

3.º Suplemento
Boletim Oficial

6 | 2019



BANCO DE
PORTUGAL
EUROSISTEMA

BOLETIM OFICIAL DO BANCO DE PORTUGAL

6 | 2019 3.º SUPLEMENTO



8 julho 2019 • www.bportugal.pt • Legislação e Normas • SIBAP

Índice

Apresentação

CONSULTAS PÚBLICAS

Consulta Pública n.º 2/2019 – Projeto de Instrução relativo ao reporte de incidentes de cibersegurança

Apresentação

O *Boletim Oficial* do Banco de Portugal, previsto no n.º 3 do artigo 59.º da sua Lei Orgânica, em formato eletrónico a partir de janeiro de 2012, tem como objetivo divulgar os diplomas normativos designados por Instruções, produzidos no exercício da sua competência regulamentar.

Acessoriamente, esta publicação reúne e disponibiliza os Avisos do Banco de Portugal (sempre publicados no *Diário da República*), as Cartas Circulares tidas como relevantes, bem como outras informações.

A sua periodicidade é mensal, sendo disponibilizado ao dia 15 de cada mês ou no primeiro dia útil seguinte, em www.bportugal.pt. Excepcionalmente serão publicados suplementos sempre que o carácter urgente, quer de Instruções, quer de outros atos que por lei devam ser publicados, o justifique.

Para além do *Boletim Oficial*, o Banco de Portugal disponibiliza um *Manual de Instruções*, constituído pela totalidade das Instruções em vigor, consultável em Legislação e Normas – SIBAP.

O *Boletim Oficial* eletrónico contém:

- **Instruções**

Atos regulamentares do Banco de Portugal designados por Instruções, numeradas sequencialmente dentro do ano

a que respeitam, classificadas tematicamente.

- **Avisos do Banco de Portugal**

Publicados em *Diário da República*.

- **Cartas Circulares**

Emitidas pelo Banco de Portugal e que, apesar do seu conteúdo não normativo, se entende dever ser objeto de divulgação alargada.

- **Informações**

Selecionadas e cujo conteúdo justifica a sua inclusão no Boletim, numa perspetiva de compilação e difusão mais generalizada, designadamente:

- Comunicados do Banco de Portugal e do Banco Central Europeu;
- Lista das Instituições de Crédito, Sociedades Financeiras, Instituições de Pagamento e Instituições de Moeda Eletrónica registadas no Banco de Portugal;
- Seleção de referências e resumos de legislação nacional e comunitária respeitante a matérias que se relacionam com a atividade das Instituições sujeitas à supervisão do Banco de Portugal.





CONSULTAS PÚBLICAS



Consulta Pública do Banco de Portugal n.º 2/2019

Projeto de Instrução relativo ao Reporte de Incidentes de Cibersegurança

O Banco de Portugal submete a Consulta Pública até 19 de agosto de 2019, um projeto de instrução relativo ao reporte de incidentes de cibersegurança.

Enquadramento

As entidades supervisionadas pelo Banco de Portugal devem reportar qualquer situação com impacto negativo nos resultados ou capital próprio, incluindo eventos de índole operacional. Por seu lado, as instituições de crédito classificadas como significativas e com sede em Portugal reportam diretamente ao Banco Central Europeu (BCE), nos termos do Regulamento (UE) n.º 468/2014 do BCE, de 16 de abril de 2014, os incidentes de cibersegurança.

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 BCE. Assim, e no que respeita a estas últimas, o reporte dos aludidos incidentes passa a ser feito ao Banco de Portugal via Portal *BPnet*, mediante o preenchimento de um modelo de reporte estabelecido para o efeito que será reencaminhado automaticamente ao BCE. Adicionalmente, este reporte será enviado também ao Centro Nacional de Cibersegurança (CNCS), nos termos da Lei n.º 46/2018, de 13 de agosto, sempre que a entidade estiver classificada como Operador de Serviços Essenciais (OSE).

Nos termos desta Instrução, 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.

