BANCO DE PORTUGAL
EUROSISTEMA

Projeto de Instrução

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). São considerados incidentes de cibersegurança todos os eventos que tenham um efeito adverso na segurança dos sistemas, aplicações ou redes; que comprometam a informação que estes sistemas, aplicações e redes processam, armazenam ou partilham; e/ou que infrinjam as políticas de segurança de informação e uso dos sistemas, aplicações ou redes das entidades.

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).

Antes da referida decisão, 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 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 normativo 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.º1, 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, 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 – 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) Empresas de Investimento;
c) Instituições de pagamento e instituições de moeda eletrónica;
d) Sucursais de instituições de crédito com sede no estrangeiro.

3 – 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 c) do número dois 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 cibernéticos 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 d) do número dois do artigo anterior devem comunicar ao Banco de Portugal, em base individual, a ocorrência de incidentes cibernéticos 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
Impacto na reputação	Sim	-

Critérios	Significativo	Severo
Ativação de mecanismos de gestão de crises	Sim	-
Encaminhamento para instâncias internas superiores	Sim	-
Incumprimentos legais ou regulamentares	Sim	-
Comunicação a Equipa de Resposta a Incidentes de Segurança Informática Nacional (CERT.PT), agência de segurança ou polícia	Sim	-
Risco sistémico	Sim	-
Avaliação de especialista	Sim	-

** 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 envolveu uma área de negócio (subcontratada externamente ou não) crítica para a confiança dos consumidores ou clientes e/ou é significativa em termos de dimensão;
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 gestão e/ou direção. Neste contexto, entende-se como cargo relevante de gestão e/ou direção o responsável de qualquer função 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 comunicação formal do mesmo a autoridades competentes, 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 (p. ex. 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 – Podem ainda ser considerados significativos ou severos todos os incidentes que recebam essa reclassificação por parte 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 comunicação

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: supervisao.prudencial@bportugal.pt, preenchendo e juntando o ficheiro Excel constante do anexo.

Artigo 6.º

Forma de comunicação

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 informação adicional relevante para o Banco de Portugal, sob a forma de um ou vários anexos, carregando os ficheiros no serviço "Reporte de Incidentes de Cibersegurança". Os dados pessoais de clientes e/ou utilizadores afetados que constem nos anexos devem ser enviados de forma anonimizada.

3 – As entidades devem dar reposta a qualquer pedido de informação adicional por parte do Banco de Portugal sobre os incidentes de cibersegurança reportados.

Artigo 7.º

Modelo de comunicação

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, preenchendo para o efeito os campos de informação assinalados com a cor vermelha no modelo de reporte. 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, preenchendo os campos de informação assinalados com a cor azul no modelo de reporte. 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, preenchendo para o efeito os campos de informação assinalados com a cor verde no modelo de reporte. 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 ou ao BCE qualquer informação adicional relevante sobre o incidente que possa ter implicações para o relatório final que foi 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 podem enviar ao Banco de Portugal, de forma voluntária, qualquer documentação relevante que sirva de suporte ao reporte de incidentes 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.

8 – 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 cibsergurança”). 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.

9 – 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.

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

Artigo 8.º

Entrada em vigor e disposição final

1 – A presente Instrução entra em vigor no dia seguinte ao 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.

BANCO DE PORTUGAL
EUROSISTEMA

Anexo – Modelo de reporte

Os campos obrigatórios para cada tipo de reporte estão identificados nas cores seguintes

Reporte inicial	☐	até 2 horas
Reporte intercalar	☐	até 10 dias úteis após o reporte inicial
Reporte final	☐	até 30 dias úteis após o reporte inicial

Data do reporte

ID do incidente (para reportes intercalares ou finais)

Incidente reclassificado como não significativo ☐

Incidente reclassificado como não de cibersegurança ☐

Reporte de Incidentes Cibernéticos

	Código JST (se aplicável)					
	Nome da entidade afetada					
	Tipo de entidade afetada					
	País da entidade afetada (escolher da lista)					
	Pessoa de contacto na entidade para atualizações		Email		Telefone	
	Segunda pessoa de contacto na entidade para atualizações		Email		Telefone	
	Data de deteção do incidente					

