pela presente Instrução (doravante designadas "entidades") devem classificar como significativos ou severos os incidentes de cibersegurança que preencham, pelo menos, um dos seguintes critérios de materialidade:

Critérios	**Significativo**	**Severo**
Utilizadores afetados	> 50 000 utilizadores **ou** > 25 % da base de clientes	-
Impacto económico	> 5 milhões EUR em custos diretos e indiretos **ou** > 0,1% dos fundos próprios* de nível 1	> 25 milhões EUR em custos diretos e indiretos **ou** > 0,5% dos fundos próprios* de nível 1

Critérios	Significativo	Severo
Impacto na reputação	✓	-
Ativação de mecanismos de gestão de crises	✓	-
Encaminhamento para instâncias internas superiores	✓	-
Incumprimentos legais ou regulamentares	✓	-
Notificação formal a autoridades competentes a nível nacional ou internacional	✓	-
Risco sistémico	✓	✓
Avaliação de especialista	✓	✓

** 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.*

2 – A avaliação de materialidade dos incidentes deve ser feita com base nos critérios e indicadores descritos acima, de natureza não cumulativa, atendendo às especificações constantes do artigo 4.º da presente Instrução.

Artigo 4.º

Especificações relativas a critérios e indicadores de materialidade

1 – Para determinar o número de utilizadores afetados, devem ser considerados todos os clientes – nacionais ou estrangeiros, particulares ou empresas – que possuam uma relação contratual com as entidades abrangidas pela presente Instrução a fim de aceder a um determinado serviço e que tenham sofrido ou possam vir a sofrer qualquer consequência negativa resultante da ocorrência do incidente de cibersegurança. No cálculo do número de utilizadores afetados, podem ser apresentadas estimativas baseadas na duração prevista do incidente e no histórico de atividade. As entidades devem ainda ter em conta o número total de utilizadores contratualmente vinculados no momento do incidente, independentemente de serem considerados utilizadores ativos ou passivos dos serviços afetados.

2 – Para o cálculo do potencial impacto económico, devem ser consideradas as perdas globais, diretas e indiretas, associadas à ocorrência do incidente de cibersegurança. As perdas globais devem ser avaliadas em termos absolutos ou, em alternativa, com base na importância relativa para a entidade (p. ex., através dos fundos próprios de nível 1). O cálculo das perdas indiretas deve considerar apenas os custos incorridos ou aqueles onde se possa demonstrar uma elevada probabilidade de virem a ocorrer.

3 – Para efeitos do disposto no número anterior, devem ser tidas em conta as perdas diretas resultantes da indisponibilidade do serviço e as perdas indiretas decorrentes da resolução do incidente, em particular, as seguintes:

i) custos resultantes da apropriação indevida de fundos e/ou ativos, bem como quaisquer perdas futuras decorrentes do incidente de cibersegurança;
ii) custos relacionados com a remediação e reposição da segurança dos sistemas (p. ex. contratação de equipas forenses, substituição de *software/hardware*, entre outros);
iii) custos judiciais e/ou associados à resolução de conflitos;
iv) taxas por incumprimento de obrigações contratuais e/ou possíveis sanções.

4 – O possível impacto na reputação deve ser tido em conta na avaliação de materialidade, considerando especificamente se:

i) o incidente teve cobertura mediática nacional e/ou internacional por parte de grandes jornais ou agências noticiosas, sejam tradicionais (p. ex. jornais) ou digitais (p. ex. blogues ou redes sociais) e/ou a cobertura mediática deu indicação de que a imprensa e, em geral, a opinião pública consideram que o incidente é suficientemente relevante para ser discutido;
ii) o incidente afetou sistemas, subcontratados externamente ou não, críticos para a confiança dos utilizadores, designadamente sistemas que possam comprometer dados pessoais ou dados financeiros dos utilizadores e/ou sistemas essenciais para a manutenção da estabilidade do mercado (p. ex. sistemas de pagamentos);
iii) existe possibilidade de incumprimento de requisitos regulamentares;
iv) foram ou podem vir a ser aplicadas sanções por autoridades competentes, em resultado de um incumprimento de regulação relativa a segurança dos sistemas, componentes e redes;
v) do incidente resultaram perdas de confidencialidade e integridade de dados sensíveis, nomeadamente dados de carácter pessoal;
vi) o tipo de incidente tem caráter recorrente.

5 – Devem ser classificados como significativos todos os incidentes que impliquem a ativação de mecanismos de gestão de crises, nomeadamente de:

i) planos de continuidade de negócio ou de recuperação de desastres;
ii) seguros ou outros instrumentos similares de cobertura de perdas relacionadas com o incidente;
iii) mecanismos ou procedimentos internos de resposta a crises, como planos de contingência, equipas ou comités de crise, comités de cibersegurança, entre outros.