Resumidamente, este instrumento regulamentar visa:

- Estabelecer o dever de comunicação de incidentes de cibersegurança significativos ou severos em entidades supervisionadas pelo Banco de Portugal e pelo BCE;
- Harmonizar os diferentes reportes de incidentes de cibersegurança do Banco de Portugal, BCE e CNCS, através da implementação de um modelo de reporte único, com uma taxonomia e terminologia comuns, por forma a reduzir a multiplicidade de reportes e consequente sobreposição de esforços;
- Centralizar a comunicação dos incidentes de cibersegurança num ponto único de contacto, no Portal *BPnet* (www.bportugal.net), via Área de Supervisão Prudencial, no serviço “*Reporte de Incidentes de Cibersegurança*”, que reencaminhará os reportes de forma automática e imediata ao BCE e/ou CNCS quando aplicável.



BANCO DE PORTUGAL
EUROSISTEMA

Cabe notar que a presente proposta da Instrução não preclude o reporte de incidentes de carácter severo relativo à prestação de serviços de pagamento, regulamentado na Instrução do Banco de Portugal n.º 1/2019, a qual se mantém em vigor, nem o reporte à Comissão Nacional de Proteção de Dados sempre que o incidente de cibersegurança resultar numa violação da proteção dos dados de pessoas singulares, ao abrigo do Regulamento Geral de Proteção de Dados.

Resposta à consulta pública

Os contributos para esta consulta pública devem ser apresentados através do preenchimento do ficheiro *Excel* disponível nesta página *web* e remetidos até 19 de agosto de 2019, para o endereço de correio eletrónico: consultas.publicas.dsp@bportugal.pt.

Para a colocação de questões deverá ser utilizado o referido endereço de correio eletrónico.

Ressalva-se que o Banco de Portugal poderá publicar os contributos recebidos ao abrigo desta consulta pública, devendo os respondentes que se oponham à publicação da sua comunicação – integral ou parcial – assinalar o campo indicado para o efeito no contributo enviado.



Projeto de Instrução

Índice

Texto da Instrução

Anexo – Modelo de reporte

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 carácter 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 carácter 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 BPnet (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 *BPnet*, 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 *BPnet*.

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 resposta 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 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.

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,



BANCO DE PORTUGAL
EUROSISTEMA

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 desagramento 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.



Anexo – Modelo de reporte

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

Reporte inicial	<input type="checkbox"/>	até 2 horas
Reporte intercalar	<input type="checkbox"/>	até 10 dias úteis após o reporte inicial
Reporte final	<input type="checkbox"/>	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)	<input type="text"/>	<input type="text"/>
Nome da entidade afetada	<input type="text"/>	
Tipo de entidade afetada	<input type="text"/>	<input type="text"/>
País da entidade afetada (escolher da lista)	<input type="text"/>	<input type="text"/>
Pessoa de contacto na entidade para atualizações	<input type="text"/>	Email <input type="text"/> Telefone <input type="text"/>
Segunda pessoa de contacto na entidade para atualizações	<input type="text"/>	Email <input type="text"/> Telefone <input type="text"/>
Data de deteção do incidente	<input type="text"/>	<input type="text"/>

DESCRIÇÃO DO INCIDENTE

<p>Reporte inicial</p> <p>Solicita-se uma descrição geral do incidente</p>	<input type="text"/>
<p>Reporte intercalar</p> <p>Solicita-se uma descrição detalhada do incidente. Incluir informação (se conhecida e/ou aplicável):</p> <ul style="list-style-type: none"> - 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 terceiros partes/ fornecedores afetados (nome do fornecedor afetado, como foi afetado) e qual o impacto sobre a entidade supervisionada 	<input type="text"/>
<p>Reporte final</p> <p>Solicita-se informação atualizada relativamente ao Reporte Intercalar e mais detalhes de:</p> <ul style="list-style-type: none"> - Vulnerabilidades técnicas exploráveis (indicar número CVE, se conhecido) - Vetor de entrada - Escalamento interno/ gestão de crises / acções relevantes tomadas - A investigação (partes externas envolvidas) - Acções de remediação tidas - Controlos de segurança adicionais aplicados como resultado do incidente - Lições aprendidas - Análise da causa raiz - Outras informações relevantes 	<input type="text"/>