	DESCRIÇÃO DO INCIDENTE	
	Reporte inicial Solicita-se uma descrição geral do incidente	
	Reporte intercalar Solicita-se uma descrição detalhada do incidente. Incluir informação (se conhecida e/ou aplicável): - Contexto da deteção de incidente, quem esteve envolvido, o que aconteceu, como o incidente foi detetado - Atacante(s), causa do incidente - Sistemas/áreas afetados e impacto - Canais afetados - Especificar se houve terceiras partes/ fornecedores afetados (nome do fornecedor afetado, como foi afetado) e qual o impacto sobre a entidade supervisionada	
	Reporte final Solicita-se informação atualizada relativamente ao Reporte Intercalar e mais detalhes de: - Vulnerabilidades técnicas exploráveis (indicar número CVE, se conhecido) - Vetor de entrada - Escalamento interno/ gestão de crises / ações relevantes tomadas - A investigação (partes externas envolvidas) - Ações de remediação tidas - Controlos de segurança adicionais aplicados como resultado do incidente - Lições aprendidas - Análise da causa raiz - Outras informações relevantes	

BANCO DE PORTUGAL
EUROSISTEMA

INFORMAÇÃO SOBRE O INCIDENTE					
Tipo de incidente (possível múltiplas seleções)	**Malware** ☐	**Engenharia Social** ☐	**Segurança da informação** ☐	**Intrusão/Tentativa de Intrusão** ☐	**Ataque à Disponibilidade do serviço** ☐
	Ransomware ☐	*Phishing / *ishing* ☐	Corrompimento/ fuga de dados acidental ☐	Ataque de *brute force* ☐	
	Trojan horse ☐	*Spear phishing* ☐	Utilização indevida de credenciais de acesso por interno ☐	Injeção de script malicioso e/ou comando SO ☐	**Outro** ☐
	Virus/worm ☐	*Pretexting* ☐	Utilização indevida de credenciais de acesso por fornecedor ☐	Exploração de outra vulnerabilidade ☐	
	Mobile malware ☐	Outra engenharia social ☐			
	Se outro, pf especificar:				
	Informação adicional:				
	Malware ☐	**Recolha de informação** ☐	**Fraude** ☐	**Intrusão/Tentativa de Intrusão** ☐	**Conteúdo abusivo** ☐
	Infeção ☐	*Scan* ☐	Utilização indevida ou não autorizada de recursos ☐	Comprometimento de conta ☐	SPAM ☐
	Distribuição ☐	*Sniffing* ☐	Utilização ilegítima de nome de terceiros ☐	Tentativa de login ☐	Direitos de autor ☐
	Command & Control ☐				Pornografia infantil, racismo, apologia da violência ☐
	Indeterminado ☐				
	Incidente classificado como *APS (Advanced Persistent Threat)*? ○ Sim ○ Não				
Incidente descoberto por	Segurança TI ☐		Auditor externo ☐		Atacante (aviso) ☐
	Empregado interno ☐		Fornecedor externo ☐		Outro ☐
	Auditoria interna ☐		Cliente ☐		
	Se outro, pf especificar:				
Informação sobre o(s) atacante(s)	Terroristas ☐		Hacktivistas ☐		Desconhecidos ☐
	Hackers com patrocínio de estados ☐		Empregados internos ☐		Outros ☐
	Outros hackers ☐				
	Se outro, pf especificar:				