6 – Devem ser classificados como significativos todos os incidentes que impliquem um processo de acompanhamento e/ou tomada de decisões por parte de instâncias internas relevantes, como sejam titulares de cargos de direção de topo que acompanhe o incidente, numa base continuada, durante o período da sua ocorrência e resolução, fora do âmbito de qualquer procedimento periódico de notificação (p. ex., Diretor de Sistemas de Informação, Diretor de Riscos ou outro cargo equivalente).

7 – Qualquer incidente de cibersegurança deve ser considerado significativo se resultar em incumprimentos legais ou regulamentares por parte da entidade afetada. Constituem motivos de incumprimento de obrigações legais, entre outros factos, os seguintes:

i) não cumprimento de prazos regulatórios, incluindo prazos de reporte de informação financeira;
ii) incapacidade de cumprir obrigações legais e contratuais perante os clientes ou consumidores do serviço (p. ex. pagamentos, transferências, execução de ordens de compra ou venda de títulos, entre outros);
iii) incumprimento de regulação em matéria de prevenção do branqueamento de capitais e do terrorismo;
iv) potencial risco jurídico associado a uma elevada probabilidade de ocorrerem litígios.

8 – Devem ser considerados significativos todos os incidentes que impliquem uma notificação formal do mesmo a autoridades competentes nacionais ou internacionais, nomeadamente a:

i) equipas de Resposta a Incidentes de Segurança Informática na União Europeia;
ii) autoridades nacionais de cibersegurança e de proteção de dados pessoais (CNCS e CNPD);
iii) órgãos de polícia, nacional ou internacional (p. ex. Polícia Judiciária ou Europol).

9 – Qualquer incidente de cibersegurança com potencial risco sistémico deve ser considerado significativo, em particular, sempre que:

i) exista possibilidade de efeito contágio a outras entidades (p. ex. falhas comuns de segurança em sistemas e/ou redes);
ii) coloque em causa a estabilidade do setor financeiro, com base na interdependência entre entidades;
iii) outra entidade for alvo do mesmo incidente de cibersegurança;
iv) o incidente expuser vulnerabilidades relevantes para o setor.

10 – Os incidentes podem ser considerados significativos ou severos com base na avaliação de um especialista da entidade, tendo em conta os critérios definidos no número 1 do artigo 3.º da presente Instrução e/ou eventuais critérios internos previamente estabelecidos pela entidade para avaliar se os incidentes representam um elevado risco de disrupção de serviços, de ocorrência de sanções legais ou regulatórias, de perda de reputação e/ou de possível impacto sistémico. Podem ainda ser considerados significativos ou severos todos os incidentes que recebam essa reclassificação por parte de um especialista do Banco de Portugal ou do BCE, mediante fundamentação adequada, tendo em conta os seguintes fatores:

i) eventuais falhas ou interrupções de funções críticas e/ou serviços essenciais;
ii) possível efeito de contágio;
iii) ocorrência de custos elevados e/ou imprevistos, que possam comprometer a continuidade da entidade.

11 – Na impossibilidade do incidente ser avaliado com base nos critérios e indicadores referidos nos artigos 3.º e 4.º da presente Instrução, ou em caso de dúvida, as entidades devem sempre comunicar o incidente ao Banco de Portugal.

Artigo 5.º

Canal de reporte

1 – As entidades devem comunicar ao Banco de Portugal os incidentes classificados como significativos ou severos através do Portal BP*net* (www.bportugal.net) via Área de Supervisão Prudencial através do serviço "*Reporte de Incidentes de Cibersegurança*", mediante o preenchimento do modelo de reporte estabelecido para o efeito.

2 – As instituições de crédito significativas devem preencher o reporte em língua inglesa e as restantes entidades devem fazê-lo em língua portuguesa.

3 – Nos casos em que a entidade não tem temporariamente capacidade operacional para assegurar a comunicação do incidente no Portal BP*net*, ou nos casos em que o mesmo esteja indisponível, em resultado do incidente ou por outro motivo de natureza eminentemente técnica (devidamente justificado), o reporte poderá ser efetuado, a título excecional, através de correio eletrónico remetido para o seguinte endereço: csirt_report@bportugal.pt, preenchendo e juntando o ficheiro Excel disponível no Portal BP*net*, que deve ser descarregado após a publicação da presente Instrução.

Artigo 6.º
Forma de reporte

1 – As entidades devem recolher a informação possível sobre o incidente, com o objetivo de preencher, numa base de melhor esforço, os campos de informação requeridos no reporte, nomeadamente de acordo com as instruções de preenchimento que constam do manual técnico disponível no Portal BP*net*.