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



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



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



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

First report	<input type="checkbox"/>	within 2 hours
Interim report	<input type="checkbox"/>	within 10 working days of the first report
Final report	<input type="checkbox"/>	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)	<input type="text"/>				
Name of entity affected	<input type="text"/>				
Type of entity affected	<input type="text"/>				
Country of entity affected (choose from the list)	<input type="text"/>				
Contact person within the institution for updates	<input type="text"/>	Email	<input type="text"/>	Phone	<input type="text"/>
Second contact person within the institution for updates	<input type="text"/>	Email	<input type="text"/>	Phone	<input type="text"/>
Incident detection date	<input type="text"/>				

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



INFORMATION ON THE INCIDENT																										
Incident type multiple selections possible	<table border="1"> <tr> <td>Malware <input type="checkbox"/></td> <td>Social engineering <input type="checkbox"/></td> <td>Insider/Third Party Provider Threat <input type="checkbox"/></td> <td>Unauthorised access <input type="checkbox"/></td> <td>Denial of service <input type="checkbox"/></td> </tr> <tr> <td>Ransomware <input type="checkbox"/></td> <td>Phishing / 'ishing <input type="checkbox"/></td> <td>Accidental data leakage/corruption <input type="checkbox"/></td> <td>Brute force attack <input type="checkbox"/></td> <td></td> </tr> <tr> <td>Trojan horse <input type="checkbox"/></td> <td>Spear phishing <input type="checkbox"/></td> <td>Intentional misuse of access rights by insider <input type="checkbox"/></td> <td>Malicious script injection and/or OS commanding <input type="checkbox"/></td> <td>Other <input type="checkbox"/></td> </tr> <tr> <td>Virus/worm <input type="checkbox"/></td> <td>Pretexting <input type="checkbox"/></td> <td>Intentional misuse of access rights by service provider <input type="checkbox"/></td> <td>Other exploited Vulnerability <input type="checkbox"/></td> <td></td> </tr> <tr> <td>Mobile malware <input type="checkbox"/></td> <td>Other social engineering <input type="checkbox"/></td> <td></td> <td></td> <td></td> </tr> </table>	Malware <input type="checkbox"/>	Social engineering <input type="checkbox"/>	Insider/Third Party Provider Threat <input type="checkbox"/>	Unauthorised access <input type="checkbox"/>	Denial of service <input type="checkbox"/>	Ransomware <input type="checkbox"/>	Phishing / 'ishing <input type="checkbox"/>	Accidental data leakage/corruption <input type="checkbox"/>	Brute force attack <input type="checkbox"/>		Trojan horse <input type="checkbox"/>	Spear phishing <input type="checkbox"/>	Intentional misuse of access rights by insider <input type="checkbox"/>	Malicious script injection and/or OS commanding <input type="checkbox"/>	Other <input type="checkbox"/>	Virus/worm <input type="checkbox"/>	Pretexting <input type="checkbox"/>	Intentional misuse of access rights by service provider <input type="checkbox"/>	Other exploited Vulnerability <input type="checkbox"/>		Mobile malware <input type="checkbox"/>	Other social engineering <input type="checkbox"/>			
	Malware <input type="checkbox"/>	Social engineering <input type="checkbox"/>	Insider/Third Party Provider Threat <input type="checkbox"/>	Unauthorised access <input type="checkbox"/>	Denial of service <input type="checkbox"/>																					
	Ransomware <input type="checkbox"/>	Phishing / 'ishing <input type="checkbox"/>	Accidental data leakage/corruption <input type="checkbox"/>	Brute force attack <input type="checkbox"/>																						
Trojan horse <input type="checkbox"/>	Spear phishing <input type="checkbox"/>	Intentional misuse of access rights by insider <input type="checkbox"/>	Malicious script injection and/or OS commanding <input type="checkbox"/>	Other <input type="checkbox"/>																						
Virus/worm <input type="checkbox"/>	Pretexting <input type="checkbox"/>	Intentional misuse of access rights by service provider <input type="checkbox"/>	Other exploited Vulnerability <input type="checkbox"/>																							
Mobile malware <input type="checkbox"/>	Other social engineering <input type="checkbox"/>																									
If Other, please specify:																										