BANCO DE PORTUGAL
EUROSISTEMA

IMPACTO DO INCIDENTE & RAZÃO DO REPORTE			
Impacto do incidente (possível múltiplas seleções)	**Fuga de informação** ☐ Fuga de informação relacionada com a instituição? ☐ Fuga de informação sensível de clientes? ☐ Disrupção de serviço crítico? ☐ Se sim, horas de disrupção: Fornecedor externo afetado? ☐ ATMs afetadas? ☐ Fraude em banca online? ☐ Houve perdas financeiras diretas ou indirectas? ☐ Perdas financeiras diretas em euros Perdas financeiras indiretas estimadas em euros Outros impactos ☐ Se outro, pf especificar:	Verificou-se a quebra de requisitos legais ou regulatórios ☐ Se sim, pf indicar	Verificou-se alguma cobertura mediática? ☐ Se sim, pf especifique os media/jornais/blogs que abordaram o tópico
Razão para o reporte do incidente (possível múltiplas seleções)	Incidente reportado publicamente e/ou com potencial impacto reputacional significativo ☐ O impacto financeiro estimado é acima de EUR 5 milhões de euros ou 0,1% do capital CET1 ☐ O incidente foi escalado internamente até ao *Chief Information Officer* (ou equivalente) fora do circuito normal de reporte ☐ É previsível que o incidente conduza a quebras de obrigações legais ou regulatórias ☐	Desencadeados procedimentos de gestão de crises (incluindo ciber) ☐ O incidente foi reportado ao CERT/CSIRT nacional, polícia ou agência de segurança ☐ O incidente pode afetar outras instituições/ organizações (impacto sistémico) ☐ A análise de significância não leva a conclusões claras, pelo que se procede ao reporte do incidente ☐	
Serviços e componentes afetados (possível múltiplas seleções)	Estações de trabalho/ clientes *(laptops, PCs, OSs, user applications, etc)* ☐ Aplicações empresariais (SAP, Oracle, etc) ☐ Outros ☐ Se outros, pf especificar:	Aplicações cliente/ software relacionadas com banca (vendas, transacionais, crédito, risco, etc) ☐ Plataformas internet *(webservers, application servers, etc)* ☐	Redes e telecomunicações *(firewalls, routers, switches, PBX, etc)* ☐ Gestão e armazenamento de dados *(fileservers, databases, data warehouses, etc)* ☐
Áreas de negócio afetadas (possível múltiplas seleções)	Finanças Corporativas ☐ Banca Comercial ☐ Gestão de Ativos ☐ Se outros, pf especificar:	Vendas e trading ☐ Pagamentos e Contabilidade ☐ Corretagem de Retalho ☐	Banca de Retalho ☐ Serviços de Agências ☐ Outros ☐

BANCO DE PORTUGAL
EUROSISTEMA

INVESTIGAÇÃO E RESOLUÇÃO DO INCIDENTE				
O incidente foi escalado internamente para a gestão de topo, ao nível de grupo, para ações fora dos procedimentos habituais? Ao nível de grupo CIO, CISO, COO, CRO, CEO, Membros do conselho de administração, etc.	Escalamento: ○ Sim ○ Não			
	Se Sim, pf especificar:			
Foi ativado um Plano de Continuidade de Negócio?	Ativação de PCN: ○ Sim ○ Não			
Foi ativado um Plano de Recuperação de Desastre?	Ativação de PRD: ○ Sim ○ Não			
Foram ativados procedimentos de Gestão de Crise?	Ativação de GC: ○ Sim ○ Não			
Quem lidera a investigação ao incidente?	Investigação: ○ Grupo ○ Entidade afetada ○ Outro			
A polícia ou outras agências de segurança estão envolvidas na investigação?	Polícia: ○ Polícia ○ Outro ○ Não			
Quem lidera as ações de remediação?	Remediação: ○ Grupo ○ Entidade afetada ○ Outro			
É conhecida a data a partir da qual a entidade foi afetada?	Data em que entidade foi afetada: ○ Sim ○ Não			
	Se Sim, pf indicar a data			
O incidente encontra-se resolvido? Se não, para quando é expectável a sua resolução?	Resolução: ○ Sim ○ Não			
	Se Não, pf indicar a data			
Qual foi o vetor de entrada do incidente? (possível múltiplas seleções)	Website ☐	E-mail ☐	Dispositivos perdidos/ roubados ☐	
	Mensagens instantâneas ☐	Rede de terceiros ☐	Redes sociais/ salas de *chat* ☐	
	Telefone ☐	Dispositivos não autorizados ☐	Outro ☐	
	Abuso de privilégios administrativos ☐			
	Se outros, pf especificar:			
Vulnerabilidades/ fraquezas expostas (possível múltiplas seleções)	Gestão inadequada de patching ☐	Configurações inadequadas de segurança sobre hardware e software em equipamentos ☐	Controlos de segurança de software aplicacional desadequados ☐	
	Software não autorizado/ versão errada ☐	Defesas de perímetro inadequadas ☐	Defesas desadequadas contra DDoS ☐	
	Gestão inadequada de privilégios de conta ☐	Controlo inadequado sobre portos, protocolos e serviços de rede ☐	Testes de segurança e penetração desadequados ☐	
	Proteção inadequada de email/ browser web ☐	Resiliência e/ou back-ups inadequados de sistemas ou ficheiros ☐	Segmentação de rede desadequada ☐	
	Defesas inadequadas de malware ☐	Dispositivos de rede inseguros (*firewalls*, *routers*, *switches*) ☐	Lacunas ao nível de *compliance* e sensibilização de empregados ☐	
	Gestão inadequada de identidade para acessos ☐	Gestão e monitorização inadequados de logs ☐	Outro ☐	
	Se outros, pf especificar:			