2 – As entidades podem enviar, de forma voluntária, qualquer documentação relevante que sirva de suporte ao reporte de incidente e que facilite o acompanhamento do incidente por parte do supervisor, nomeadamente informação com maior detalhe sobre a arquitetura dos sistemas afetados, o impacto provável do incidente, medidas mitigadoras adotadas e/ou previstas ou outros documentos equivalentes que sejam relevantes. A documentação deverá ser enviada para o Banco de Portugal, sob a forma de um ou vários anexos, através de correio eletrónico remetido para o seguinte endereço: csirt_report@bportugal.pt. O correio eletrónico deve mencionar explicitamente o ID do incidente reportado ao abrigo da presente Instrução, sendo que quaisquer dados pessoais e/ou financeiros de utilizadores afetados que constem nos anexos deverão ser enviados de forma anonimizada.

3 – Nos casos em que os incidentes sejam classificados como significativos ou severos, o Banco de Portugal e/ou o BCE podem acompanhar a resolução do incidente e solicitar, se necessário, informação adicional.

Artigo 7.º
Modelo de reporte

1 – O reporte de incidentes divide-se em três secções – inicial, intercalar e final – que devem ser preenchidas, de forma incremental e sequencial, numa base de melhor esforço.

2 – As entidades devem submeter o reporte inicial ao Banco de Portugal no prazo de até 2 horas após a deteção do incidente. O reporte inicial deve incluir informação de caráter geral sobre o incidente, descrevendo as suas principais características assim como possíveis consequências e eventual impacto transfronteiriço. Na impossibilidade de apresentar dados reais, as entidades devem recorrer a estimativas baseadas na melhor informação disponível.

3 – Seguidamente, compete às entidades enviar um reporte intercalar num prazo que, em circunstância alguma, deverá exceder os 10 dias úteis após o envio do reporte inicial. O reporte intercalar deve conter informação detalhada sobre o tipo de incidente e o seu impacto.

4 – Por último, as entidades devem submeter um reporte final no prazo de até 30 dias úteis após o reporte inicial. O reporte final deve refletir a informação recolhida na investigação interna das causas do incidente, bem como potenciais medidas mitigadoras adotadas ou previstas para resolver o

incidente e evitar a sua recorrência no futuro. Este reporte deve incluir i) valores reais sobre o impacto do incidente, substituindo eventuais estimativas em reportes anteriores e ii) uma descrição, clara e rigorosa, das medidas mitigadoras adotadas ou previstas.

5 – Na eventualidade do incidente não ficar inteiramente resolvido no prazo de 30 dias úteis após o reporte inicial, as entidades devem ainda assim submeter o reporte final ao Banco de Portugal no prazo estipulado para o efeito. Posteriormente, as entidades devem comunicar ao Banco de Portugal (csirt_report@bportugal.pt) – explicitando o ID do incidente – qualquer informação adicional relevante sobre o incidente que possa ter implicações para o relatório final submetido anteriormente.

6 – Todos os campos de informação no reporte são de preenchimento obrigatório. As entidades podem optar por preencher qualquer campo de informação antes dos prazos fixados para o efeito, desde que disponham de informação fiável e rigorosa para o fazer. Nos casos em que o incidente seja resolvido de forma imediata, nas primeiras 2 horas após a sua deteção, as entidades podem enviar diretamente o reporte final com todos os campos de informação devidamente preenchidos, ficando dispensadas do envio dos restantes modelos de reporte.

7 – As entidades são responsáveis por avaliar eventuais alterações ao estado do incidente, quer sejam no sentido do seu agravamento (p. ex. de "não significativo" para "significativo" ou "severo") ou desagravamento (p. ex. de "significativo" para "não significativo" ou "não de cibersegurança"). As entidades devem reportar ao Banco de Portugal, de forma imediata, num prazo máximo de 1 dia útil, qualquer incidente inicialmente classificado como "não significativo" e posteriormente reclassificado como "significativo" ou "severo", devendo justificar, detalhadamente, as causas para o agravamento da sua classificação no campo de descrição do incidente.

8 – As entidades devem ainda informar o Banco de Portugal de qualquer incidente de cibersegurança "significativo" ou "severo" que seja reclassificado como "não significativo" ou "não de cibersegurança", assinalando os campos de informação estabelecidos para o efeito no modelo de reporte. Nestes casos, deixa de ser obrigatório o preenchimento integral do modelo de reporte, com exceção das caixas que assinalam a reclassificação do incidente e do campo de descrição do incidente que deverá apresentar uma justificação da entidade para o desagravamento da classificação do incidente.

Artigo 8.º

Entrada em vigor e disposição final

1 – A presente Instrução entra em vigor 30 dias úteis a partir da data da sua publicação.

2 – A Instrução do Banco de Portugal n.º 1/2019, de 15 de janeiro de 2019, mantém-se em vigor, pelo que o cumprimento das obrigações de comunicação constantes da presente Instrução não isentam as entidades de apresentar os reportes exigidos por aquela Instrução, quando aplicáveis.