Additional information:	<table border="1"> <tr> <td>Malware <input type="checkbox"/></td> <td>Collection of information <input type="checkbox"/></td> <td>Fraud <input type="checkbox"/></td> <td>Unauthorised access <input type="checkbox"/></td> <td>Abusive content <input type="checkbox"/></td> </tr> <tr> <td>Infection <input type="checkbox"/></td> <td>Scan <input type="checkbox"/></td> <td>Unauthorised or improper use of resources <input type="checkbox"/></td> <td>Account compromised <input type="checkbox"/></td> <td>SPAM <input type="checkbox"/></td> </tr> <tr> <td>Distribution <input type="checkbox"/></td> <td>Sniffing <input type="checkbox"/></td> <td>Illegitimate use of someone's name <input type="checkbox"/></td> <td>Login attempt <input type="checkbox"/></td> <td>Copyright <input type="checkbox"/></td> </tr> <tr> <td>Command & Control <input type="checkbox"/></td> <td></td> <td></td> <td></td> <td>Child pornography, racism and violence apology <input type="checkbox"/></td> </tr> <tr> <td>Not identified <input type="checkbox"/></td> <td></td> <td></td> <td></td> <td></td> </tr> </table>	Malware <input type="checkbox"/>	Collection of information <input type="checkbox"/>	Fraud <input type="checkbox"/>	Unauthorised access <input type="checkbox"/>	Abusive content <input type="checkbox"/>	Infection <input type="checkbox"/>	Scan <input type="checkbox"/>	Unauthorised or improper use of resources <input type="checkbox"/>	Account compromised <input type="checkbox"/>	SPAM <input type="checkbox"/>	Distribution <input type="checkbox"/>	Sniffing <input type="checkbox"/>	Illegitimate use of someone's name <input type="checkbox"/>	Login attempt <input type="checkbox"/>	Copyright <input type="checkbox"/>	Command & Control <input type="checkbox"/>				Child pornography, racism and violence apology <input type="checkbox"/>	Not identified <input type="checkbox"/>				
Malware <input type="checkbox"/>	Collection of information <input type="checkbox"/>	Fraud <input type="checkbox"/>	Unauthorised access <input type="checkbox"/>	Abusive content <input type="checkbox"/>																						
Infection <input type="checkbox"/>	Scan <input type="checkbox"/>	Unauthorised or improper use of resources <input type="checkbox"/>	Account compromised <input type="checkbox"/>	SPAM <input type="checkbox"/>																						
Distribution <input type="checkbox"/>	Sniffing <input type="checkbox"/>	Illegitimate use of someone's name <input type="checkbox"/>	Login attempt <input type="checkbox"/>	Copyright <input type="checkbox"/>																						
Command & Control <input type="checkbox"/>				Child pornography, racism and violence apology <input type="checkbox"/>																						
Not identified <input type="checkbox"/>																										
Incident classified as an Advanced Persistent Threat?	<input type="radio"/> Yes <input type="radio"/> No																									
Incident discovered by	<table border="1"> <tr> <td>IT security <input type="checkbox"/></td> <td>External auditor <input type="checkbox"/></td> <td>Attacker (warning) <input type="checkbox"/></td> </tr> <tr> <td>Staff member <input type="checkbox"/></td> <td>Third party provider <input type="checkbox"/></td> <td>Other <input type="checkbox"/></td> </tr> <tr> <td>Internal Audit <input type="checkbox"/></td> <td>Customer <input type="checkbox"/></td> <td></td> </tr> </table>	IT security <input type="checkbox"/>	External auditor <input type="checkbox"/>	Attacker (warning) <input type="checkbox"/>	Staff member <input type="checkbox"/>	Third party provider <input type="checkbox"/>	Other <input type="checkbox"/>	Internal Audit <input type="checkbox"/>	Customer <input type="checkbox"/>																	
IT security <input type="checkbox"/>	External auditor <input type="checkbox"/>	Attacker (warning) <input type="checkbox"/>																								
Staff member <input type="checkbox"/>	Third party provider <input type="checkbox"/>	Other <input type="checkbox"/>																								
Internal Audit <input type="checkbox"/>	Customer <input type="checkbox"/>																									
If Other, please specify:																										
Information regarding the attacker(s)	<table border="1"> <tr> <td>Terrorists <input type="checkbox"/></td> <td>Hacktivists <input type="checkbox"/></td> <td>Unknown <input type="checkbox"/></td> </tr> <tr> <td>Foreign agencies - state-sponsored hackers <input type="checkbox"/></td> <td>Inside job/Unaware employee <input type="checkbox"/></td> <td>Other <input type="checkbox"/></td> </tr> <tr> <td>Other hackers (e.g. criminals, script kiddies, etc) <input type="checkbox"/></td> <td></td> <td></td> </tr> </table>	Terrorists <input type="checkbox"/>	Hacktivists <input type="checkbox"/>	Unknown <input type="checkbox"/>	Foreign agencies - state-sponsored hackers <input type="checkbox"/>	Inside job/Unaware employee <input type="checkbox"/>	Other <input type="checkbox"/>	Other hackers (e.g. criminals, script kiddies, etc) <input type="checkbox"/>																		
Terrorists <input type="checkbox"/>	Hacktivists <input type="checkbox"/>	Unknown <input type="checkbox"/>																								
Foreign agencies - state-sponsored hackers <input type="checkbox"/>	Inside job/Unaware employee <input type="checkbox"/>	Other <input type="checkbox"/>																								
Other hackers (e.g. criminals, script kiddies, etc) <input type="checkbox"/>																										
If Other, please specify:																										



IMPACT OF THE INCIDENT & REASON FOR REPORTING					
Impact of the incident multiple selections possible	<p>Unauthorised release of information? <input type="checkbox"/></p> <p>Information related to the institution leaked? <input type="checkbox"/></p> <p>Sensitive client information leaked? <input type="checkbox"/></p> <p>Disruption of critical service? <input type="checkbox"/></p> <p>If yes, hours of disruption: <input type="text"/></p> <p>Third party provider affected? <input type="checkbox"/></p> <p>ATMs affected? <input type="checkbox"/></p> <p>Online banking fraud? <input type="checkbox"/></p> <p>Direct or indirect financial loss? <input type="checkbox"/></p> <p>Direct financial loss in euros <input type="text"/></p> <p>Estimated indirect financial loss in euros <input type="text"/></p> <p>Other impact <input type="checkbox"/></p> <p>If Other, please specify: <input type="text"/></p>	<p>Were any legal or regulatory requirements breached? <input type="checkbox"/></p> <p>If yes, please specify <input type="text"/></p>	<p>Was there any media coverage? <input type="checkbox"/></p> <p>If yes, please specify the media/newspapers/blogs that covered the topic <input type="text"/></p>		
	Reason for reporting the incident multiple selections possible	<p>Incident publicly reported and/or can cause significant reputational damage <input type="checkbox"/></p> <p>The estimated financial impact is above EUR 5 million euros or 0.1% of CET1 capital <input type="checkbox"/></p> <p>Incident was internally escalated up to the Chief Information Officer (or equivalent) outside of regular reporting <input type="checkbox"/></p> <p>Incident is likely to lead to breaches of legal or regulatory obligation <input type="checkbox"/></p>	<p>Crisis management procedures triggered (including cyber insurance) <input type="checkbox"/></p> <p>Incident was reported to the national CERT/CSIRT, security agency or police <input type="checkbox"/></p> <p>Incident may affect other institutions/organisations (systemic impact) <input type="checkbox"/></p> <p>The significance assessment does not lead to a clear outcome so the incident is reported <input type="checkbox"/></p>		
		Services and components affected multiple selections possible	<p>Endpoints/clients (laptops, PCs, OSs, user applications, etc) <input type="checkbox"/></p> <p>Enterprise software applications (SAP, Oracle, etc) <input type="checkbox"/></p> <p>Other <input type="checkbox"/></p> <p>If Other, please specify: <input type="text"/></p>	<p>Banking-related user applications/software (sales, trading, credit, risk, etc) <input type="checkbox"/></p> <p>Internet platforms (webservers, application servers, etc) <input type="checkbox"/></p>	<p>Networking and telecommunications (firewalls, routers, switches, PBX, etc) <input type="checkbox"/></p> <p>Data management and storage (file servers, databases, data warehouses, etc) <input type="checkbox"/></p>
			Business lines affected multiple selections possible	<p>Corporate Finance <input type="checkbox"/></p> <p>Commercial Banking <input type="checkbox"/></p> <p>Asset Management <input type="checkbox"/></p> <p>If Other, please specify: <input type="text"/></p>	<p>Trading & Sales <input type="checkbox"/></p> <p>Payment & Settlement <input type="checkbox"/></p> <p>Retail Brokerage <input type="checkbox"/></p>



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