BANCO DE PORTUGAL
EUROSISTEMA

The mandatory fields for each report are marked in the following colours

First report	☐	within 2 hours
Interim report	☐	within 10 working days of the first report
Final report	☐	within 30 working days of the first report

Report date

Incident ID (for interim or final report)

Incident reclassified as non-significant ☐

Incident reclassified as non-cyber ☐

Cyber incident report

JST code (if applicable)						
Name of entity affected						
Type of entity affected						
Country of entity affected (choose from the list)						
Contact person within the institution for updates		Email		Phone		
Second contact person within the institution for updates		Email		Phone		
Incident detection date						

DESCRIPTION OF THE INCIDENT

First report Please provide a general description of the incident	
Interim report Please provide a detailed description of the incident. Include information (if known and/or applicable) -Background to incident detection, who was involved, what happened, how the incident was discovered -Attacker(s), cause of the incident -Affected areas/systems and impact -Channels affected -Specify whether a third party/outsourced provider was affected (name of the provider affected, how it was affected) and how the supervised entity was impacted	
Final report Please update the information from the interim report and add details of: -Technical vulnerability exploited (provide CVE number if known) -Entry vector -Internal escalation / crisis management / relevant actions taken -The investigation (external parties involved) -Remediation actions taken -Additional security controls applied as a result of the incident -Lessons learned -Root cause analysis -Any other relevant information	

BANCO DE PORTUGAL
EUROSISTEMA

INFORMATION ON THE INCIDENT

Incident type
multiple selections possible

Malware ☐	**Social engineering** ☐	**Insider/Third Party Provider Threat** ☐	**Unauthorised access** ☐	**Denial of service** ☐
Ransomware ☐	Phishing / *ishing ☐	Accidental data leakage/corruption ☐	Brute force attack ☐	
Trojan horse ☐	Spear phishing ☐	Intentional misuse of access rights by insider ☐	Malicious script injection and/or OS commanding ☐	**Other** ☐
Virus/worm ☐	Pretexting ☐	Intentional misuse of access rights by service provider ☐	Other exploited Vulnerability ☐	
Mobile malware ☐	Other social engineering ☐			
If Other, please specify:				

Additional information:

Malware ☐	**Collection of information** ☐	**Fraud** ☐	**Unauthorised access** ☐	**Abusive content** ☐
Infection ☐	Scan ☐	Unauthorised or improper use of resources ☐	Account compromised ☐	SPAM ☐
Distribution ☐	Sniffing ☐	Illegitimate use of someone's name ☐	Login attempt ☐	Copyright ☐
Command & Control ☐				Child pornography, racism and violence apology ☐
Not identified ☐				

Incident classified as an Advanced Persistent Threat? ○ Yes ○ No

Incident discovered by

IT security ☐	External auditor ☐	Attacker (warning) ☐
Staff member ☐	Third party provider ☐	Other ☐
Internal Audit ☐	Customer ☐	
If Other, please specify:		

Information regarding the attacker(s)

Terrorists ☐	Hacktivists ☐	Unknown ☐
Foreign agencies - state-sponsored hackers ☐	Inside job/Unaware employee ☐	Other ☐
Other hackers (e.g. criminals, script kiddies, etc) ☐		
If Other, please specify:		

BANCO DE PORTUGAL
EUROSISTEMA

IMPACT OF THE INCIDENT & REASON FOR REPORTING

Impact of the incident
multiple selections possible

- ☐ **Unauthorised release of information?**
- ☐ Information related to the institution leaked?
- ☐ Sensitive client information leaked?
- ☐ Disruption of critical service?
  - If yes, hours of disruption:
- ☐ Third party provider affected?
- ☐ ATMs affected?
- ☐ Online banking fraud?
- ☐ Direct or indirect financial loss?
  - Direct financial loss in euros
  - Estimated indirect financial loss in euros
- ☐ Other impact
  - If Other, please specify:

- ☐ Were any legal or regulatory requirements breached?
  - If yes, please specify
- ☐ Was there any media coverage?
  - If yes, please specify the media/newspapers/blogs that covered the topic

Reason for reporting the incident
multiple selections possible

- ☐ Incident publicly reported and/or can cause significant reputational damage
- ☐ The estimated financial impact is above EUR 5 million euros or 0.1% of CET1 capital
- ☐ Incident was internally escalated up to the Chief Information Officer (or equivalent) outside of regular reporting
- ☐ Incident is likely to lead to breaches of legal or regulatory obligation
- ☐ Crisis management procedures triggered (including cyber insurance)
- ☐ Incident was reported to the national CERT/CSIRT, security agency or police
- ☐ Incident may affect other institutions/organisations (systemic impact)
- ☐ The significance assessment does not lead to a clear outcome so the incident is reported

Services and components affected
multiple selections possible

- ☐ Endpoints/clients (laptops, PCs, OSs, user applications, etc)
- ☐ Enterprise software applications (SAP, Oracle, etc)
- ☐ Other
  - If Other, please specify:
- ☐ Banking-related user applications/software (sales, trading, credit, risk, etc)
- ☐ Internet platforms (webservers, application servers, etc)
- ☐ Networking and telecommunications (firewalls, routers, switches, PBX, etc)
- ☐ Data management and storage (fileservers, databases, data warehouses, etc)

Business lines affected
multiple selections possible

- ☐ Corporate Finance
- ☐ Commercial Banking
- ☐ Asset Management
- ☐ Trading & Sales
- ☐ Payment & Settlement
- ☐ Retail Brokerage
- ☐ Retail Banking
- ☐ Agency Services
- ☐ Other
  - If Other, please specify:

BANCO DE PORTUGAL
EUROSISTEMA

INVESTIGATION AND RESOLUTION OF THE INCIDENT

Was the incident escalated internally to senior (top) management at group level for action outside of day-to-day procedures? At group level CIO, CISO, COO, CRO, CEO, ExCo, ExBoard	Escalation: ○ Yes ○ No If Yes, please specify:
Was a business continuity plan activated?	BCP activated: ○ Yes ○ No
Was a disaster recovery plan activated?	DRP activated: ○ Yes ○ No
Were crisis management procedures activated?	CM activated: ○ Yes ○ No
Who is leading the investigation of the incident?	Investigation: ○ Group ○ Affected entity ○ Other
Are the police or other security agencies involved in the investigation?	Police: ○ Police ○ Other ○ None
Who is leading the remediation actions?	Remediation: ○ Group ○ Affected entity ○ Other
Is the date from which the entity was affected known?	Date incident affected entity: ○ Yes ○ No If Yes, please enter the date
Is the incident resolved? If not, by when do you expect to resolve the incident?	Resolution: ○ Yes ○ No If No, please enter the date
What was the entry vector of the incident? multiple selections possible	☐ Website ☐ E-mail ☐ Lost / stolen devices ☐ Instant messaging ☐ Third party network ☐ Chat rooms / social media ☐ Phone ☐ Unauthorised devices ☐ Other ☐ Abuse of Administrative Privileges If Other, please specify:
Vulnerabilities/weaknesses exposed multiple selections possible	☐ Inadequate patch management ☐ Inadequate security configurations for secure hardware and software on devices, laptops, workstations, servers ☐ Inadequate application software security controls (web-based and other applications) ☐ Unauthorised software/wrong version ☐ Inadequate boundary defences ☐ Inadequate DDoS defences ☐ Inadequate privileged account management ☐ Inadequate control of network ports, protocols and services ☐ Inadequate penetration and security testing ☐ Inadequate email/web browser protection ☐ Inadequate resilience and/or back-up of systems or files ☐ Inadequate network segmentation ☐ Inadequate malware defences ☐ Unsecured network devices (firewalls, routers, switches) ☐ Lack of staff awareness and/or compliance ☐ Inadequate identity access management ☐ Inadequate maintenance and monitoring of logs ☐ Other If Other, please specify: